Practical quantum random number generator based on measuring the shot noise of vacuum states

Yong Shen,[1] Liang Tian,[1,2] and Hongxin Zou[1,*]

[1]*Department of Physics, The National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*College of Optoelectronic Science and Engineering, The National University of Defense Technology, Changsha 410073, People's Republic of China*

(Received 30 March 2010; published 16 June 2010)

The shot noise of vacuum states is a kind of quantum noise and is totally random. In this paper a nondeterministic random number generation scheme based on measuring the shot noise of vacuum states is presented and experimentally demonstrated. We use a homodyne detector to measure the shot noise of vacuum states. Considering that the frequency bandwidth of our detector is limited, we derive the optimal sampling rate so that sampling points have the least correlation with each other. We also choose a method to extract random numbers from sampling values, and prove that the influence of classical noise can be avoided with this method so that the detector does not have to be shot-noise limited. The random numbers generated with this scheme have passed ENT and DIEHARD tests.

DOI: 10.1103/PhysRevA.81.063814 PACS number(s): 42.50.Lc, 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Random numbers are essential in a very wide application range, such as statistical sampling [1], computer simulations [2], and cryptography [3]. Pseudorandom numbers, which are generated from a short random seed by employing deterministic algorithms, are widely used in modern digital electronic information systems. Although the pseudorandom number generator (PRNG) has been highly refined in terms of the generation rate and robustness against random tests owing to the development of computer science and technology, it cannot generate an unpredictable truly random number. Distinct from the PRNG, a truly random number generator (TRNG) is based on the physically random processes rather than computational algorithms; therefore, the random numbers generated by a TRNG are unpredictable and truly random.

A TRNG can be divided into two types [4]. Type one is based on the chaotic behavior of classical deterministic systems, while type two is based on the truly probabilistic nature of fundamental quantum processes. Type one can be treated as a projection measurement in a subsystem and its randomness mainly originates from the absence of enough information from the global system. If the global system is known, the output of type one is predictable and no longer random. So type one cannot be totally trusted. However, type two, a quantum random number generator (QRNG), can provide us with true random numbers with proven randomness.

The QRNG has made significant achievement in recent years. The earliest QRNG is based on performing single-photon detections [5]. However, it has a fatal weakness because there is no single-photon source. Even though later this problem is dodged skillfully by proposing a scheme based on weak coherent states [6], the random number generation rate of this scheme is limited to tens of megabits per second by the avalanche photodiode (APD) single-photon detector (SPD), which has a dead time of tens of nanoseconds. In order to enhance the generation rate, a scheme is proposed [4,7] that is based on measuring the phase noise of a single-mode laser. The phase noise used in this scheme is a kind of quantum noise, which is different than the scheme based on a chaotic semiconductor laser [8–10]. However, the electronic noise and the phase noise of the interferometer may influence the randomness of this scheme. There is also another scheme based on the measurement of the shot noise of vacuum states [11]. Moreover, a lot of the imperfections in this scheme, such as the limited bandwidth of the detector and the electronic noise, have not been considered. In fact, these nonideal factors are fatal for the randomness of generated numbers. More recently, a scheme based on entangled quantum particles was also proposed, which does not require any assumptions about the internal workings of the device [12].

In this paper we present an improved practical QRNG scheme based on measuring the shot noise of vacuum states and proving its randomness. The low-frequency noise of the laser is suppressed using the frequency-shift technique. Considering that the bandwidth of our detectors is limited, we derive the relationship between the bandwidth of detectors and the sampling rate so that the sampling points are independent of each other. Also, we use the method proposed in Ref. [7] to extract random numbers and prove that electronic noise has little influence over the randomness of the system. Since the bandwidth of the shot noise is infinite, the random number generation rate in this scheme is just determined by the bandwidth of the homodyne detector.

II. THEORETICAL MODEL

The Wigner function of a vacuum state is [13]

$$W_0(x,p) = \frac{1}{\pi}\exp(-x^2 - p^2). \tag{1}$$

It is obvious that the vacuum state is isotropic in the phase space. So when we use homodyne detection to measure the vacuum noise, without loss of generality, we consider that what we measure is the X quadrature. Since the Wigner function is a quasiprobability distribution, we obtain [13]

$$|\psi_0(x)|^2 = \int_{-\infty}^{\infty} W_0(x,p)dp = \pi^{-1/2}\exp(-x^2), \tag{2}$$

*hxzou@nudt.edu.cn

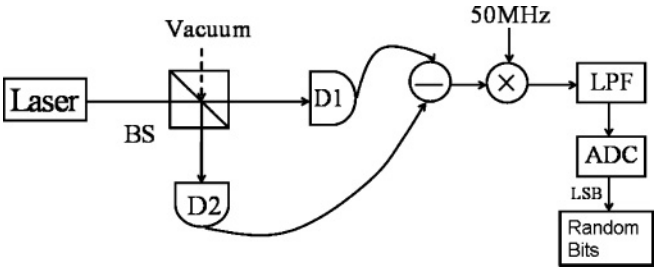

FIG. 1. Schematic of the experiment for QRNG based on measuring the shot noise of vacuum states by using the homodyne detection. Laser, NP Photonics (1550 nm); BS, beam splitter; D1-2, photon detectors; LPF, low-pass filter; ADC, 14-bit analog-digital convertor; LSB, the least significant bit of the digital number.

where $\psi_0(x)$ is the wave function of a vacuum state in the X representation. According to postulates of quantum mechanics, when we measure the X quadrature of vacuum states, the results are totally random and satisfy the Gaussian distribution. So we can extract random bits from the measurement results.

III. EXPERIMENTAL SETUP

The experimental setup of our QRNG is shown in Fig. 1. The laser source is a 1550-nm continuous-wave fiber laser (NP Photonics), which generates the local oscillator (LO). The LO is split by a 50:50 beam splitter and detected by a broadband balanced detector with photodiode G8376-05 by Hamamatsu. As discussed, we use homodyne detection to measure the X quadrature of a vacuum state, and the output of the subtractor is [14]

$$\Delta I = k\alpha_{\mathrm{LO}}\hat{x}, \tag{3}$$

where the constant k contains all the dimensional prefactors and α_{LO} is the displacement of the LO. The effective bandwidth of our detector is over 100 MHz and the signal-to-noise ratio (SNR) is near 6 dB for 10 mW of coherent light.

In our experiment the laser has large relative intensity noise (RIN) in low frequency, which is a kind of classical noise. Since the common-mode rejection ratio of our homodyne detector is limited to 40 dB, the RIN cannot be totally eliminated by the detector. That would induce large classical noise into our measurement. In order to avoid RIN, the output of the subtractor is mixed with a 50-Hz carrier and filtered by a low-pass filter (LPF) whose cut-off frequency is $f_0 = 12$ MHz. So we actually use the 24-Hz sideband frequency spectrum of the shot noise, which is centered at 50 MHz, to generate random numbers. The power spectrums of the filtered signal and the electronic noise of the detector are shown in Fig. 2. We can see that the SNR of the filtere signal is about 6 dB. The spectrum analyzer we used has more noise at low frequency than at high frequency, so the power spectrums are a little oblique. The filtered signal $x(t)$ is sampled and converted to digital data by a data acquisition card (NI PXIe-5122). Then we take the least significant bit of the digital data as the random number.

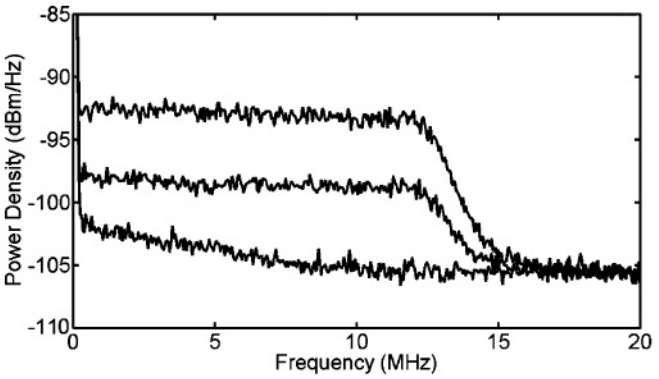

FIG. 2. The lines from top to bottom are the power spectrums of the filtered signal, the electronic noise of the detector, and the electronic noise of the spectrum analyzer, respectively.

IV. COPING WITH NON-IDEAL FACTORS IN EXPERIMENT

A. The realistic filter and the sampling rate

In fact, the sampling rate is not arbitrary for a certain detection bandwidth and it will impact on the the randomness of generated numbers. Then we will find the proper sampling rate for our system. If the filter is ideal, the power spectrum density of the filtered signal $x(t)$ is

$$P_x(\omega) = \begin{cases} \frac{\pi}{\omega_0} & (|\omega| \leqslant \omega_0) \\ 0 & (|\omega| > \omega_0), \end{cases} \tag{4}$$

where $\omega_0 = 2\pi f_0$. $x(t)$ is just the shot noise within ω_0. Since our system is invariant under time translation, which means that $x(t)$ is a stationary random signal, the self-correlation function $R(t,t+\tau)$ of $x(t)$ is determined by the time interval τ and has no relationship with t. So we obtain $R(t,t+\tau) = R(\tau)$. According to the Wiener-Khintchine theorem [15,16] we obtain

$$R(\tau) = \frac{1}{2\pi}\int_{-\infty}^{\infty} P(\omega)e^{j\omega\tau}d\omega = \frac{\sin(\omega_0\tau)}{\omega_0\tau}. \tag{5}$$

The zeros of $R(\tau)$ are $\tau = i/(2f_0)$ $(i = 1,2,3,\ldots)$.

When the sampling period is T_s and the nth sampling value is $x_s(n)$, the self-correlation function of the sampling signal $R_s(n)$ is

$$R_s(n) = E[x_s(0)x_s(n)] = E[x(0)x(nT_s)] = R(nT_s), \tag{6}$$

where $E(x)$ stands for the mean value of a random variable x. Since the sampling points are used to generate random numbers, they should be uncorrelated with each other. $R_s(n)$ must be 0 for all possible n, which means $R(\tau_n) = 0$, where $\tau_n = nT_s$ $(n = 1,2,3,\ldots)$. Therefore, T_s must be one of the zeros of $R(\tau)$, that is, the sampling frequency should satisfy

$$f_s = \frac{1}{T_s} = \frac{2f_0}{j} \quad (j = 1,2,3,\ldots). \tag{7}$$

However, the realistic filter is not ideal, and its falling edge is not as steep as the ideal one. As shown in Fig. 2, we can see

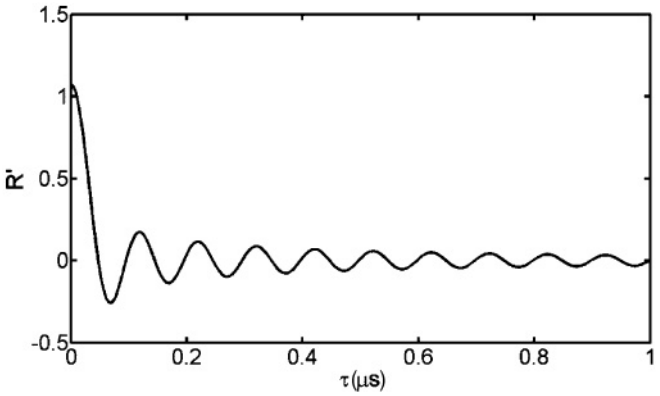

FIG. 3. The relationship between the self-correlation function R' and the time interval τ.

that above 12 MHz, the power intensity of the filtered signal $x'(t)$ attenuates at the rate of 6 dB/MHz. It can be written as

$$P_{x'}(\omega) = \begin{cases} \frac{\pi}{\omega_0} & (|\omega| \leqslant \omega_0) \\ \frac{\pi}{\omega_0} e^{-a(|\omega|-\omega_0)} & (|\omega| > \omega_0), \end{cases} \tag{8}$$

where $a = 1/(2\pi)\ln(10^{0.6})$ MHz^{-1}. $x'(t)$ can be divided into two parts,

$$x'(t) = x(t) + f(t), \tag{9}$$

where $x(t)$ is the shot noise within ω_0 and $f(t)$ is a signal with the frequency component above ω_0 that has not been totally eliminated by the filter. The power spectrum density of $f(t)$ is

$$P_f(\omega) = \begin{cases} 0 & (|\omega| \leqslant \omega_0) \\ P_{x'}(\omega) & (|\omega| > \omega_0). \end{cases} \tag{10}$$

It is obvious that $x(t)$ and $f(t)$ are independent. According to Eq. (8) we obtain the self-correlation function of $x'(t)$,

$$\begin{aligned} R'(\tau) &= \frac{1}{2\pi}\int_{-\infty}^{\infty} P'(\omega)\, e^{j\omega\tau} d\omega \\ &= \frac{\sin(\omega_0\tau)}{\omega_0\tau} + \frac{\tau\sin(\omega_0\tau)}{\omega_0(a^2+\tau^2)} + \frac{a\cos(\omega_0\tau)}{\omega_0(a^2+\tau^2)}, \end{aligned} \tag{11}$$

where the first term is due to $x(t)$ while the second and the third terms are due to $f(t)$. The relationship between the self-correlation function and the time interval τ is shown in Fig. 3. We can see that $R'(\tau)$ has no periodical zeros. So, we cannot find a sampling frequency to make the sampling values $x'_s(n)$ uncorrelated with each other. However, when the sampling frequency satisfies Eq. (7), $x_s(n)$ are uncorrelated with each other, where $x_s(n) = x(nT_s)$. We take $x(t)$ as the signal from which we extract random numbers, while $f(t)$ is treated as noise. In our experiment j is chosen to be 1 and we actually use a sampling frequency of 24 MHz.

B. Electronic noise and the method of extracting random numbers

Besides the imperfection of the filter, there is another noise source in our system. The broadband electrical amplifier used in this system exhibits classical electronic noises $e(t)$. The nth value we actually sample is

$$x''_s(n) = x_s(n) + f_s(n) + e_s(n) = x_s(n) + g_s(n), \tag{12}$$

where $f_s(n)$ and $e_s(n)$ are the values of $f(t)$ and $e(t)$ at sampling points, respectively, and $g_s(n) = e_s(n) + f_s(n)$. Since $x(t)$ is independent of $f(t)$ and $e(t)$, $x_s(n)$ is independent of $g_s(n)$.

The sampling values $\{x''_s(n)\}$ are digitized by a 14-bit analog-to-digital converter (ADC) in the data acquisition card, and the corresponding digital data are $\{x''_d(n)\}$. Since the sampling values are not totally random and do not satisfy uniform distribution [7], the 14-bit digital data cannot be used as random numbers. Therefore, we should extract random numbers from $\{x''_d(n)\}$.

One way is to compare $x''_d(n)$ with 0, the mean value of $x''_d(n)$, and the nth random bit is assigned as either "1" if $x_d(n) > 0$ or "0" if $x''_d(n) < 0$ [4]. However, using this method the result will be influenced by nonideal factors in the system. For example, when $g_s(n) = \epsilon$, the probabilities of "1" and "0" are

$$\begin{aligned} P(1|\epsilon) &= \frac{1}{\sigma\sqrt{2\pi}}\int_{(1/2)Q-\epsilon}^{\infty} e^{-(x^2/2\sigma^2)} dx, \\ P(0|\epsilon) &= \frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{-(1/2)Q-\epsilon} e^{-(x^2/2\sigma^2)} dx, \end{aligned} \tag{13}$$

where σ is the standard deviation of $x_s(n)$ and Q is the resolution of the ADC in volts per step. When $\epsilon \neq 0$, $P(1|\epsilon) \neq P(0|\epsilon)$. Since the electronic noise in a broadband electrical amplifier is a kind of classical noise, it is predictable if information about the global system is sufficient. So the generated bits are also not random.

In this experiment we take $\{x''_l(n)\}$, the LSB of $\{x''_d(n)\}$, as the original random bits, and the influence caused by those nonideal factors can be avoided, as shown in the following.

The shot noise $x_s(n)$ can be written as

$$x_s(n) = x_d(n)Q + \delta_n, \tag{14}$$

where $x_d(n)$ is the analog-to-digital conversion result of $x_s(n)$ and δ_n is the quantization error which satisfies $|\delta_n| < 1/2Q$. Let $g'_s(n) = g_s(n) + \delta_n$, and $g'_d(n)$ be the analog-to-digital conversion result of $g'_s(n)$. When $x''_d(n)$ is not overflow, we obtain

$$x''_l(n) = x_l(n) \oplus g'_l(n), \tag{15}$$

where $x_l(n)$ is the LSB of $x_d(n)$, $g'_l(n)$ is the LSB of $g'_d(n)$, and $\oplus$ is the operation of XOR. Actually Eq. (15) is just a kind of one-time pad [17], where $\{x_l(n)\}$, $\{g'_l(n)\}$, and $\{x''_l(n)\}$ is corresponding to the key, the plaintext, and the ciphertext, respectively. So it has the "perfect secrecy," providing that (i) $x_l(n)$ and $g'_l(n)$ are independent, and (ii) $x_l(n)$ are random [18]. Perfect secrecy means that for a given N-bit train $\{g'_l(n)\}$, the probability that $\{x''_l\}$ be any N-bit train is always 2^{-N}, that is, $\{x''_l(n)\}$ is random. In our experiment the two conditions are satisfied, as proven in the following.

(i) Since $x_s(n)$ is independent with $f_s(n)$ and $e_s(n)$, $x_d(n)$ is independent with $g_d(n)$. Besides, the probability distribution of δ_n knowing $x_d(n)$ is

$$P(\delta_n|x_d(n)) = \begin{cases} \frac{1}{A}\exp\left(-\frac{[x_d(n)Q+\delta_n]^2}{2\sigma^2}\right) & \left(|\delta_n| \leqslant \frac{1}{2}Q\right) \\ 0 & \left(|\delta_n| > \frac{1}{2}Q\right), \end{cases} \tag{16}$$

where $A = \int_{-0.5Q}^{0.5Q} \exp(-\frac{[x_d(n)Q+\delta_n]^2}{2\sigma^2})d\delta_n$. Since $\sigma \approx 1000Q \gg Q$ in our experiment, δ_n is nearly uniformly distributed when knowing $x_d(n)$, that is, δ_n is independent with $x_d(n)$, so we obtain that $x_d(n)$ is independent with $g'_d(n)$. Therefore, $x_l(n)$ is independent with $g'_l(n)$.

(ii) Since $\{x_s(n)\}$ are Gaussian-distributed random numbers and independent with each other, $\{x_l(n)\}$ are also independent with each other. If the probabilities $P(\text{odd})$ that $x_l(n) = 1$ and $P(\text{even})$ that $x_l(n) = 0$ are both 0.5, then $\{x_l(n)\}$ are random. However, in practice the probability $P(\text{odd})$ and $P(\text{even})$ are not perfectly equal and show a small bias δ, that is, $P(\text{even}) = 0.5 + \delta$ and $P(\text{odd}) = 0.5 - \delta$. Since $x_s(n)$ is a Gaussian-distributed random number with a mean of 0, it is obvious that $P(\pm i) > P(\pm(i+1))$, where $P(i)$ is the probability that $x_d(n) = i$ and $i = 0,1,2,\ldots$. So we obtain

$$P(\text{even}) - P(0) < P(\text{odd}) < P(\text{even}) + P(0), \tag{17}$$

that is, $|\delta| < 1/2P(0) = 1/2\text{erf}(Q/2\sqrt{2}\sigma) \approx 2 \times 10^{-4}$, where erf is the error function.

In order to further improve the randomness, we perform a bitwise XOR operation between two trains of random number $\{x''_{l1}(n)\}$ and $\{x''_{l2}(n)\}$ and get a train $\{x''_{l3}(n)\}$ [19,20], which is

$$x''_{l3}(n) = x''_{l1}(n) \oplus x''_{l2}(n) = x_{l3}(n) \oplus g'_{l3}(n), \tag{18}$$

where $x_{l3}(n) = x_{l1}(n) \oplus x_{l2}(n)$ and $g'_{l3}(n) = g'_{l1}(n) \oplus g'_{l2}(n)$. When this method is used, the random number generation rate is actually 12 MHz. With this method the bias in $x_{l3}(n)$ is diminished to $|2\delta^2|$ [7], which is less than 1×10^{-7}. Therefore, $x_{l3}(n)$ can be treated as random.

The two conditions mentioned are both satisfied, so $x''_{l3}(n)$, the numbers generated by our QRNG, are truly random.

It should be noted that we cannot decrease δ by choosing a σ as large as possible, since when $x''_d(n)$ is overflow, Eq. (15) does not hold. Therefore, σ cannot be too large. In our experiment, the probability that $x''_d(n)$ is overflow is

$$P(\text{overflow}) = \text{erfc}\left(\frac{\left(2^{13} - \frac{1}{2}\right)Q}{\sqrt{2}\sigma''}\right) \approx 1 \times 10^{-13}, \tag{19}$$

where $\sigma'' \approx 1100Q > \sigma$ is the standard deviation of $x''_s(n)$ and erfc is the complementary error function. The probability is so small as to be ignored.

V. CONCLUSION

We record a bit file of 1×10^9 bits for random test using two standard batteries, ENT [21] and DIEHARD [22], to evaluate the performance of our QRNG, and the corresponding test results are shown in Tables I and II. It shows that the random numbers generated by our QRNG can pass the two tests.

TABLE I. Results of the ENT test suite for a 10^9-bit sequence.

Entropy = 1.000 000 bit per bit
(the optimum compression would reduce the bit file by 0%)
χ^2 distribution is 0.38
(randomly would exceed this value by 53.73% of the times)
Arithmetic mean value of data bits is 0.5000 (0.5 = random)
Monte Carlo value for π is 3.141 529 406 (error 0.00%)
Serial correlation coefficient is −0.000 021
(totally uncorrelated = 0.0)

In this paper we present a random number generation scheme based on measuring the shot noise of vacuum states. Several nonideal factors in this scheme have been taken into account, such as the limited bandwidth of the detector, the imperfection of the LPF, and the electronic noise in the circuit. By choosing a suitable sampling frequency and using the LSB of the sampling data as random numbers, the generated numbers are proven to be truly random and can pass ENT and DIEHARD tests even though those nonideal factors exist. The final generation rate is 12 Mbits/s, which is only limited by the bandwidth of the LPF and the detector. Since electronic noise will not influence the randomness of the numbers generated, the detector does not need to be shot noise limited. That will significantly reduce the difficulty of the experiment and the generation rate can be easily enhanced up to gigahertz by using a broadband homodyne detector.

TABLE II. Results of the DIEHARD statistical test suite for a 10^9-bit sequence. For the cases of multiple p-values, a Kolmogorov-Smirnov (KS) test is used to obtain a final p-value, which measures the uniformity of the multiple p-values. Overlapping-Pairs-Sparse-Occupancy (OPSO) Overlapping-Quadruples-Sparse-Occupancy (OQSO). The test is considered successful if all final p-values satisfy $0.01 \leqslant p\text{-values} \leqslant 0.99$.

Statistical test	P-value	Result
Birthday spacings	0.028 131 (KS)	Success
Overlapping permutations	0.878 165	Success
Ranks of 31 × 31 matrices	0.401 160	Success
Ranks of 32 × 32 matrices	0.535 883	Success
Ranks of 6 × 8 matrices	0.081 696 (KS)	Success
Monkey tests on 20-bit words	0.366 845 (KS)	Success
Monkey test OPSO	0.839 116 (KS)	Success
Monkey test OQSO	0.380 140 (KS)	Success
Monkey test DNA	0.101 756 (KS)	Success
Count 1's in stream of bytes	0.492 151	Success
Count 1's in specific bytes	0.275 160 (KS)	Success
Parking lot test	0.802 237 (KS)	Success
Minimum distance test	0.869 451 (KS)	Success
Random spheres test	0.530 595 (KS)	Success
Squeeze test	0.836 490 (KS)	Success
Overlapping sums test	0.091 417 (KS)	Success
Runs test (up)	0.675 106	Success
Runs test (down)	0.435 543	Success
Craps test (number of wins)	0.108 638	Success
Craps test (number of throws per game)	0.434 041	Success

ACKNOWLEDGMENTS

The authors thank Hong Guo's group for useful discussions. The work is supported by the key project of Preparatory Research Foundation of the National University of Defense Technology (Grant No. JC08-02-01) and National Natural Science Foundation of China (Grant No. 10904174).

[1] S. L. Lohr, *Sampling: Design and Analysis* (Duxbury Press, Florence, 1999).
[2] N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).
[3] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996).
[4] B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
[5] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[6] W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).
[7] H. Guo, Wenzhuo Tang, Y. Liu, and W. Wei, e-print arXiv:0908.2893v3 [quant-ph].
[8] A. Uchida *et al.*, Nat. Phot. **2**, 728 (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. Phot. **4**, 58 (2009).
[11] A. Trifonov and H. Vig, US Patent No. 7,284,024 (16 October 2007).
[12] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[13] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997).
[14] M. J. Collett, R. Loudon, and C. W. Gardiner, J. Mod. Opt. **34**, 881 (1987).
[15] N. Wiener, Acta Math. **55**, 117 (1930).
[16] A. Khintchine, Math. Ann. **109**, 604 (1934).
[17] G. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).
[18] C. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[19] B. Barak, R. Shaltiel, and E. Tromer, in *Cryptographic Hardware and Embedded Systems-CHES 2003*, edited by C. D. Walter, K. Ko, and C. Paar (Springer-Verlag, Berlin, 2003), pp. 166–180.
[20] M. Epstein, L. Hars, R. Krasinski, M. Rosner, and H. Zheng, *Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts*, Lecture Notes in Computer Science, Vol. 2779 (Springer-Verlag, Berlin, 2003), p. 152.
[21] J. Walker [http://www.fourmilab.ch/random/].
[22] G. Marsaglia, DIEHARD: A Battery of Tests of Randomness [http://www.stat.fsu.edu/pub/diehard/], 1995.