Bias-free true random-number generator

Wei Wei and Hong Guo*

CREAM Group, State Key Laboratory of Advanced Optical Communication Systems and Networks and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China

**Corresponding author: hongguo@pku.edu.cn*

Received March 26, 2009; revised May 6, 2009; accepted May 7, 2009; posted May 19, 2009 (Doc. ID 109336); published June 11, 2009

We propose what we believe to be a new approach to nondeterministic random-number generation. The randomness originated from the uncorrelated nature of consecutive laser pulses with Poissonian photon statistics and that of photon number detections is used to generate random bit, and the von Neumann correction method is used to extract the final random bit. This method is proved to be bias free in randomness generation, provided that the single photon detections are mutually independent. Further, it has the advantage in fast random bit generation, since no postprocessing is needed. A true random-number generator based on this method is realized, and its randomness is tested and guaranteed using three statistical test batteries.

OCIS codes: 030.5260, 270.5568.

Random numbers are essential in an extremely wide application range, such as statistical sampling [1], computer simulations [2], randomized algorithm [3], and cryptography [4]. Pseudorandom numbers generated with certain algorithms are widely used in modern digital electronic information systems. Although pseudorandom-number generators (PRNGs) have been highly refined in terms of generation rate and robustness against random test, thanks to the development of computer science and technology, the algorithm-based PRNG cannot generate true randomness and so has the essential drawback in the applications, which require physical randomness, such as quantum cryptography that requires unpredictable bit strings to ensure the inability of estimation [5]. True random numbers should be unpredictable and unreproducible. For this reason, physical random phenomena, such as the decay of radioactive nucleus [6], thermal noise in resistors [7], frequency jitter of electronic oscillators [8], photon emission noise [9,10], etc., are used as physical sources for nondeterministic random-number generations. Random number generators based on these physical random processes are termed as true random-number generators (TRNGs), and those based on photon emission noise extract random bits either from the random time intervals between photon emissions of semiconductors [9] or from the collapse of the photon wave function on random gating cycle [10]. In these schemes, the timing precision is a limitation to the random-bit generation rate.

In this Letter, we propose a new approach to realize a TRNG based on photon number detection of weak laser pulse. The main advantage of this new type of TRNG is that it has equal probabilities for the bits of ones and zeros and is bias free from the variability of the device and the environment. Moreover, this new type of TRNG can be realized with a simple and compact setup. It can generate random numbers at a high speed and is limited only by the repetition rate of the single-photon detector (SPD). These advantages make it applicable for quantum cryptography and other applications, which require fast generation of true random bits.

According to the quantum theory of laser, the photon statistics for laser operating above threshold approaches to Poissonian [11], indicating that laser light has the unity second-order correlation function [11] and the photon numbers of different laser pulses are mutually independent. A TRNG can be implemented based on this fact. Since the photon number distribution of partially absorbed light follows a Bernoulli transform of the initial field [12], provided that the detections are mutually independent, it can be proved that the photon numbers detected by a photodetector from weak laser pulses are also Poissonian distributed, i.e., $P_\eta(n)=(\eta\lambda)^n\exp(-\eta\lambda)/n!$, where λ is the mean photon number of the weak laser pulses and η is the detection efficiency of the photodetector. The probabilities of $n_1>n_2$ and $n_1<n_2$ are equal, where n_1 and n_2 are the photon numbers of two consecutive pulses. In the experiment, we use an avalanche photodiode (APD) operating in gated Geiger mode for the photon detection, which does not distinguish the photon numbers above zero. Thus, we code $n_1>0$ and $n_2=0$ as bit **1** and $n_1=0$ and $n_2>0$ as bit **0**. Then, for two consecutive detections, the probabilities $P(\mathbf{1})$ and $P(\mathbf{0})$ of generating bits **1** and **0**, respectively, follow

$$P(\mathbf{1})=P(\mathbf{0})=P_\eta(n>0)P_\eta(n=0)=e^{-\eta\lambda}(1-e^{-\eta\lambda}). \tag{1}$$

It is then evident that the probabilities of generating the bits of ones and zeros are *intrinsically* equal, and hence a TRNG based on this method is physically unbiased.

The experiment setup of our TRNG is shown in Fig. 1. Laser pulses (300 ps at 1550 nm) are generated by a pulsed distributed feedback (DFB) diode laser (id300, id Quantique), and the mean photon number of each pulse can be continuously adjusted by a flexible attenuator (FA). The photon number is detected by an InGaAs APD-based SPD (id200, id

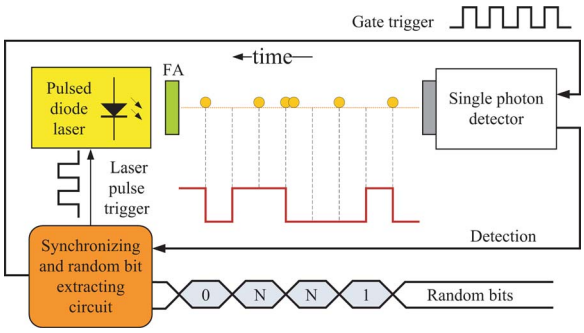

Fig. 1. (Color online) Schematic experiment setup of our TRNG. FA, flexible attenuator. 1, bit 1. 0, bit 0. N, not used.

Quantique) working in gated Geiger mode. The gate width of 2.5 ns is chosen in the experiment to minimize the probability of the dark count. We develop a FPGA-based circuit for system synchronization and random-bit extraction. The true random bits are derived from the sequence of detection signals using von Neumann correction method [13]. Using this method, we scan the random sequence from left to right reading successive pairs of photon detections. The outputs of $n_1>0$ and $n_2=0$ and $n_1=0$ and $n_2>0$ are adopted as the bits **1** and **0**, respectively, while those of $n_1>0$ and $n_2>0$ and $n_1=0$ and $n_2=0$ are abandoned, although they also contain randomness that can be extracted by other correction procedures (see, e.g., [14]). However, for doing this some postprocessing is needed, which may *greatly* reduce the random bit generation rate. We, instead, adopt the von Neumann correction method for our TRNG because it is simple and easy to implement with digital logic and no postprocessing is needed. The repetition frequency of the generation and detection of laser pulses is chosen as 1 MHz, and the dark count probability for our SPD is measured to be 3×10^{-5} with a gate width of 2.5 ns. The detection efficiency of SPD is ~10% (specification of id Quantique).

To ensure that our TRNG generates true random bits, we must confirm that every single-photon detection of the laser pulses is mutually independent. In detection, the after-pulse effect of the APD may cause some correlations between two consecutive detection results. For an APD operating in gated Geiger mode, carriers are trapped after every avalanche. If some of them emit during the next gate-on time, it can trigger a new avalanche (after pulse), even though no photon is absorbed. For the detection with InGaAs APDs, after pulse is frequently found when the repetition frequency exceeds 1 MHz. Since only traps with an emission lifetime comparable with or longer than the time interval between two consecutive gates generate after pulses, we can introduce a dead time following an avalanche, during which no gate is applied to the APD. This is an effective way to eliminate the after-pulse effect [15]. For the SPD of our experiment, a dead time of 8 μs is chosen, and our experiment results show that the probability of after pulse is negligible and the nonsignal counts come only from the dark counts.

A technically important issue for TRNG is its efficiency to extract true random bits from random events, η_{TRNG}, which is defined as the number of random bits per random event. For our TRNG, a random event is a photon number detection of a weak laser pulse. Thus, η_{TRNG} is equal to half of the probability that a random bit is generated by a pair of detections, i.e.,

$$\eta_{\mathrm{TRNG}}=\frac{P(\mathbf{1})+P(\mathbf{0})}{2}=e^{-\eta\lambda}(1-e^{-\eta\lambda}). \tag{2}$$

When $\eta\lambda=\ln 2\approx0.693$, we get the optimal η_{TRNG} as 0.25. This is also the point that the probabilities of detecting zero or above zero photons are equal. The value of η_{TRNG} varying with $\eta\lambda$ is illustrated in Fig. 2. It shows that when η_{TRNG} is at its maximum, it is not sensitive to slight fluctuations of $\eta\lambda$ around 0.693. Experimentally, we adjust the FA to the state where the probabilities of detecting zero and above zero photons are approximately equal. In this case, our TRNG generates intrinsically unbiased random bits at the optimal rate permitted by the current setup.

We use three batteries of statistical tests to evaluate the performance of our TRNG. They are ENT, a psuedorandom number sequence test program [16], Diehard, a battery of tests [17], and STS, a statistical test suite for random and psuedorandom number generators for cryptographic applications [18]. We record a bit file of 9.45×10^8 bits for the tests. The ENT results of our TRNG are entropy=1.000000 bit per bit (and the optimum compression would reduce the bit file by 0%) χ^2 distribution is 1.49 (and randomly would exceed this value by 22.17% of the times) arithmetic mean value of data bits is 0.5000 (0.5=random), Monte Carlo value for π is 3.141747714 (error of 0.00%), and serial correlation coefficient is 0.000041 (totally uncorrelated=0.0). A DIEHARD test, with a data sample of 10–11 Mbytes, is considered successful if $0.01\le p\le0.99$ is satisfied [17]. For multiple p-value cases, we use a Kolmogorov–Smirnov (KS) test to obtain a final p value, and the test result is based on the final p value. The results of the DIEHARD test for our

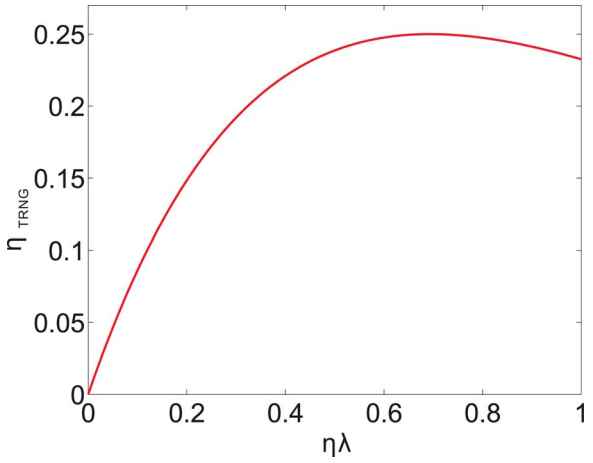

Fig. 2. (Color online) Random-bit efficiency η_{TRNG} as a function of $\eta\lambda$. η, detection efficiency of SPD; λ, mean photon number of each laser pulse.

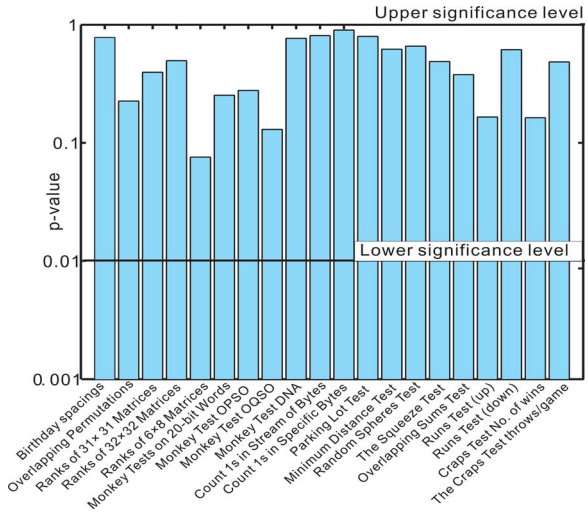

Fig. 3. (Color online) Results of DIEHARD. All tests are passed at lower (upper) significance level of 0.01 (0.99).

TRNG are illustrated in Fig. 3 and show that all final p values are within 0.01–0.99. The last one is for each test of STS; the long sequence is divided into 920 separate smaller streams of 10^6 bits. An individual bit stream is usually considered to pass a particular test when $p \geq 0.01$, and consequently, 98%–100% of all the bit streams are expected to pass a particular test owing to statistical fluctuations [18]. Figure 4 shows that all tests are passed with the final p values (after KS test) above the significance level, and all testing results are within the confidence interval for the proportion of pass. The above three random tests show that our TRNG has a good quality in randomness.

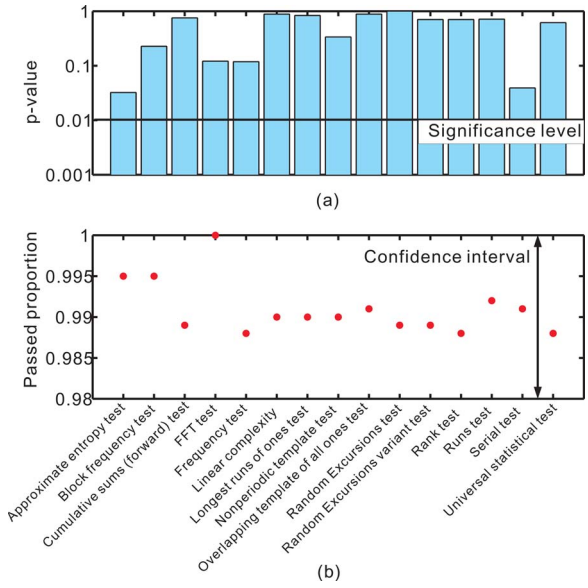

Fig. 4. (Color online) Results of STS. All tests are passed at the significance level of 0.01.

We propose a new approach to realize a TRNG that is intrinsically bias free. Its randomness is based on the photon-number detection of weak laser pulses. Compared with other bias free TRNGs, e.g., those based on photon emission noise, the complicated timing circuits with high precision are not needed in our TRNG and thus are convenient to be implemented. Currently, the random-bit generation rate of our TRNG is restricted only by the repetition rate of our InGaAs APD-based SPD. Hence, a faster TRNG can be experimentally implemented with a faster, say, silicon APD-based SPD and the random-bit generation rate can be up to gigabit/second, which is suitable for high-speed applications.

This work is supported by the Key Project of National Natural Science Foundation of China (NSFC) (grant 60837004). We are grateful to X. Peng, W. Jiang, J. W. Zhang, T. Liu, J. Yang, Z. G. Zhang, and F. Grosshans for their help and suggestions during the drafting of this Letter.

References

1. S. L. Lohr, *Sampling: Design and Analysis* (Duxbury, 1999).
2. J. E. Gentle, *Random Number Generation and Monte Carlo Methods (Statistics & Computing)*, 2nd ed. (Springer-Verlag, 2003).
3. M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis* (Cambridge U. Press, 2005).
4. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC, 1997).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
6. J. Walker, http://www.fourmilab.ch/hotbits/hardware3.html.
7. W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, IEEE Trans. Circuits and Syst., I: Fundam. Theory Appl. **44**, 521 (1997).
8. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, IEEE Trans. Comput. **52**, 403 (2003).
9. M. Stipčević and B. Medved Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
10. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
11. D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, 1994).
12. U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge U. Press, 1997).
13. J. von Neumann, in *Monte Carlo Method*, National Bureau of Standards Applied Mathematics Series (1951), Vol. 12, pp. 36–38.
14. Y. Peres, Ann. Stat. **20**, 590 (1992).
15. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
16. J. Walker, http://www.fourmilab.ch/random/.
17. G. Marsaglia, http://www.stat.fsu.edu/pub/diehard/.
18. NIST, http://csrc.nist.gov/rng/.