International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2141-2146

A Low-Cost True Random Bits Generator Based on Chaotic System and Light Nature

Dr. Alaa Kadhim F[1] and Hakeem Imad Mhaibes[2]

[1]Assistant Professor, Computer Science Department, University of Technology, Baghdad, Iraq.
E-mail :dralaa_cs@yahoo.com

[2]Computer Center, Kut Technical Institute, Middle Technical University, Baghdad, Iraq.
E-mail :hakeem_emad@yahoo.com

Abstract

Quantum nature of light and chaos theory helped the cryptographic researchers to improve the security of many application systems. They exploit these fields in both cryptographic algorithms and random numbers generation. In this paper, a low cost and simple true random number generator (TRNG) is proposed. The proposed TRNG exploits the behavior of the chaotic system and quantum nature of light. A diode laser operates as a source of light. The chaotic logistic map used to control the intensity power of a diode laser. The resulting laser beam possesses chaotic behaviors, which are unpredicted, highly sensitive to initial states, and random like. In addition, the detected light exhibits the stochastic and non-deterministic quantum nature. These properties make it a perfect source of entropy. Therefore, the proposed TRNG takes the desired properties from both areas. Experiment results and statistical analyses show that the true random numbers generated by a proposed TRNG possess highly properties of randomness, which is a suitable to use in the cryptographic systems.

Keywords: Quantum nature of light, Chaos theory, PWM, TRNG, Statistical Test.

INTRODUCTION

The cryptography keys highly dependent on the characteristics of random numbers [1]. Random numbers are a string of digits ordered in a random manner if one digit knew; it is not possible to predict the upcoming digit [2] [3]. Commonly, all cryptographic systems follow the principle of the Kerckhoffs', it assumes that the design of a cryptographic system publically known, and the security of the system depends entirely on the keys. Therefore, if the adversary knew the specific design, then the clients need only to change the specific key. In this situation, the next key must be random, unpredicted and randomly selected from the key pool [4]. Moreover, the design of a cryptographic system must reside on a perfect random numbers generator (RNG) [5]. Therefore, there are many RNGs have been proposed, most of them are not theoretically provable true random.

In general, there are two classes of RNG, pseudo random number generators (PRNGs) and true random number generators (TRNGs). PRNG is generally based on deterministic algorithms that generate pseudo random numbers from a specific initial seed, the produced random numbers appear to be true random [6], and deterministic with the chaotic dynamic system [7]. While TRNGs operate by specific physical devices to measure the nondeterministic and stochastic sources of nature [8], such as a thermal noise from a semiconductor [9], radioactive decay [10], atmosphere noises [11], single photon detection [12], and quantum phase fluctuations [13].

The proposed TRNG exploits the behavior of chaotic system and properties of light. A semiconductor laser used, which is the most common type of laser as a source of light. The chaotic function used to control the intensity power of the semiconductor laser using pulse width modulation technique (PWM). The resulting laser beam possesses chaotic behavior, which is unpredicted, highly sensitive to initial states, and random like [14]. Moreover, the light exhibits the stochastic and non-deterministic quantum nature [15]. These properties make it a perfect source of entropy. A photo detector (PD) detects the laser beam and converts light intensity into current represented by voltage. These detected randomize voltages are digitizing using 10-bit ADC. The received voltages converted into corresponding integer values. The distribution of these values follow Gaussian distribution of random values. After that, the values converted into binary by tacking least significant bit (LSB) for each 10-bit sample voltage. These bits are the original random bits. It is obvious that the determinism and autocorrelation are increasing when the selected binary bits are increasing from LSB to MSB (select 2-LSB and 3-LSB and so on, up to MSB) [16]. Therefore, the MSB shows more deterministic of chaos properties, while in the LSB the deterministic properties does not exist in the final obtained random bits. This fact improves our work and gives more desired results of randomness. The final output sequences of random bits examined and tested by statistical analysis of random sequence. Experiment results and numerical analysis shows that the true random numbers generated by a proposed TRNG possess highly properties of randomness, which is a suitable to use in the cryptographic systems.

RANDOM NUMBERS GENERATION USING CHAOS THEORY

Chaos is a mathematical branch, which studies the nonlinear dynamical systems. The aspects of these systems are; highly sensitive dependence on initial states, have completely

unpredictable behaviors and cannot effectively be controlled [17]. Cryptographic researchers exploited these properties for designing a random number generator to generate pseudo random numbers. Generally, the standard formula that exhibits very complex chaotic phenomena called logistic map equation. This equation is a simple nonlinear polynomial mapping, was popularized by the biologist Robert May in 1976, the main purpose of it was to describe the growth of biological populations [18].

The logistic map formulated as follow:

$$f(y_i) = ry_i(1 - y_i) \quad (1)$$

This equation is an iterative map, where *y* is the state variable that most accepts values between zero and one. While *r* is the growth rate or control parameter, which could be any value between one and four.

Figure (1), illustrates how *r* parameter controls the behavior of a logistic map with 7 values. If r < 1 then the trajectory (subsequent states) will converge to 0, therefore there is no chaotic behavior. See below picture of different values of r. when r > 3.5 the trajectory never repeat itself, and it gives chaotic behavior, which is unpredictable in long runs (increase the randomness).

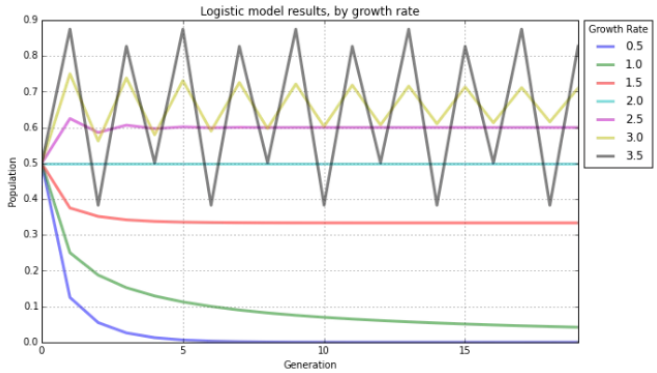

Figure 1: Population from a Logistic map with different growth rates.

When growth rate is close to 4, the system gives full chaotic behavior, See figure (2) which is the bifurcation diagram that shows the dynamic possible long term values of a logistic map. The system is bounded between 0 and 1, and have one steady state at approximately from 1 to 2.9. After increasing *r*, almost from 3.0 to 3.5, the system will have two steady states as shown in figure (2). When *r > 3.6* the system increasing the periodicity and become unpredictable (chaotic behaviors) [17].

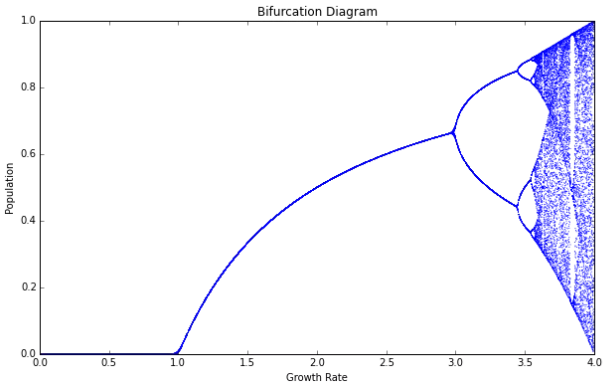

Figure 2: The bifurcation diagram of the Logistic map.

In figure (3), the illustration of sensitivity of a logistic map to an initial condition. It shows how slightly different two initial conditions (0.5, 0.50001) with same growth parameter r=3.99. They start almost at the same position and eventually after 35 generations, the state will have completely unrelated patterns (population).

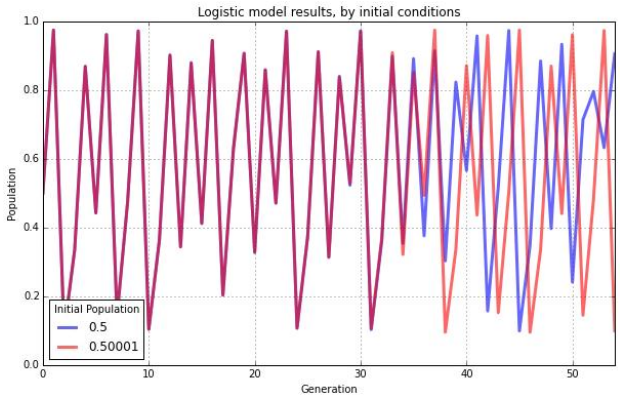

Figure 3: Explains the sensitivity of logistic map to two almost same initial population.

Figure (4); shows the quantitative measurement of Lyapunov exponent in chaotic systems. The positive values represent the chaotic behavior of the dynamic system and the negative values represent the non-chaotic behavior of the dynamic system. The Lyapunov formula is:

$$L = \lim_{n\to\infty} \sum_{i=1}^{n} \ln |f(Y)| \quad (2)$$

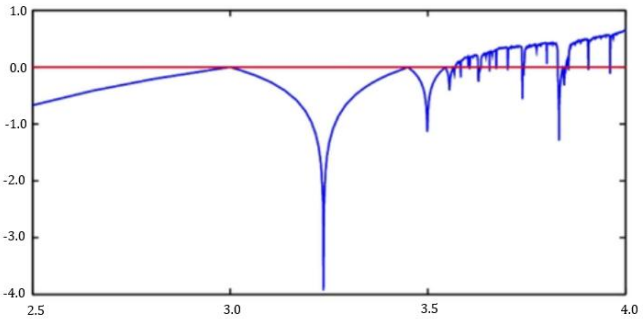

Figure 4: The Lyapunov exponent of the Logistic map.

PULSE WIDTH MODULATION (PWM)

PWM is a powerful modulation technique used to control analog circuits in a wide variety of sophisticated applications through the digital outputs of a microprocessor. An analog circuit is the one whose output is linearly proportional to its input. Digital output is used to control a pulsing signal; these signals are switching between on-time and off-time rapidly at constant frequency [19].

The voltage (current) can be simulated at a high speed, by changing the duration of time the signal is on-time corresponding to duration of time the signal is off-time. The longer time the signal spends in on-time state, the higher power supplied to the load [20]. The time when the signal in on-time state is called pulse width (or duty cycle), which is the inverse of frequency of the period (or waveform). It is possible to generate varying volts by modulating (changing) the pulse width. When the digital signal in on-time state half of the time and in off-time state half of the time, then this digital signal has a duty cycle of 50%. If the percentage of a duty cycle is 75%, this means that the digital signal is 75 % on-time and 25% off-time, and so on. Figure (5); illustrate duty cycle that can be varied between 0 % and 100%.

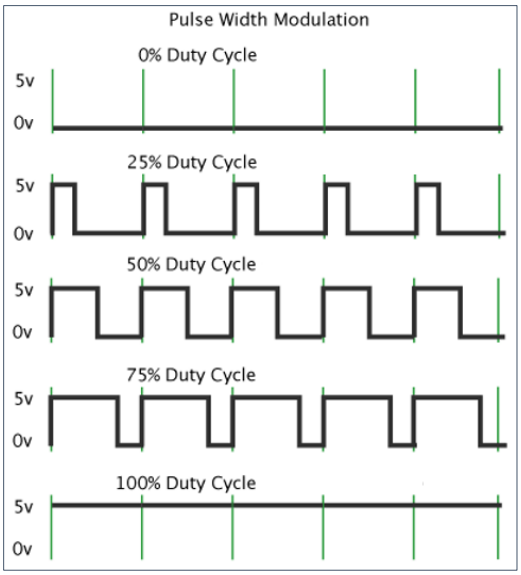

Figure 5: Different duty cycles of PWM.

PWM technique used in the proposed design to feed the semiconductor laser with varying load. The Arduino Microcontroller has a PWM controller. By setting the period in the counter that provides the modulation wave, and with chaotic duty cycles obtained from logistic equation, it is possible to have chaotic simulation in the generated light. Next section describe the proposed models.

EXPERIMENTAL SETUP: SCHEME FOR RANDOM BITS GENERATOR

Figure (6), shows the general scheme of the proposed method. The nonlinear chaotic logistic map initialized with a suitable initial state y_0 and used to generate sequence numbers. These chaotic sequences used to initialize PWM. A PWM technique used in this project to let a diode laser operates chaotically.

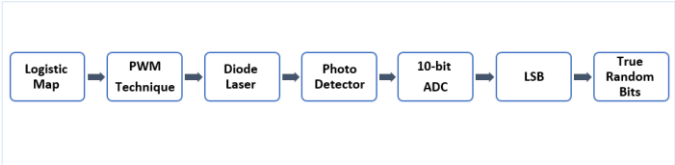

Figure 6: General scheme for true random bits generator.

Using a diode laser has two advantages; it is cheap (cost about 1.5 USD) and convenient. Since the result from logistic map are values between 0 and 1, that make the laser operates with low intensity power level. The resulting laser beam is unpredicted, high sensitive to initial states, and random like. Experiment state that the phase noise of laser is inversely proportional to its power. By operating the laser at a low intensity power level, the quantum uncertainty dominant over noise, therefore the chaotic laser beam exhibits the stochastic and nondeterministic quantum nature [21]. Therefore, these properties make it a perfect source of entropy.

Figure (7) illustrate the experimental setup of the proposed physical TRNG. In this project, an Arduino UNO used as a microcontroller, which is cheap and well-known microcontroller. It has ATMEGA Chip inside that has 16MHz system clock. Arduino also has a PWM controller inside. The PWM controller is a selectable duty cycle. The duty cycle (or pulse width) is the on-time state that is proportional to the period [22].

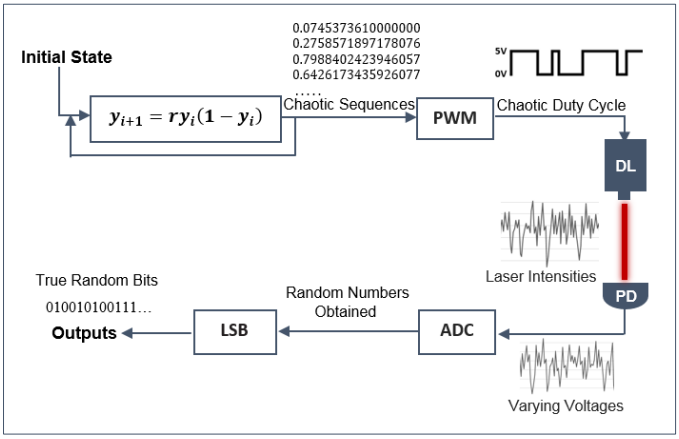

Figure 7: Experimental setup of proposed random bits generation. Logistic map equation no.(1); PWM, Pulse Width Modulation; DL, diode laser; PD, photo detector; ADC, 10-bits analog-to-digital Convertor; LSB, least significant bits.

To operate the PWM, the proposed software must consider three things; the on-chip counter that sets the period for modulating square waves, the on-time in the PWM register (fed by the chaotic numbers), and the specific output pin (diode laser in this case).

The chaotic numbers are used to simulate the on-time (duty cycle) through the PWM's digital output pin, and hence generate

chaotic duty cycles. Each number from a chaotic sequence is converted to a specific on-time state at high speed, this is done programmatically by using Arduino Programming language function analogWrite(pinNum,y_n). This function has two parameters; the First parameter is a selectable output pin and the second parameter is the chaotic numbers obtained from the logistic map that represent the on-time states that have the values between 0 and 255. The output results are the light intensities, which detected and converted into voltages using a PD. Since a laser has intrinsic random nature due the characteristic of light. Although, there are many differences between the amounts of detected intensities that are corresponding to the amounts of laser power at a specific time. Figure (8), illustrate the randomize intensities detected by a PD.

These randomize voltages are Gaussian distributions and digitizing using Arduino 10-bit ADC. In figure (9), the histogram graph represents an estimation of the probability distribution of the detected continues data.

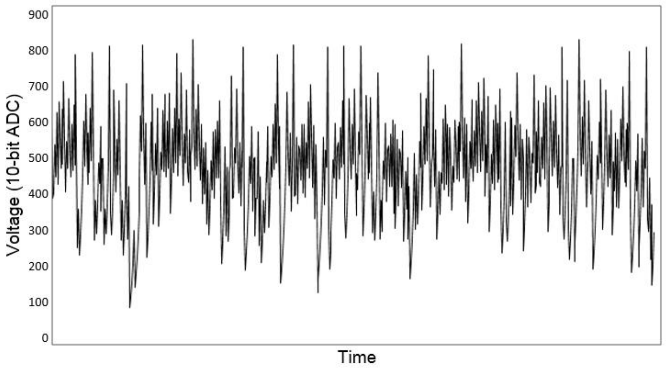

Figure 8: 10-ADC shows the varying voltage detected by LDR.

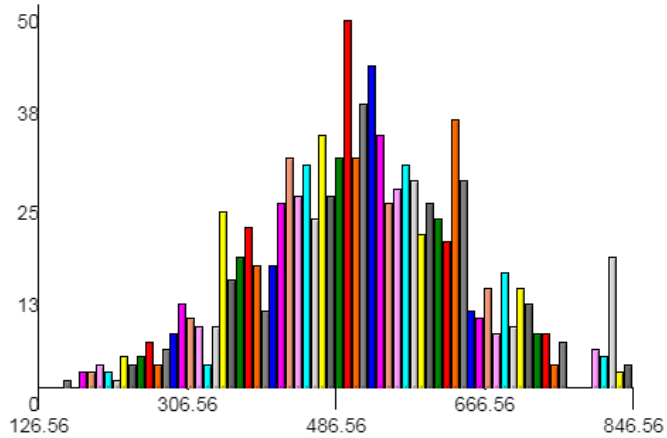

Figure 9: Histogram of the N samples resulting from 10-bit ADC.

The analogRead(pinNum) function reads the intensities from the specified analog pin. This function mapped the received voltages (varying between 0 and 5 volts) into corresponding integer values (varying between 0 and 1023) [23]. These generated numbers converted into binary by tacking 1-LSB of each 10-bit sample voltage. These bits are the original random bits, in another word, take the parity of each 10-bit binary number, and check whether these bits are even or odd. Even value represents 0 and odd value represents 1.

The retaining of bits that selected from the LSB to MSB is proportional to the memory time of the software. The deterministic properties of the chaos theory are lost when the extraction is to take the LSB while the determinism and autocorrelation are increasing when the selected binary bits are increasing from LSB to MSB (tack 2-LSB and 3-LSB and so on, up to MSB) [24]. Therefore, the MSB shows more deterministic of chaos properties, while in the LSB the deterministic properties do not exist in the final obtained random bits. This fact improves our work and gives more desired results of randomness. In this work, we take the LSB only to extract a pure random bit. However, it is possible to select and extract more n-LSB, and this will yield more extraction rate.

STATISTICAL ANALYSIS

To be confidence that the generated binary bits are true random, some special statistical analysis are necessary. Firstly we examined the proposed random bits generator to check whether it produce independent random bits or not using autocorrelation test. Secondly, we examined the final output by statistical tests of randomness. The autocorrelation test applied in time series data, where the data contains a sequence of observations gathered by time. The present of dependency (autocorrelation) between the generated bits implies a weak generator [25]. In this case, the autocorrelation function (ACF) used to determine the underlying patterns of dependencies in the invariant random bits sequence. The true random bits sequence should have values calculated from autocorrelation test is close to zero.

The ACF computed according to the formula:

$$\hat{p}(h) = \frac{\sum_{k=h}^{T}(y_k-\bar{y})(y_{k-h}-\bar{y})}{\sum_{k=1}^{T}(y_k-\bar{y})^2} \quad (3)$$

Where, y_k is the value of random bits sequence at time t, h is the lag order, T is the number of values in the sequence, y_{k-h} is the value of lag-k and finally $\bar{y}$ represents the mean value of full samples. Mean value calculated by the following function.

$$\bar{y} = \frac{\sum_{i=1}^{N} y_i}{N} \quad (4)$$

As an example, N represents the numbers of bits obtained by above proposed generator, in this case N=50000 and lag order is 10. Figure (10) shows the original time series of N values that represents the distributions of 1 and 0 over time. This plot implies that the distributions ratio of 1 and 0 are equal as expected for true random values.

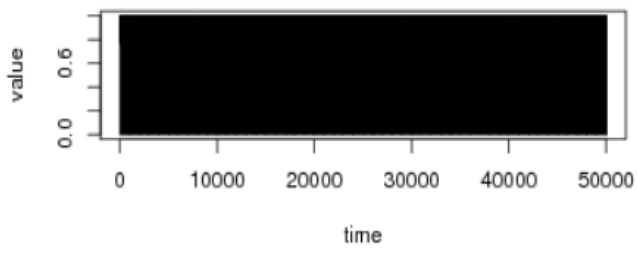

Figure 10: Original time series N/50000

Figure (11) shows the autocorrelation plot (or correlogram) that summarizes the relationships between the final true bits in a time series. At first, the plot starts at 1, because the time is equal to zero at this time and the time is comparing with itself. All values that calculated form ACF should be bounded between -1 and 1.

In order to evaluate the truly random sequences, the autocorrelation test suggests that, the true random sequence must be bounded between tow confidence lines. The upper doted blue line represents the Upper Confidence Level (UCL) and the Lower doted blue line represents the Lower Confidence Level (LCL). If the generated binary sequence is truly random, then the all calculated values of ACF must be between the UCL and LCL. Otherwise the generated binary sequence is not true random (autocorrelation exists within data).

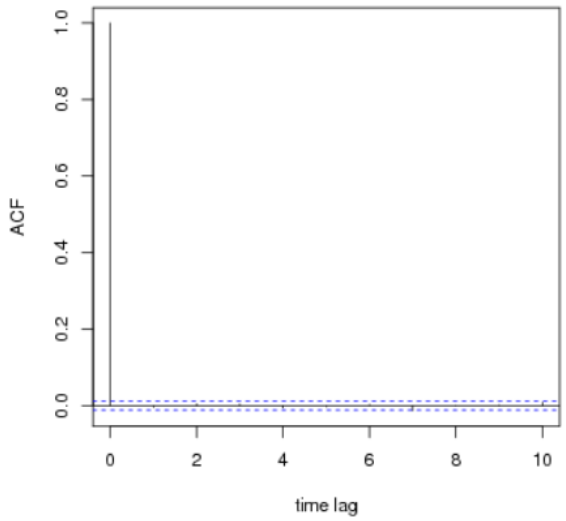

Figure 11: Autocorrelation Test, N/50000.

It is clear that the proposed generator produces true random bits sequence that have all values obtained from ACF calculations close to zero. Table (1), gives the results obtained from autocorrelation test.

Table 1: ACF results.

Autocorrelation Function, N/50000	
Time lag k	ACF(k)
1	-0.003739
2	0.004079
3	0.003699
4	-0.005879
5	-0.00234
6	0.002639
7	-0.013337
8	-0.00036
9	0.00078
10	0.007758

The statistical tests for randomness designed to determine whether a specific given sequence of numbers are random or not. Several test suites are available as the option to analyze the random binary sequences. These suites are the NIST statistical test suits for randomness [25], the DIEHARD statistical test suits for randomness [26], the Donald Knuth's statistical test suits for randomness [27], and the Crypt-XS statistical test suits for randomness [28]. Each one of the previous suite has numbers of different statistical tests, and each test detects specific aspect of randomness. Experiment states that, each suit has redundant of some test, so there is no need to apply all the suites. In this work, the suggested suite is the NIST (National Institute of Standards and Technology) test suite, which include the most independent needed tests that are sufficient for random test.

In NIST Suite, a P-value computed for each test from the binary sequence. A test is success for a given binary sequence if the corresponding P-value is greater than a significance level α. otherwise the test is fail. In this work, $\alpha = 0.01$, the samples = 100, and each sample is 1MBs size. Table (1) shows the result of the generated binary sequence from the proposed generator. Table (2), shows that the results are successfully passed the 16 NIST test suite.

Table 1: NIST test results.

Test name	**P-value**	**Result**
Frequency	0.987100	Success
Longest runs of ones	0.286742	Success
Runs test	0.988500	Success
Lempel-Ziv compression	0.435236	Success
Discrete Fourier transform	0.999734	Success
Cumulative sums	0.993132	Success
Rank	0.665342	Success
Random excursions	0.714166	Success
Random excursions variant	0.920510	Success
Approximate	0.786433	Success
Linear complexity	0.999231	Success
Universal Statistical	1.000000	Success
Rank	0.565011	Success
Serial	0.993445	Success
Overlapping	0.444320	Success
Non-periodic	0.521323	Success

CONCLUSION

The propose generator is a new, simple and low cost TRNG, and the implementations is convenient and compact. The randomness of this physical generator guaranteed by the characteristics of chaos theory and the intrinsic random nature

of the light. By retaining a 1-LSB, the final output binary sequences are highly randomize and the deterministic of the chaos is not exist in the long run. The statistical and theoretical analyses prove that the final outputs are true random and it is applicable in specialized applications.

REFERENCES

[1] Schneier and P. Sutherland, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley, New York, 1995.

[2] Jun B, Kocher P. "The Intel random number generator", Cryptography Research, Inc, White paper prepared for Inter Corp, 1999.

[3] Wang and Yongge, "Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL". Heidelberg: Springer LNCS, 2014.

[4] A. Kerckhoffs, "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[6] M. Luby, "Pseudorandomness and Cryptographic Applications", Princeton Univ Press, 1996.

[7] B. Stoyanov, K. Szczypiorski, and K. Kordov, "Yet Another Pseudorandom Number Generator", arXiv, Int. journal of electronics and telecommunications, vol. 63, no. 2, pp. 195–199, 2017.

[8] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast Physical Random Number Generator Using Amplified Spontaneous Emission," Optics Express, vol. 18, pp. 23584–23597, November 2010.

[9] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A High Speed Random Number Source For Cryptographic Applications On A Smartcard", IEEE Transaction on Computer, 52(4), pp. 403–409, 2003

[10] J. Walker, HotBits: "Genuine Random Numbers Generated by Radioactive Decay", http://www.fourmilab.ch/hotbits, 2002.

[11] W. T. Holman, J. A. Connelly, and A. B. Downlatabadi, "An Integrated Analog/Digital Random Noise Source", IEEE Transaction on Circuits and System I, 44(6), pp. 521–528, 1997.

[12] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. "A fast and compact quantum random number generator". Review of Scientific Instruments 71, 1675, 2000.

[13] Y. Shi, B. Chng, and C. Kurtsiefer "Random numbers from vacuum fluctuations" Center for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore, 2016.

[14] G. Álvarez and S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos", Vol. 16, No. 8, pp. 2129–2151, 2006.

[15] R. Loudon, "The quantum theory of light", 3rd edition, Oxford University Press, New York, NY, 2000.

[16] X. Fang, B. Wetzel, J-M. Merolla and J. M. Dudley, "Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources", IEEE Transactions on Circuits and Systems, Regular Papers, Vol. 61, No. 3, 2014.

[17] Strogatz and Steven, "Nonlinear Dynamics and Chaos", Perseus Publishing, 2000.

[18] Robert M May. "Simple mathematical models with very complicated dynamics". Nature. Vol. 261, 459-467, 1976.

[19] Holmes, D.G., Lipo, T.A, "Pulse Width Modulation for Power Converters, Principles and Practice", 1st edition, Wiley IEEE Press, 2003.

[20] J. Sun, D.M. Mitchell, M.F. Greuel, P.T. Krein and R.M. Bass, "Averaged modeling of PWM converters operating in discontinuous conduction mode", IEEE Transactions on Power Electronics, Vol. 16, Issue: 4, 482 – 492, Jul 2001.

[21] K. Vahala and A. Yariv, "Occupation fluctuation noise: A fundamental source of linewidth broadening in semi-conductor lasers," Appl. Phys. Lett. 43, 140, 1983.

[22] J. Oxer and H. Blemings, "Practical Arduino: Cool Projects for Open Source Hardware", 1st Edition. Apress, 2010.

[23] B. Evans, "Beginning Arduino Programming", 1st. Edition, Apress, 2011.

[24] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh speed random nuber generation based on a chaotic semiconductor laser", Physical Review Letters, vol. 103, pp. 24 – 28, Jul 2009.

[25] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh,M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo,"A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications,"NIST Special Publication 800-22, 2010.

[26] "Diehard test suite," http://www.stat.fsu.edu/pub/diehard/, Last check in July 2011

[27] Knuth D, "The art of computer programming: semiemperical algorithms", Addison Wesley, Reading, USA, 1998.

[28] Gustafson H. et al. "A computer package for measuring the strength of encryption algorithms" , J. Computer Security, vol. 13, pp. 687-697, 1994.