Quantum random-number generator based on a photon-number-resolving detector

Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu,* and Heping Zeng†

State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, China

(Received 21 December 2010; published 23 February 2011)

We demonstrated a high-efficiency quantum random number generator which takes inherent advantage of the photon number distribution randomness of a coherent light source. This scheme was realized by comparing the photon flux of consecutive pulses with a photon number resolving detector. The random bit generation rate could reach 2.4 MHz with a system clock of 6.0 MHz, corresponding to a random bit generation efficiency as high as 40%. The random number files passed all the stringent statistical tests.

DOI: 10.1103/PhysRevA.83.023820 PACS number(s): 42.50.Ar, 42.50.Lc, 05.40.−a

I. INTRODUCTION

Random number generators (RNG's) are indispensable devices in many fields ranging from commercial applications like lottery games to scientific applications like Monte Carlo simulations. The algorithm-based RNG's from a simple computer algorithm are fast and easily obtained but somehow deterministic, which cannot be used for secure applications such as cryptography. Even complex Monte Carlo simulations using pseudorandom numbers can produce erroneous results [1]. True random numbers should be unpredictable and irreproducible. For this reason, physical random phenomena, such as the decay of radioactive nucleus [2], thermal noise in resistors [3], frequency jitter of electronic oscillators [4,5], photon emission noise [6–13], photon entanglement [14,15], laser phase noise [16], vacuum state [17,18], using a beam splitter [19,20], and so on are used for nondeterministic random-number generation. Besides the "randomness" of the generated series of bits, the generation rate is also of paramount importance in practical applications. System complexity, cost, reliability, and sensitivity to control parameters for an RNG should be taken into account as well.

Taking advantage of the inherent randomness of quantum systems, quantum random number generators (QRNG's) can provide a series of random bits that are by no means predictable. Efficient and high speed QRNG based on single-photon detection has been demonstrated in the last decade [8,14,21], which were basically realized in the joint detection of single photons with either a spatial or temporal discrimination, or a combination of both. Most of the light sources in QRNG's used attenuated lasers as weak coherent-state sources which could not offer ideal single-photon pulses. Multiphoton pulses from the coherent light sources could not be distinguished from the one-photon pulses by a standard single-photon detector. Thus, the multiphoton pulses had to be abandoned in the QRNG's, decreasing the generation efficiency of the random bits.

In this paper, we demonstrate an approach to realize a true random number generator based on the multiphoton pulse detection by the photon number resolving detector (PNRD). Owing to the PNRD [22] employed in the scheme, the exact number of photons for each pulse from a coherent light source could be identified. The photon numbers in consecutive pulses were compared and used to generate the random-number bits, increasing the generation efficiency of the random bits. The scheme based on photon number resolving detection provided high-quality randomness at high speed without any necessity of classical postprocessing with software or hardware.

II. EXPERIMENTAL SCHEME FOR QRNG'S BASED ON PHOTON-NUMBER-RESOLVING DETECTION

According to the theory in quantum optics, the distribution of photons from an attenuated laser with a constant intensity obeys the Poissonian law of small numbers. The probability of containing n photons in a pulse with the average photon number per pulse of $\bar{n}$ can be written as

$$P(n) = \frac{\bar{n}^n e^{-\bar{n}}}{n!}. \tag{1}$$

The exact number of photons contained in each light pulse is absolutely independent and unpredictable [25]. Considering the photoelectric counting statistics of the coherent optical field, the photon detections are mutually independent as well. The photodetector of efficiency η can be considered as a perfect detector of 100% efficiency with a beam splitter with transmittance of η in front of it. The random sampling nature of the beam splitting process gradually randomizes the statistics, irrespective of the original statistics of the incoming photons. Therefore, the photon numbers detected by photodetector from the coherent light source are also Poissonian distributed. The probability of detecting n photons with a detector of η efficiency when the average photon number per pulse is $\bar{n}$ can be

$$p(n) = \frac{(\eta\bar{n})^n e^{-\eta\bar{n}}}{n!}. \tag{2}$$

Let us assume n_1 and n_2 as the photon numbers of two consecutive pulses. As shown in Fig. 1 by comparing the detecting output of odd clock cycles (n_1) with the detecting output of the following even clock cycles (n_2), we can code $n_1 > n_2$ as bit 1 and $n_1 < n_2$ as bit 0. If $n_1 = n_2$, the cycle is abandoned. In this way, we could take the inherent advantage of photon number distribution to get perfect random numbers. For two consecutive detections, the probability of getting

*gwu@phy.ecnu.edu.cn
†hpzeng@phy.ecnu.edu.cn

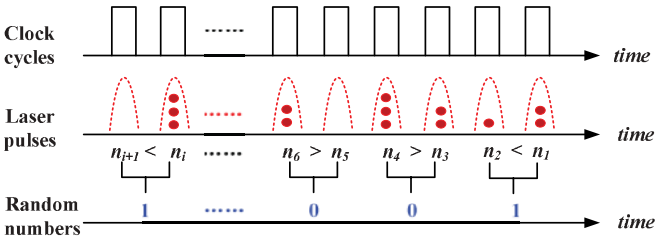

FIG. 1. (Color online) Random number generation scheme based on photon statistics.

random bit "1" and "0" would be

$$P_R(1) = p(0)p(1) + p(0)p(2) + p(0)p(3), \ldots, \\ p(1)p(2) + p(1)p(3), \ldots, \\ p(n)p(n+1), \ldots, \quad (3)$$

$$P_R(0) = p(1)p(0) + p(2)p(0) + p(3)p(0), \ldots, \\ p(2)p(1) + p(3)p(1), \ldots, \\ p(n+1)p(n), \ldots, \quad (4)$$

where $p(n)$ presents the probability of detection n photons within one pulse. Although $p(n)$ differs from one to another, the total probability of get random bit "1" $P_R(1)$ equals $P_R(0)$, which provides the unbiased base of the RNG. To obtain the exact number of photons detected within the pulse, a PNRD is required. Considering the photon number resolving capability of the detector, we need to set the discrimination up-boundary N for the detected photon number. If $n_1 \geqslant N$, and $n_2 \geqslant N$, we consider it as the same case of $n_1 = n_2$, and abandon the cycle. Therefore, there exists a random bit generation efficiency η_R. η_R is defined as the number of random bits per random event and can be written as

$$\eta_R = \frac{P(1) + P(0)}{2} \\ = \frac{1 - p(0)p(0) - p(1)p(1) - (n > N)p(n > N)}{2}. \quad (5)$$

Then, for a given N, η_R is a function of $\bar{n}$ according to the Poissonian law. Obviously, if we could set a larger discrimination up-boundary N, the higher the efficiency η_R would be. With infinite N, the maximum efficiency would be 50%. In previous RNG schemes by comparing the consecutive photon pulse detection with single-photon detectors, the up-boundary N was 1. Thus the optimal η_R could only reach 25%. And with the increase of the average detected photon number, the efficiency decreased is shown in Fig. 2. But with PNRD's, N could be larger than 1, increasing the random bit generation efficiency. However, limited by the photon number resolving capability and the complexity of the discrimination circuit, N could not be infinitely large. In our design, we set $N = 7$, meaning that photon pulses containing $n \geqslant 7$ were considered as identical. We simulated the random bit generation efficiency as a function of the average detected photon per pulse with $N = 7$ as shown in Fig. 2. The optimal η_R of 42.5% could be achieved when $\bar{n} = 4.10$. And η_R was changed slowly and smoothly when $\bar{n}$ was around 3–5 photons.

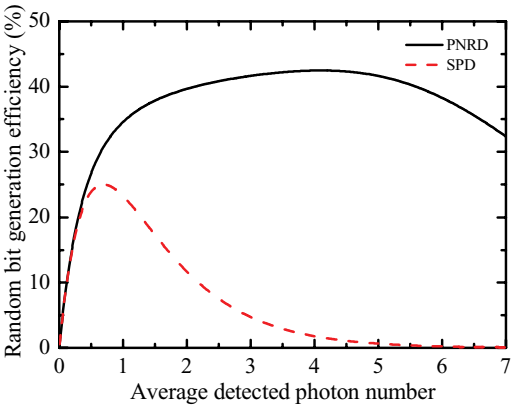

FIG. 2. (Color online) Random bit generation efficiency (η_R) as a function of average detected photon number. Black straight line: with PNRD ($N = 7$); red dashed line: with single-photon detector ($N = 1$).

III. EXPERIMENTAL REALIZATION OF QRNG WITH A PHOTON NUMBER RESOLVING DETECTOR

Figure 3 shows the configuration of the QRNG with PNRD. The photons in the coherent state were from an attenuated pulsed laser diode emitting at 850 nm. The repetition rate of the laser was 6.0 MHz and the pulse duration was 920 ps. The laser pulse was attenuated to contain dozens of photons per pulse before being sent to the detection part. The detector we used in the experiment was a photon-number-resolving detector based on a silicon multipixel photon counter (MPPC). The MPPC was made up of multiple silicon avalanche photodiode pixels [22–24]. The active area of the MPPC was 1 mm^2 with 10×10 pixels (S10362-11, Hamamatsu). Each pixel responded to the arriving photon and produced an avalanche pulse independently when the device was operated in the Geiger mode. As all the pixels shared the same cathode and anode outputs, the output of the MPPC was the sum of the response of every single pixel. The MPPC worked in the passively quenched mode. The bias voltage of the APD was 68.9 V and the gain of each pixel was about 7×10^5. The

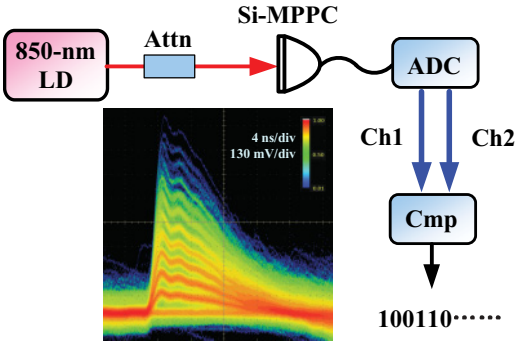

FIG. 3. (Color online) Configuration of the QRNG. LD: laser diode emitting at 850 nm; Attn: optical intensity attenuator; ADC: analog-to-digital convertor with seven levels; Cmp: comparator. Inset: Color grading waveform of the APD response.

operation temperature of the MPPC was set at −28°C keeping the total dark counts at 8.5 kHz. The detection efficiency of the MPPC was about 6% around 850 nm. To make full use of all the pixels, the beam spot of the incident photon pulse was adjusted to be a little larger than the photosensitive area of the MPPC. A 4-ns sampling gate that was synchronous to the laser source was used to extract the photon clicks, decreasing the afterpulsing effect and dark counts. The output signal of the MPPC was sent to two cascade-connected 10-dB broadband amplifiers. The response of the Si-MPP was measured by a 6-GHz oscilloscope and is shown in the inset of Fig. 3. According to the simulation in Sec. II, we controlled the intensity of the incident laser pulse to have the average detection photon number to be around 3–5. The average photon number was 3.83 in the generation of the random bits, close to the optimal average photon number for our QRNG.

The maximum detection rate of the MPPC was 8 MHz due to the passive charging and discharging of all the pixels. However, according to the charging and discharging feature of silicon APD, about 120 ns were necessary for recharging without any quenching-reset system. If a photon-induced avalanche pulse used up all of the carriers, the consecutive photon-induced avalanche might not get enough carriers to reflect all the photons that trigger the MPPC. Therefore, the outputs could not faithfully reflect the photon number in the following pulse, meaning that the detected photon number distribution did not obey Poissonian law any longer. Thus the randomness would be destroyed. Therefore, we operated it with the system clock of 6 MHz to avoid the error counts by recharging. Naturally, the RNG system could work properly with the system clock below 6 MHz.

We digitalized the response of the MPPC by a seven-level amplitude detection analog-to-digital conversion (ADC), which could classify the incoming photon pulses into eight different levels. Therefore, we could distinguish from the 0-photon pulse, 1-photon pulse up to $n \geqslant 7$-photon pulse. A comparator compared the detected photon numbers in the odd clock cycle (Ch1) with that in the even clock cycle (Ch2). In this way, the random bit series was generated.

In the experiment, we took the test at the system clock of 6 MHz, and the bit generation rate was 2.4 MHz. Therefore,

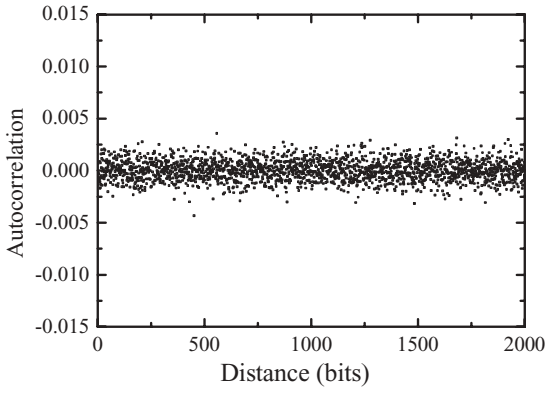

FIG. 4. Bit autocorrelation as a function of bit distance.

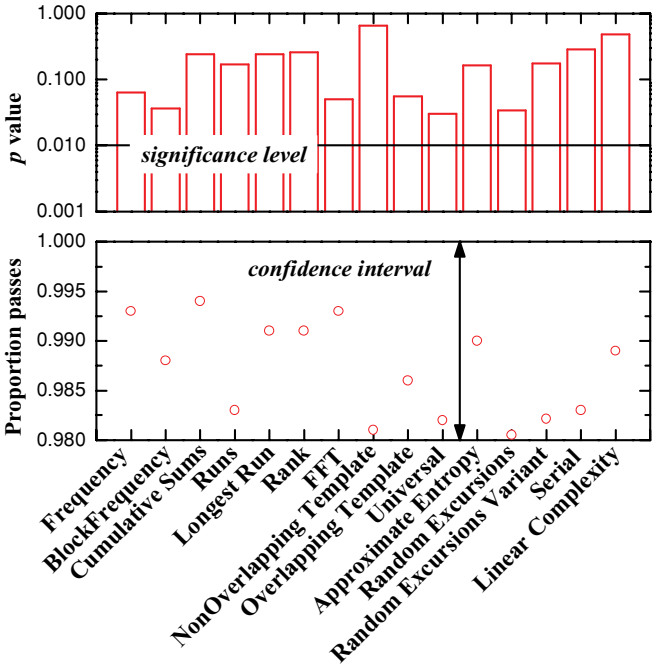

FIG. 5. (Color online) Results of the STS 2.1.1 tests on 1000 × 10^6 bit patterns of binary bits.

$\eta_R = 40\%$, agreeing with the theoretical simulation. We tested the autocorrelation between bits at distance m according to

$$\Gamma_m = \frac{1}{M}\sum_{i=1}^{M-1} x_i \oplus x_{(i+m) \bmod M}, \tag{6}$$

where $\{x_i\}_i^{M-1} = 0$ is a sequence of M bits. Applying this test on 10^6 raw bits, we found no particular correlation except the case $m = 1$ as shown in Fig. 4. The correlation between adjacent bits was on the order of 2×10^{-3}.

The random bit series was also sent to "Statistical Test Suite" (STS 2.1.1) from NIST [26,27] for verifying the reliability of the randomness. The result is shown in Fig. 5. In this test, the large experimental data were divided into 1000 separate smaller streams of 10^6 bits. It is usually considered to pass a particular test when $p \geqslant 0.01$, and consequently, 98%–100% of all the bit streams are expected to pass a particular test owing to statistical fluctuations. In all the tests, the quantum random number series passed successfully, indicating the reliability of the RNG.

The random bit generation rate of the scheme was limited by the maximum detection rate of the MPPC due to the charging and discharging time of the APD. With passive charging and discharging model, the maximum detection rate for QRNG could not be higher than 6.0 MHz for the true randomness. Meanwhile if the effective active recharge circuit could be applied on MPPC to speed up recovery, the PNRD could work up to around dozens of MHz. Therefore, the random generation rate could upgrade to tens of MHz.

IV. CONCLUSION

In conclusion, we demonstrated a new type of QRNG based on photon distribution randomness by employing photon

number resolving detection. The random bit generation rate could reach 2.4 MHz when the system clock was 6.0 MHz, corresponding to a random bit generation efficiency as high as 40%. The random number files were subjected to stringent statistical tests and were found to pass all. This convenient scheme could get a much higher bit generation rate, if suitable active recharge circuits or some kinds of ultrahigh-speed silicon avalanche photodiode were to be developed.

ACKNOWLEDGMENTS

This work was funded, in part, by the National Natural Science Fund of China (10904039, 10990101, and 91021014), Key Project Sponsored by the National Education Ministry of China (108058), Research Fund for the Doctoral Program of Higher Education of China (200802691032), and Shanghai Rising-Star Program (10QA1402100).

[1] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, Phys. Rev. Lett. **69**, 3382 (1992).
[2] J. Walker, [http://www.fourmilab.ch/hotbits/hardware3.html].
[3] W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, IEEE Trans. Circuit Syst., I: Fundam. Theory Appl. **44**, 521 (1997).
[4] J. T. Gleeson, Appl. Phys. Lett. **81**, 1949 (2002).
[5] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. B. Varanonuovo, IEEE Trans. Comput. **52**, 403 (2003).
[6] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[7] M. Stipčević and B. Medved Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
[8] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
[9] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
[10] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photo. **4**, 58 (2010).
[11] M. A. Wayne and P. G. Kwiat, Opt. Exp. **18**, 9351 (2010).
[12] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Opt. Exp. **18**, 13029 (2010).
[13] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Exp. **18**, 18763 (2010).
[14] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).
[15] O. Kwon, Y. Cho, and Y. Kim, Appl. Opt **48**, 091774 (2009).
[16] B. Qi, Y. Chi, H. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
[17] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photonics, **197**, 1 (2009).
[18] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).
[19] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2007).
[20] G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis, Phys. Rev. A **77**, 054101 (2008).
[21] W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).
[22] K. Yamamoto, K. Yamamura, K. Sato, T. Ota, H. Suzuki, and S. Ohsuka, IEEE Nuclear Science Symposium Conference Record. **30-102**, 1094 (2006).
[23] P. Eraerds, M. Legré, A. Rochas, H. Zbinden, and N. Gisin, Opt. Express **15**, 14539 (2007).
[24] M. Akiba, K. Tsujino, K. Sato, and M. Sasaki, Opt. Express **17**, 16885 (2009).
[25] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, England, 1997).
[26] NIST Statistical Tests Suite, [http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html].
[27] D. Branning and M. Bermudez, J. Opt. Soc. Am. B **27**, 1594 (2010).