Iraqi J. Laser, Part A, Vol.12, pp. 1-5 (2013)

IRAQI JOURNAL OF LASER

Random Number Generation for Quantum Key Distribution Systems Based on Shot-Noise Fluctuations in a P-I-N Photodiode

Shelan K. Tawfeeq

Institute of Laser for Postgraduate Studies, University of Baghdad, Baghdad, Iraq

(Received 19 March 2013; accepted 7 April 2013)

Abstract: A simple setup of random number generator is proposed. The random number generation is based on the shot-noise fluctuations in a p-i-n photodiode. These fluctuations that are defined as shot noise are based on a stationary random process whose statistical properties reflect Poisson statistics associated with photon streams. It has its origin in the quantum nature of light and it is related to vacuum fluctuations. Two photodiodes were used and their shot noise fluctuations were subtracted. The difference was applied to a comparator to obtain the random sequence.

Introduction

Random numbers are now needed in broad spectrum of applications. These applications range from computational methods needed in simulations and programming like Monte Carlo simulation to generation of encryption codes for cryptography. Also these random numbers can be used in commercial applications like lottery games.

Many methods are used for random number generation. Mainly these methods are based on either simple mathematical techniques which give pseudo random numbers or physical sources that give truly random numbers. Using pseudo random numbers or truly random numbers depends on the application. Pseudo random numbers are deterministic and periodic and are not sufficient for recent applications of quantum cryptography where unconditional security is required. To achieve unconditional security which is based on laws of quantum physics true random numbers are needed. In these applications that use quantum cryptography true random numbers are essential for random bases orientation change. The latter means random change for photon polarization in quantum key distribution based on BB84 protocol and random change in analyzers orientation in entanglement quantum key distribution for Bell's inequality tests.

There are many physical processes that can give unpredictable random phenomena such as beta-particle emission from radioactive materials, the random photon emission period from trapped ions, the random spatial distribution of laser photons, the random transmission or reflection of photons at 50/50 beam splitter , shot-noise fluctuations in an electronic circuit thermal noise in resistors, frequency jitter of electronic oscillators, photon emission noise [1], and vacuum state [2]. Other sources for true random number generation depend on measuring phase noise of a single-mode laser [3] or dark pulses thermally generated in single photon avalanche photodiodes operating in the Geiger mode [4].

Most of these sources for random numbers generation have not been widely used due to their high cost, complexity, instability, impracticality, low bit generation rate,

precautions for those using radioactive materials and sensitivity to mechanical alignment and unequal detectors quantum efficiency for those using 50/50 beam splitters and single-photon detectors [2].

In this paper a simple low cost random number generator is presented. The physical concept is based on a physical random phenomenon, shot noise. The shot noise is generated in two p-i-n photodiodes as a result of equally dividing the optical power emitted from a CW semiconductor laser source. The photocurrent fluctuations, shot noise, generated at the p-i-n photodiodes are subtracted and the result is compared to a threshold level to generate a sequence of zeros and ones [5].

Shot Noise Theory

Shot noise was first studied by Schottky in 1918. He predicted that a vacuum tube would have two intrinsic sources of time-dependent current fluctuations. Noise from the thermal agitation of electrons (thermal noise) and noise from the discreteness of the electrical charge (shot noise) [2,6].

Thermal noise has an electrical power of $4kT\Delta f$which is independent on f, white noise. Here, *k* is Boltzmann's constant, *T* is the temperature and Δf is the effective receiver noise bandwidth [7].

This noise power can directly be measured by the amount of heat that is dissipated in a cold reservoir. Alternatively, voltage fluctuations themselves can also be measured. Their mean squared value equals to $4kTR\Delta f$ where *R* is the resistor value [7].

Shot noise is an electric current that consists of a stream of electrons that are generated at random times. Even when a constant power is incident on a photodetector, photons are absorbed and electron–hole pairs are generated at random time intervals. Current can be written in the form [8],

$$I(t) = \sum_{n=1}^{N_e} q\,h_c(t - t_n) \equiv \bar{I} + i_s(t) \quad (1)$$

where,

q is the magnitude of the electron charge

$t_n$is the arrival time of the n_{th} photon

$N_e$is the total number of electrons generated over a fixed time interval T_d

$h_c(t)$ is the response function which governs the shape of the current pulse produced by each absorbed photon. It is normalized such that

$$\int_0^{Td} h_c(t)dt = 1 \quad (2)$$

$h_c(t)$ behaves like a delta function for most photodetectors because the duration of each current pulse is much shorter than T_d [8]

The average current $\bar{I}$ can be calculated as [9],

$$\bar{I} = \sum_n q\langle h_c(t - t_n\rangle = \sum_n \frac{q}{T_d}\int_0^{T_d} h_c\,(t - t_n)dt = q \equiv qR_e \quad (3)$$

where,

$dt/T_d$is the probability of a photon being absorbed in the time interval dt

$R_e = N_e/T_d$ represents the average rate of electron generation,

$R_e = \eta R_{ph}$ whereη is photodectector's quantum efficiency and R_{ph} is the average rate of photon arrival related to the incident power as $R_{ph} = P_{in}/h\upsilon_o$.

This leads to the relation $\bar{I} = R_d P_{in}$, with $R_d = \eta q/h\upsilon_o$ is the responsivity of the photodetector and $h\upsilon_o$ is the photon energy.

The fluctuating part of the current, $i_s(t) = I(t) - \bar{I}$, is responsible for the shot noise.

The average value for this current vanishes but it has a finite variance. The fluctuating part which is defined as shot noise is a stationary random process whose statistical properties reflects Poisson statistics associated with photon streams [10].

Practically, i_s(t) follows Gaussian statistics whenever the number of photons involved is not too small [11].

Shot noise is not generated at the receiver, it has its origin in the quantum nature of light and it is related to vacuum fluctuations. This means that shot noise is a manifestation of the intrinsic quantum nature of light and it sets the minimum noise level for any photodetector [11].

From Equation 1, the autocorrelation function for $i_s(t)$ can be calculated as,

$$\langle i_s(t)i_s(t+\tau)\rangle = q^2\sum_m\sum_n|\langle h_c(t - t_m)\,h_c(t - t_n + \tau)\rangle - \langle h_c(t - t_m)h_c(t - t_n + \tau)\rangle| \quad (4)$$

As the arrival times of photons are uncorrelated, only the $m = n$ terms contribute in the double sum, assuming that the incident optical signal is coherent [11].
In approximating $h_c(t)$ with a delta function, the autocorrelation function can be written as [9],

$$\langle i_s(t) i_s(t+\tau)\rangle = \int_{-\infty}^{\infty} S_s(t) \exp(2\pi i f \tau)\, df \quad (5)$$

where,

$S_s(f) = q\bar{I}$ is the spectral density of shot noise

Equation (5) represents an example of the Wiener–Khintchine theorem, which is applicable to any stationary stochastic process.
The spectral density of shot noise is frequency - independent and is a two-sided spectral density as negative frequencies are included in Equation (6) [9].
If only positive frequencies are considered, the one –sided spectral density becomes $2qI_p$.
The noise variance, σ_s^2 , is obtained by [9],

$$\sigma_s^2 = \langle i_s^2(t)\rangle = 2qI_p\Delta f \quad (6)$$

The effective receiver noise bandwidth Δf depends on the receiver's design. It corresponds to the intrinsic photodetector's bandwidth if fluctuations in the photocurrent is going to be measured. If dark current is considered, it will generate shot noise too. The noise variance will be equal to [6],

$$\sigma_s^2 = \langle i_s^2(t)\rangle = 2q(I_p + I_d)\Delta f \quad (7)$$

Shot noise is a superposition of impulses occurring at random times. For impulses with same shapes, $F(t)$, then,

$$I(t) = \sum_i F(t - t_i) \quad (8)$$

The impulse shapes can be randomly chosen, $F(a, t)$, depending on a parameter a. This means that $I(t)$ may be written as,

$$I(t) = \sum_i F(a_i, t - t_i) \quad (9)$$

The parameters a_i are chosen independently from a common distribution. The times t_i form a Poisson sequence with rate n impulses per second [11].

Experiment and Results

The suggested setup for generating a sequence of random numbers is shown in Figure 1. Optiwave 9.0 software was used to analyze our proposed setup. The setup consists of a CW semiconductor laser source, a beam splitter, two identical p-i-n photodiodes, a difference amplifier and a comparator. The setup was tested for different values of the output optical power of the CW laser source.

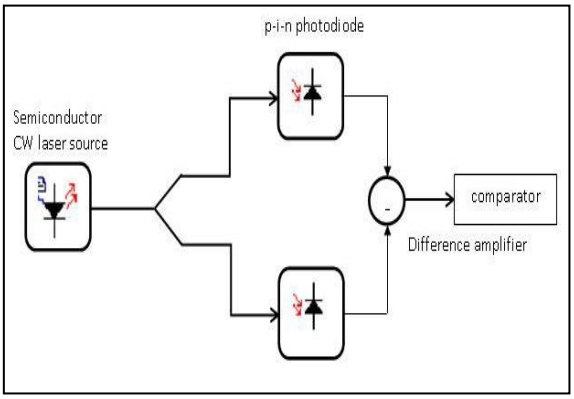

Fig.1: The circuit block diagram

Changing the values of the output power of the CW laser source gives different values for shot noise that is generated in the p-i-n photodiodes. As there is a 50/50 beam splitter this means that the optical power from the CW laser source is divided equally for each p-i-n photodiode. The optical power received at each p-i-n photodiode creates a photocurrent plus a fluctuation current which is defined as the shot noise. As discussed, this shot noise will be randomly generated and will not be equal for each p-i-n photodiode. The output of these p-i-n photodiodes, which are electrical signals now, are both applied to a difference amplifier in order to cancel the photocurrents that is generated as a result of detecting the optical power emitted from the CW laser source by subtracting them. As far as a 50/50 beam splitter is used the difference amplifier should give zero current. But a random value for the difference in fluctuating currents will be obtained because they are not equal and the result of subtraction will not be equal to zero. This random difference is applied to a comparator and compared with a reference voltage of 0 V.A logic "1" is decided if the output of the

difference amplifier is larger than 0 V and a logic "0" is decided when the output of the difference amplifier is less than 0 V. The data obtained was stored in a file to check the randomness. A very simple test for randomness can be applied to test the percentage of "0"s and "1"s in the data obtained. To achieve randomness, equal percentage (50%) for "0"s and "1"s should be obtained. The number of zeros or ones will change with different values of the CW laser output power. This happens due to the fact that the value of the shot noise depends on the value of the optical signal detected by the p-i-n photodiode. The CW laser output power was changed from (0) dBm to (-60) dBm. Best results were obtained, i.e., at output power equals to (-20) dBm at which the number of zeros and ones generated were approximately equal, 50%. A MATLAB program was written to check the sequence and check the number of zeros and ones in the sequence. The sequence saved was tested for randomness by the ENT program that computes the entropy, chi square, arithmetic mean, Monte Carlo estimation of$\pi$and the serial correlation coefficient. The results were as follows, Entropy = 0.988115 bits per byte. Chi square distribution for 257 samples = 0.15, and randomly would exceed this value less than 95.8% of the times. Arithmetic mean value of data bytes = 124.2179 (127.5 = random). Monte Carlo value for Pi is 3.141232. Serial correlation coefficient =0.0000037225 (totally uncorrelated = 0.0). Figures 2 and 3 show the semiconductor CW laser diode output power and output spectrum respectively. Figures 4-6 show the waveforms for the p-i-n photodiodes signal plus shot noise, the output of the difference amplifier and the random bits sequence obtained at the comparator output.

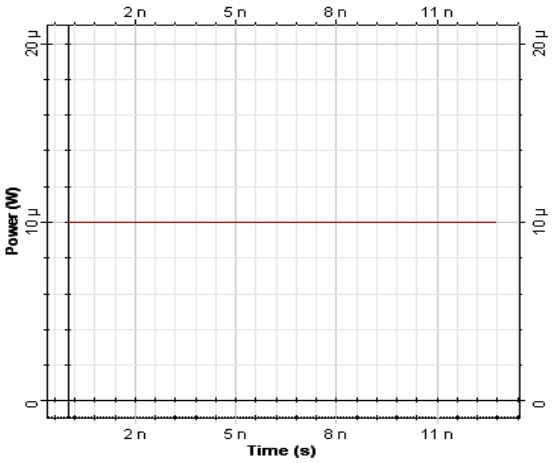

Fig.(2): Semiconductor CW laser diode output power

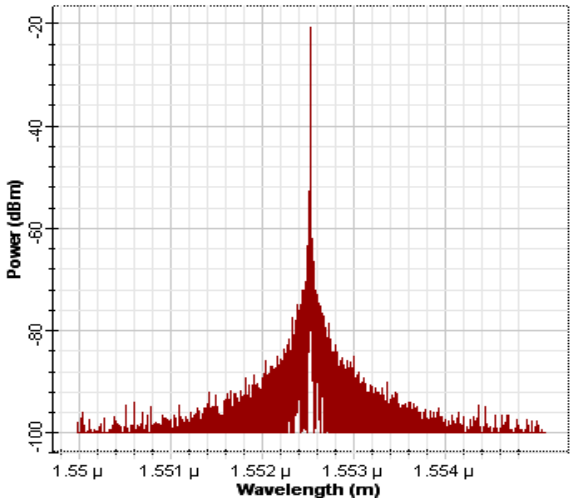

Fig. (3): Semiconductor CW laser diode output spectrum

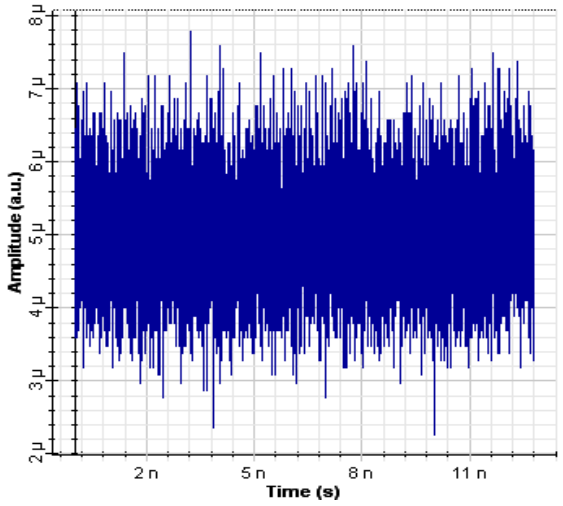

Fig. (4): p-i-n-1 photodiode output signal plus shot noise

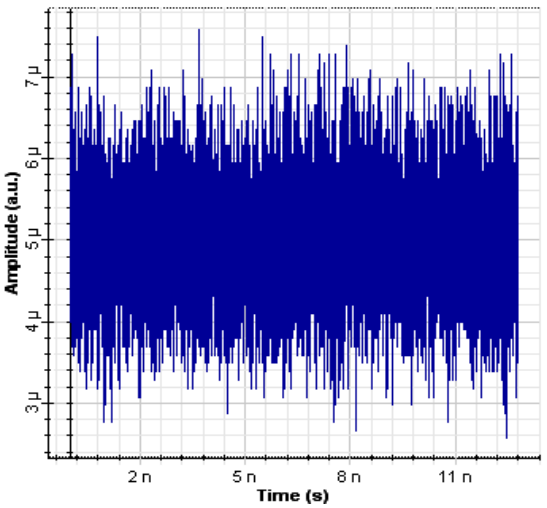

Fig. (5):p-i-n-2 photodiode output signal plus shot noise

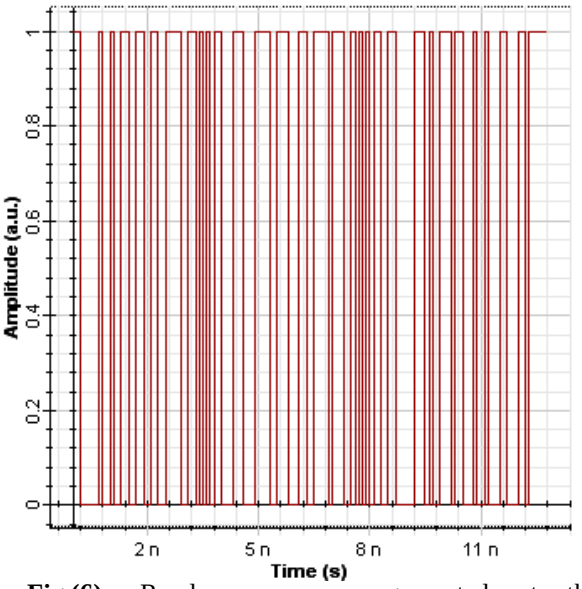

Fig.(6): Random sequence generated at the comparator output

Conclusions

A random number generation based on the shot-noise fluctuations in p-i-n photodiode have been built and checked. By using the ENT program for randomness test, results showed that randomness was at very acceptable level.

References

[1] H. Q. Ma, Y. Xie, and L. A. Wu, "Random number generation based on the time of arrival of single photons", J. Applied Optics, **44,** 7760-7763 (2005)**.**

[2] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector", Physical Review A, **83**, 023820 (2011)

[3] 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" Optics Letters, **35**, 312-314 (2010).

[4] S. K. Tawfeeq,"A random number generator based on single-photon avalanche photodiode dark counts", IEEE J. Lightwave Technology, **27**, 5665- 5667 (2009).

[5] C. S. Petrie and J. A. Connelly," The sampling of noise for random number generation",0-7803-5471 -1999 IEEE, VI-26 – VI-29.

[6] G. P. Agrawal, Fiber-Optic communication System, 4th. Ed. John –Wiley & Sons, Hoboken, New Jersey,2010.

[7] C. Beenaker, Christian Schrödinger, "Quantum shot noise" , physics Today, 2013.

[8] H. A. Haus, Electromagnetic noise and QuamtumOptics Measurements, Springer, New York, 2000.

[9] G.P. Agrawal, LightwaveTechnology, John –Wiley & Sons, Hoboken, New Jersey, 2005.

[10] B. E. A. Saleh and M. Teich, Fundamentals of Photonics, Wiley, New York, 1991.

[11]L. Mandel and E. Wolf, Coherence and Quantum Optics, Cambridge University Press, New York, 1995.

[12] E. N. Gilbert and H. O. Pollak, "Amplitude distribution of shot noise",The Bell system Technical Journal. 333-350 (1960).

توليد عدد عشوائي لمنظومات توزيع المفتاح الكمي بالأعتماد على تقلبات الضوضاء الطلقية في كواشف p-i-n

شيلان خسرو توفيق

معهد الليزر للدراسات العليا ، جامعة بغداد ، بغداد ، العراق

الخلاصة:تم اقتراح اعداد بسيط لمولد اعداد عشوائية. توليد الأعداد العشوائية يستند على تقلبات الضوضاء الطلقية في كاشف من نوع p-i-n. هذه التقلبات و التي تعرف بالضوضاء الطلقية هي عملية عشوائية ثابتة مع الزمن و التي لها صفات احصائية تعكس احصائيات بواسون المرافقة مع تيارات الفوتون. هذه التقلبات مصدرها في الطبيعة الكمية للضوء و لها علاقة بتقلبات الفراغ.تم استخدام كاشفين و تم طرح تقلبات الضوضاء الطلقية لهما . الفرق تم ادخاله الى مقارن للحصول على السلسلة العشوائية. اختبار النتائج باستخدام برنامج ال ENT لأختبارات العشوائية بين بان العشوائية كانت بمستويات مقبولة.