Journal of Engineering and Applied Sciences 13 (3): 629-633, 2018
ISSN: 1816-949X

Quantum Random Bits Generator based on Phase Noise of Laser

[1]F. Alaa Kadhim and [2]Hakeem Imad Mhaibes
[1]Department of Computer Science, University of Technology, Baghdad, Iraq
[2]Computer Center, Kut Technical Institute, Middle Technical University, Baghdad, Iraq

Abstract: Random numbers are essential part in many areas such as statistic, lottery, gaming, marketing, computer simulation and cryptography. Therefore, there are numbers of random number generators have been proposed, most of them are not truly random. Exploiting the nondeterministic and stochastic quantum mechanics used to generate true random numbers. In this study, we propose a Quantum Random Numbers Generator (QRNG) based on a combination of different quantum effects of light. The proposed QRNG design splits the laser beam into two beams, each of which has a different intensity of quantum phase by using polarization technique. These intensities have independent phases. These phases translated into random amplitude variations using the interference of light of these two beams. We take advantage of this output phenomenon to produce true random number. The variation of these amplitudes are following Gaussian distribution of random values that are symmetric to a mean of zero. The results followed by post processing to maximize the randomness using min-entropy evaluation and optimized using Toeplitz random extractor which is theoretically provable random extractor. These results tested using NIST (National Institute of Standards and Technology) test suite for random numbers which pass all 16 tests successfully.

Key words: Quantum mechanics, QRNG, Gaussian distribution, Toeplitz random extractor, min-entropy, National Institute of Standards and Technology

INTRODUCTION

Random numbers generation is essential part in various areas like statistic, lottery, gaming, marketing, computer simulation and cryptography (Meteopolis and Ulam, 1949). Modern cryptography is very sensitive to the properties of random numbers (Schneier and Sutherland, 1995) and make a true random number is the most important part in all cryptography protocols (Dorrendrof *et al*., 2009). The well-known Kerckhoffs's principle by Kerckhoffs (1883), says that the security of a cryptography system must reside entirely in the key. So, there are a number of researches of this field have been proposed, most of them are not theoretically provable for security purpose.

Generally, there are two groups of random generator first group based on deterministic algorithms to generate random numbers. The generated numbers from this group are called pseudo random numbers and not truly random that produce high-speed pseudo random with minimum cost, this group are called Pseudo Random Number Generators (PRNGs) (Luby and Luby 1996). Although, this software based generators have a drawback that their generated randomness is not theoretically provable due to their deterministic procedures. This drawback may cause weakness in many applications, especially in cryptography (Bucci *et al*., 2003). Second group is called True Random Number Generator (TRNGs) based on specific physical or hardware devices that measure high entropy stochastic and nondeterministic sources, the values are post processing with specific technique to produce truly random numbers (Zhang *et al*., 2016). TRNG sources can be from noises of thermal (Bucci *et al*., 2003) and noises coming from atmosphere (Holman *et al*., 1997).

The non-deterministic and stochastic quantum mechanics used to generate true random numbers (Gisin *et al*., 2002). Therefore, there are many proposed random number generators based on quantum mechanics. These Quantum Random Number Generators (QRNGs) such as single photon detection (Jennewein *et al*., 2000) an entangled system (Owens *et al*., 2008), coherent states (Ren *et al*., 2011), vacuum fluctuations (Shi *et al*., 2016), phase noise (Qi *et al*., 2010), spin noise (Katsoprinakis *et al*., 2008) and photonic emission (Ren *et al*., 2011).

In this proposed research, we build a QRNG based on a combination of different quantum effects. The semiconductor laser output fields have a random phase of quantum fluctuations due to spontaneous emission (Xu *et al*., 2012), measurement this phases directly is not technologically feasible. The design of proposed QRNG splits the laser beam into two beams using a Beam Splitter (BS). Each of which has a different intensity of quantum

Corresponding Author: F. Alaa Kadhim, Department of Computer Science, University of Technology, Baghdad, Iraq

phases using polarization technique. These intensities have independent phases. The phase variations follow Gaussian random values distribution that are symmetric to a mean of 0. Gaussian distribution or normal distribution is applied in the natural science for representing real values random variables in which their distributions most be unknown (Wegman and Carter, 1981).

The output of a Photo Detector (PD) are voltages which carry many classical noise, therefore; TRNGs cannot produce truly random number directly without post processing (or randomness extraction) (Zhang *et al*., 2016). In experience, the quantum random is mixed with a classical noise which can be controlled and observed by an adversary. The post processing employed to the results in order to distill the classical noises from the true raw data. The results followed by post processing to maximize the randomness using min-entropy evaluation and optimized using Toeplitz random extractor which is theoretically provable random extractor (Henry, 1982). Simplicity of the proposed model shows a robust, low-cost and high speed QRNG.

MATERIALS AND METHODS

Implementation: Figure 1 shows the proposed physical scheme setup, a diode laser used as the quantum phase source. Experiment states that the quantum phase fluctuation is inversely proportional to the output of the laser (Vahala and Yariv, 1983). By operating the laser at a low intensity level, the quantum uncertainty will dominant over noise (Collett, 2005).

To increase the randomness and create different intensities, the polarization technique used to modulate the intensity of a laser beam. The laser beam is linear polarized by a polarizer 45° with respect to fast axis and slow axis of a followed Quarter Wave Plate (QWP). A QWP plate used as a retarder, a device that introduces a phase difference (shift) between waves with elliptical polarization (Loudon, 2000). The output is entering into a Beam Splitter (BS). A BS is used to split the laser beam into two linearly polarized beams with different axes, means that it splits the components of polarized light with 90° (Naruse *et al*., 2015). The choice of each individual photon to go to a specific path is choosing randomly at the BS (Ma *et al*., 2013). At each path, a polarizer employed to modulate the intensity of the laser light. These two polarizer plains are normal to each other. Then, one of resulting beam has minimum intensity of light and other has maximum intensity of light. These intensities have independent phases. These phases translatedinto random amplitude variations using the interference of light for these two beams. The resulting phenomenon of

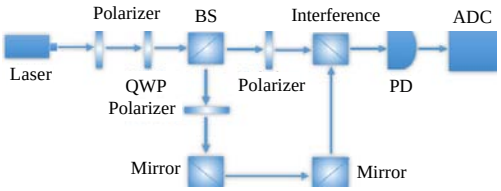

Fig. 1: Physical setup scheme of the propesed model

Fig. 2: General structure of the proposed QRNG

constructive interference and destructive interference used to produce true random numbers. The PD converts the intensity of light into voltages. The distribution of the voltages follow Gaussian distribution X on {0, 1} n that are symmetric on a mean of 0. For all QRNGs, increasing the bits extraction or sampling rate happened by increasing the speed rat of the hardware devices. Usually, sampling is proportional to correlation between the generated bits, higher sampling means higher correlation and hence the digitization have limited diversities (Qi *et al*., 2010). The PD output is then sampled and digitized by 3 bit ADC to generate true random bits. The general structure of the proposed QRNG showing in Fig. 2.

RESULTS AND DISCUSSION

Min-entropy evaluation: In order to extract pure quantum random numbers from the correlation between pure quantum data and classical noises, filtering the raw data is necessary. This done by employing a post-processing which it consists of two stages; first stage is evaluation of min-entropy and the second stage is random extraction. This section discusses the min-entropy; the subsequent section will discussed the random extraction.

Min-entropy evaluation determines the amount of final unbiased random bits that can be extracted from row random values. The equation of min entropy is:

$$H_{\infty}(X) = -\log_2\left(\max_{x\in\{0,1\}n} \Pr[X = x]\right) \quad (1)$$

The values of X follow Gaussian distribution on $\{0, 1\}^n$. The maximal probability of sample x determines the min entropy of values X.

$$P_{max} = \max_{x\in\{0,1\}n} \Pr[X = x] \quad (2)$$

There are three principles to determine min entropy; the value of the standard deviation obtained from

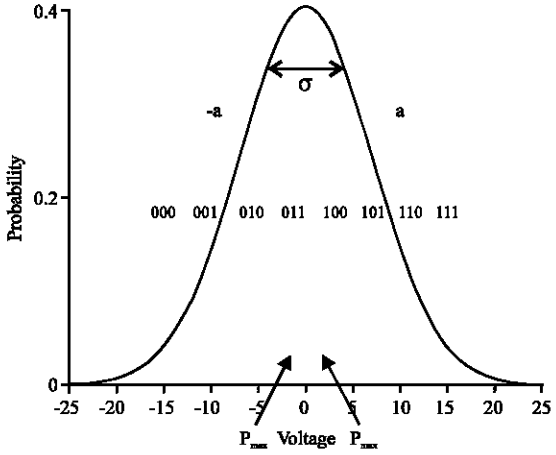

Fig. 3: Min entropy evaluation. The results voltage follow a Gaussian distribution, here mean value (μ = 0) standard deviation (σ = 7) and 3 bits ADC digitization, the width of the sample is represented by (a = 15) and (a = -15). It has 8 bins sample units with P_{max} is equal to ether '011' or '100'

Gaussian distribution, denoted by σ, the range samples obtained from the ADC and the amount of bits obtained from min-entropy. A simple evaluation of the process is showing in Fig. 3.

Gaussian distribution illustrated by the curve corresponding to normal distributions of the values called Bell curve. Gaussian distribution derived by the following Eq. 3:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{(x-\mu)^2}{2\sigma^2}} \quad (3)$$

Mean value is denoted by μ and the variance is denoted by σ^2. Value of μ represents the peak of the bell curve and value of σ^2 measures the normal distribution width. In order to standardize the Gaussian distribution, the values of μ should be 0 and σ is depends on the normal distribution width. In this case, three σ's are used.

The raw values are digitized from ADC using a binary of 3 bits (n = 3) in Eq. 3. These binary bits are corresponding by the voltages detected from the PD of our system. However, it has 8 bins sample units with P_{max} is equal to ether '011' or '100'.

Random extractor and statistical test: The evaluated output by min entropy data cannot pass the statistical test by itself because of the classical noise merged with it. Hence, the perfect random bits extracted from the evaluated row data by implementing a theoretical provable random extractor in this case, using Toeplitz universal

Table 1: Standard 5 tests of randomness

Name of the tests	Status
Frequency	Pass valus 0.160 with freedom degree "1" must be ≤3.84
Runs test	Pass velue t0 = 4.769 with freedom degree "5" must be ≤10.788
	Pass velue t1 = 2.929 with freedom degree "5" must be ≤10.788
Poker	Pass velue 3.520 with freedom degree "5" must be ≤11.1
Serial	Pass velue 4.720 with freedom degree "3" must be ≤7.81
Autocorrelation test	Shift No. 1>-> pass velue 0.495
	Shift No. 2>-> pass velue 0.041
	Shift No. 3>-> pass velue 1.742
	Shift No. 4>-> pass velue 2.042
	Shift No. 5>-> pass velue 0.263
	Shift No. 6>-> pass velue 0.170
	Shift No. 7>-> pass velue 0.269
	Shift No. 8>-> pass velue 0.391
	Shift No. 9>-> pass velue 2.473
	Shift No. 10>-> pass velue 0.044
	With freedom degree "1" must be ≤3.84

$$\begin{bmatrix} t_m & t_{m+1} & \cdots & t_{m+n-1} \\ t_{m-1} & t_m & \cdots & t_{m+n-2} \\ \vdots & t_{m-1} & \ddots & \vdots \\ t_2 & \ddots & \ddots & t_{n+1} \\ t_1 & \cdots & t_{n-1} & t_n \end{bmatrix} \times \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_{n-1} \\ d_n \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_{m-1} \\ r_m \end{bmatrix} \quad (4)$$

hashing extractor as a next step. The general random extractor is a function such as: as is shown in Eq. 4, a binary of size (m×n), Toeplitz hashing matrix is multiplying by the evaluated row data binary bits of size (n), the final outputs are perfect random binary bits from the system of size (m).

Toeplitz hashing matrix constructed by a matrix building seed of a pseudo random bits of size (m+n–1). Toeplitz hashing matrix states that all the numbers from left to right in the same diagonal are same. Here, selected size of m and n are 1024 and 1520, respectively, so, we need a seed number of 2543, pseudo random bits to construct this matrix.

The further results possess the most important desired properties of cryptographic random numbers which are unpredicted and unreproducible. To be confidence, these results are tested and evaluated by two test suite; first by the five basic standard statistical tests of randomness which are successfully passing all the five standard tests (Table 1). Then followed by the 16 NIST tests, random numbers generated by the proposed QRNG successfully pass all the 16 tests (Table 2).

Table 2: The 16 NIST test suite

Name of the tests	Status
Frequency	Pass
Longest runs of ones	Pass
Runs test	Pass
Lempel-Ziv compression	Pass
Discrete fourier transform	Pass
Cumulative sums (reverse and forward)	Pass
Binary matrix rank	Pass
Random excursions	Pass
Random excursions variant	Pass
Frequency within a block, BL = 128	Pass
Approximate entropy, BL = 10	Pass
Linear complexity, BL = 500	Pass
Maurer's, universal statistical, selected blocks = 7, length of blocks = 1280	Pass
Serial, length of the blocks = 16	Pass
Overlapping template matching	Pass
Non-overlapping template matching, template length = 9	Pass

CONCLUSION

In this study, a QRNG proposed based on nondeterministic and stochastic nature of quantum. It is obvious that the introducing of QWP and suitable use of the polarizers can be used to obtained two different quantum phases of noise, the interference of two different intensities of quantum phases of noise and that will make the system behaviors more randomness. This resulting phenomenon used to produce truly random numbers. Min entropy of raw amplitude variations are evaluated and random extraction using security provable Toeplitz universal hashing extractor done to maximize the randomness of the system.

Experimental construction of the QRNG shows low cost and high-speed QRNG. The generated numbers are random, unpredicted and unreproducible. These results passing the NIST 16 tests suites of randomness.

REFERENCES

Bucci, M., L. Germani, R. Luzzi, A. Trifiletti and M. Varanonuovo, 2003. A high speed random number source for cryptographic applications on a smartcard. IEEE. Trans. Comput., 52: 403-409.

Collett, E., 2005. Field Guide to Polarization. Vol. 15, SPIE Publisher, Bellingham, Washington, USA., ISBN:9780819458681, Pages: 134.

Dorrendorf, L., Z. Gutterman and B. Pinkas, 2009. Cryptanalysis of the random number generator of the windows operating system. ACM. Trans. Inf. Syst. Secur. TISSEC., 13: 10:1-10:32.

Gisin, N., G. Ribordy, W. Tittel and H. Zbinden, 2002. Quantum cryptography. Rev. Mod. Phys., 74: 145-195.

Henry, C., 1982. Theory of the linewidth of semiconductor lasers. IEEE. J. Quantum Electron., 18: 259-264.

Holman, W.T., J.A. Connelly and A.B. Dowlatabadi, 1997. An integrated analog/digital random noise source. IEEE. Trans. Circuits Syst. I. Fundam. Theory Appl., 44: 521-528.

Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, 2000. A fast and compact quantum random number generator. Rev. Sci. Instrum., 71: 1675-1680.

Katsoprinakis, G.E., M. Polis, A. Tavernarakis, A.T. Dellis and I.K. Kominis, 2008. Quantum random number generator based on spin noise. Phys. Rev., Vol.77,

Kerckhoffs, A., 1883. La cryptographie militaire. J. Des. Sci. Militaires, 9: 5-83.

Loudon, R., 2000. The Quantum Theory of Light. 3rd Edn., Oxford University Press, New York, USA., ISBN:9780191589782, Pages: 448.

Luby, M.G. and M. Luby, 1996. Pseudorandomness and Cryptographic Applications. Princeton University Press, Princeton, New Jersey, USA., Pages: 237.

Ma, X., F. Xu, H. Xu, X. Tan and B. Qi *et al*., 2013. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. Phys. Rev. A, 87: 1-13.

Metropolis, N. and S. Ulam, 1949. The Monte Carlo method. J. Am. Stat. Assoc., 44: 335-341.

Naruse, M., M. Berthel, A. Drezet, S. Huant and M. Aono *et al*., 2015. Single-photon decision maker. Sci. Rep., 5: 1-9.

Owens, I.J., R.J. Hughes and J.E. Nordholt, 2008. Entangled quantum-key-distribution randomness. Phys. Rev. A, Vol. 78, 10.1103/PhysRevA.78. 022307.

Qi, B., Y.M. Chi, H.K. Lo and L. Qian, 2010. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt. Lett., 35: 312-314.

Ren, M., E. Wu, Y. Liang, Y. Jian and G. Wu *et al*., 2011. Quantum random-number generator based on a photon-number-resolving detector. Phys. Rev. A, Vol. 83, 10.1103/PhysRevA.83.023820.

Schneier, B. and P. Sutherland, 1995. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley & Sons, Hoboken, New Jersey, USA., ISBN:9780471117094, Pages: 792.

Shi, Y., B. Chng and C. Kurtsiefer, 2016. Random numbers from vacuum ?uctuations. Master Thesis, Center for Quantum Technologies, National University of Singapore, Singapore.

Vahala, K. and A. Yariv, 1983. Occupation fluctuation noise: A fundamental source of linewidth broadening in semiconductor lasers. Appl. Phys. Lett., 43: 140-142.

Wegman, M. and J. Carter, 1981. New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci., 22: 265-279.

Xu, F., B. Qi, X. Ma, H. Xu and H. Zheng *et al*., 2012. Ultrafast quantum random number generation based on quantum phase fluctuations. Opt. Express, 20: 12366-12377.

Zhang, X., Y.Q. Nie, H. Liang and J. Zhang, 2016. FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers. Proceedings of the 2016 IEEE-NPSS International Conference on Real Time (RT), June 6-10, 2016, IEEE, Padua, Italy, ISBN:978-1-5090-2014-0, pp: 1-5.