Real time demonstration of high bitrate quantum random number generation with coherent laser light

T. Symul, S. M. Assad, and P. K. Lam

Citation: Applied Physics Letters 98, 231103 (2011); doi: 10.1063/1.3597793
View online: http://dx.doi.org/10.1063/1.3597793
View Table of Contents: http://scitation.aip.org/content/aip/journal/apl/98/23?ver=pdcov
Published by the AIP Publishing

Articles you may be interested in
Addendum: "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements" [Appl. Phys. Lett. 98, 171105 (2011)]
Appl. Phys. Lett. 101, 159901 (2012); 10.1063/1.4758702

An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements
Appl. Phys. Lett. 98, 171105 (2011); 10.1063/1.3578456

A high speed, postprocessing free, quantum random number generator
Appl. Phys. Lett. 93, 031109 (2008); 10.1063/1.2961000

Scheme for a quantum random number generator
J. Appl. Phys. 100, 056107 (2006); 10.1063/1.2338830

A fast and compact quantum random number generator
Rev. Sci. Instrum. 71, 1675 (2000); 10.1063/1.1150518
Real time demonstration of high bitrate quantum random number generation with coherent laser light

T. Symul, S. M. Assad, and P. K. Lam

Department of Quantum Science, Centre for Quantum Computation and Communication Technology, Australian National University, Canberra ACT 0200, Australia

(Received 11 February 2011; accepted 17 May 2011; published online 7 June 2011)

We present a random number generation scheme that uses broadband measurements of the vacuum field contained in the radio-frequency sidebands of a single-mode laser. Even though the measurements may contain technical noise, we show that suitable algorithms can transform the digitized photocurrents into a string of random numbers that can be made arbitrarily correlated with a subset of the quantum fluctuations (high quantum correlation regime) or arbitrarily immune to environmental fluctuations (high environmental immunity). We demonstrate up to 2 Gbps of real time random number generation that were verified using standard randomness tests. © 2011 American Institute of Physics. [doi:10.1063/1.3597793]

Reliable and unbiased random numbers (RNs) are needed for a range of applications spanning from numerical modeling to cryptographic communications. With the numerous improvements in quantum key distribution (QKD) protocols,1,2 fast and reliable RN generation is now one of the main technical impediments to high-speed QKD. While there are algorithms that can generate pseudo-RNs, they can never be perfectly random nor indeterministic. True RNs from physical processes may offer a surefire solution.

Several physical RN generation schemes have been proposed and demonstrated3–5 including schemes based on single photon detections.6–11 The limit in speed of these systems are in the dead time of photon counters. An alternative quantum approach to photon counting is to use the vacuum fluctuations of an electromagnetic field for RN generation.12,13 In this letter, we demonstrate a simple scheme to measure and convert vacuum field fluctuations into RNs.

The schematic of the quantum RN generator is shown in Fig. 1. A single-mode laser beam at 1550 nm is used as the light source. A few milliwatt of light is split into two equal intensity beams and detected by a pair of photodetectors in a balanced homodyne scheme. When the average laser field amplitude $\alpha$ is significantly larger than the vacuum field fluctuation the subtracted photocurrent from the pair of detectors is proportional to $\alpha X_v(\omega)$, where $X_v$ is the quadrature amplitude of the vacuum field. The balanced homodyne setup

![Diagram of RN generation schematic](image)

**FIG. 1.** (Color online) RN generation schematic. Top left figure shows the spectra of the quadrature amplitudes for the vacuum fluctuations, $X_v$ and the laser mode $X_l$. The shaded frequency range, $\Delta \omega$, shows a region where the laser source is quantum noise limited. (a) Sum (s) and difference (d) of the laser vacuum fluctuations, as well as electronic noise (e) from a pair of homodyne photodetectors. The shaded frequency range is used for generating RNs. (b) Digitized and demodulated shot noise and electronic noise spectra. (c) A filter function is used to correct for the non-uniform electronic gain. The quantum noise at this stage has an unbiased Gaussian distribution with a normalized mean at 0 dB and dark noise clearance of 8.5 dB. (d) High randomness of the final digital RNs depicted by the featureless color plot. BS: 50/50 beamsplitter; D: photodiode; ADC: analog to digital converter; NUM. PROC.: numerical processing algorithm; and Q-RN: final generated RNs.

Author to whom correspondence should be addressed. Electronic mail: cqtsma@gmail.com.

Electronic mail: ping.lam@anu.edu.au.
therefore measures the amplified quadrature amplitude of the vacuum field fluctuations. Only sideband frequencies well above the technical noise frequencies of the laser are used for RN generation [shaded region of the radio frequency (rf) spectrum of Fig. 1(a)]. This is achieved by demodulating the photocurrent with an rf frequency (1.6 GHz) followed by a low pass filter. The undulations in the spectra are due to nonuniform rf electronic gain in the photodetectors amplification stages [Fig. 1(b)]. Nevertheless, the quantum noise has a constant clearance above the electronic noise level of 8.5 dB. Using a field-programmable gate array (FPGA) a filter function can be programmed to neutralize the nonuniform electronic gain as shown in Fig. 1(c). Finally, using suitable numerical processes, the quantum noise is converted into a sequence of random digital bits as depicted by the 8-bits color code in Fig. 1(d).

In practice, vacuum fluctuations cannot be detected in complete isolation. The electronic noise of the photodetector will be superimposed onto the measured photocurrents. While it is reasonable to assume that the quantum noise of a vacuum field $X_e$ is perfectly random over all frequencies and cannot be tampered with, electronic noise may not possess these ideal properties. For this letter, we would like to consider two possible scenarios.

In the first scenario, we assume that the electronic noise is untampered. We wish to find a protocol to generate RNs solely from closely tracking the quantum fluctuations of the vacuum field. We will show that in this scenario, a 1-bit digitized encoding of the vacuum fluctuations, together with thresholding, can indeed allow arbitrarily high quantum correlation. In the second scenario we assume that the electronic noise may be tampered and is untrustworthy. We desire an algorithm that will generate RNs that are tamper-proof, even in the presence of possibly forged electronic noise. Provided that quantum noise remains the dominant source of noise, we will show that digitizing the vacuum fluctuations into multiple bits, and then discarding the most-significant bits, can indeed allow arbitrarily high environmental immunity. Correlations between environmental noise and the generated RNs can be made arbitrarily small.

We describe the measured signal as $X_m = X_v + X_e$, where $X_e$ corresponds to the electronic noise superimposed onto the vacuum fluctuations $X_v$ [see Fig. 2(a)]. $X_v$ and $X_e$ can be modeled as two uncorrelated Gaussian distributions of zero mean and variance $V_v$ and $V_e$, respectively. $X_m$ is also Gaussian with a conditional probability given by

$$P(X_m|X_v) = \frac{1}{\sqrt{2\pi V_v}} e^{-(X_m - X_v)^2/2V_v}.$$  \hspace{1cm} (1)

In order to extract $n$-bit RNs from $X_m$ with uniform probabilities, we need to transform the measured Gaussian distributed photocurrent into a uniform distribution of $Y_m = [1 + \text{erf}(X_m/\sqrt{2V_m})]/2$. The $n$-bit RNs require the distribution $Y_m$ to be divided into $2^n$ equal and nonoverlapping domains (as shown in Fig. 2 for the case of $n=3$). We can then index each domain, preferably by using Gray’s binary encoding, to minimize the perturbations due to unaccounted technical noise so that the $2^n$ domains now correspond directly to the $n$-bits RNs [see Fig. 2(b)].

We introduce a thresholding condition to reject data points that fall within a certain range $\Delta_e$ between two adjacent domains (see Fig. 2). We digitize continuous variable quantities into a binary $n$-bits with $Y_m=(Y_m^{(1)}Y_m^{(2)}\ldots Y_m^{(n)})$, where $Y_m^{(i)} \in \{0, 1\}$. $Y_m^{(i)}$ is the most significant bit (MSB) and $Y_m^{(n)}$ the least significant bit (LSB) in Gray’s binary decomposition. We define a probability of error, $P_{e,q} = P(Y_m^{(i)} \neq Y_v^{(i)})$. This quantifies the discrepancy between a measured bit and the vacuum fluctuations. Perturbation from the electronic noise, which causes the digitized bit to differ from the vacuum fluctuation, is referred to as an error. $P_{e,q}=0$ means that the generated RNs are the perfect digitization of pure vacuum fluctuations.

We also introduce the notion of information leakage from the electronic noise $I_e$. This information leakage is the amount of information that can be imposed on the final random bits by somebody having access to the electronic noise. Using Shannon’s binary information formula, we obtained

$$I_e = 1 + P_{e,q} \log_2(P_{e,q}) + (1 - P_{e,q}) \log_2(1 - P_{e,q}),$$  \hspace{1cm} (2)

where analogous to $P_{e,q}$, $P_{e,e}$ is the probability of error that the measured $i$th-bit differs from the electronic noise. $I_e=0$ means that the generated RNs are indeterminate even with full knowledge of the electronic noise.

Figure 3 shows $I_e$ and $P_{e,q}$ plotted as a function of the RN generation rate $R = n[1 - P_{\text{th}}(\Delta_e)]$ for $n=1,2,3,4,5$ bits extracted per measurement, where $P_{\text{th}}(\Delta_e)$ is the probability that a bit is rejected because it lies within one of the thresholding areas. From Fig. 3(a) we note that the amount of information leaked through the electronic noise decreases for the LSB with high bit encoding. Moreover, thresholding paradoxically increases $I_e$. Minimizing $I_e$ therefore requires high bit encoding, no thresholding, and omission of all but the LSB. In the case of 5-bits encoding, the best result obtained using this protocol was $I_e < 10^{-6}$ for the LSB.
In conclusion, we have demonstrated the generation of continuous random bit sequences at a rate of 2 Gbps in real time by sampling the broadband vacuum fluctuations. We proposed two methods of generating RNs where: (i) quantum correlation is optimized for a near ideal representation of a thresholded random subset of the vacuum fluctuations, and (ii) environmental immunity is optimized to combat against possible tampering of the electronic noise.

We thank QuintessenceLabs, M. Neharkar, and K. L. Chong for technical assistance. This research was conducted by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE110001029).

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
2. S. Braunstein and P. van Loock, Rev. Mod. Phys. 77, 513 (2005).
3. M. Isida and H. Ikeda, Ann. Inst. Stat. Math. 8, 119 (1956).
4. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 98, 231103 (2011).
5. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. 47, 759 (2000).
6. S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Omschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) 464, 1021 (2010).
7. T. Jennewein, U. Acleitner, G. Weihs, H. Weinfurther, and A. Zeilinger, Rev. Sci. Instrum. 71, 1675 (2000).
8. D. Wolfgang and E. Hildebrandt, U.S. Patent No. 6393448 B1 (21 May 2002).
9. A. Trifonov, H. Vig, U.S. Patent No. 7284024 B1 (16 October 2007).
10. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauner, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics 4, 711 (2010).
11. F. Gray, U.S. Patent No. 2632058 (17 March 1953).
12. NIST Statistical Test Suite-2.1, 2010.
13. G. Marsaglia, DIEHARD Battery of Tests of Randomness, 1995.