Design of Quantum

by Bayu Rudiyanto

Submission date: 25-Mar-2019 08:36AM (UTC+0700)
Submission ID: 1099024852
File name: Design_of_Quantum_siswanto2017.pdf (724.26K)
Word count: 3167
Character count: 17471

2017 3rd International Conference on Science in Information Technology (ICSITech)

Designing of Quantum Random Number Generator (QRNG) for Security Application

Meilana Siswanto, Bayu Rudiyanto
Renewable Energy Engineering Department,
Engineering Faculty, State Polytechnic of Jember
Jember, East Java, Indonesia
meilana_siswanto@polije.ac.id, bayu_rudianto@polije.ac.id

***Abstract*—Information security, especially cryptography still seems becoming an interested topic of researches in the recent years since it will be responsible to secure a system and data for misusing of attackers. With spreading of internet of things (IoT) applications in many fields whereas many devices will be connected to internet, security issues become one of three common issues related to IoT applications such as innovations, security and interoperability. As a new application of IoT is implemented, a new security system will be needed as well. This paper discusses on designing a quantum random number generator (QRNG) which has a potential for security solution of IoT ecosystem applications.**

Keywords*—*true random number generator; qrng; quantum random number generator; photonic-based random number generator; quantum cryptography

I. INTRODUCTION

With the rapid dan broad developments of IoT ecosystem applications, security problems are becoming a crucial issue in IoT implementations. A new implementation of internet of things will generate a new issue of security system. Investigations on ultimate security of information (cryptographic system) becomes one of the priority research interests in IoT implementation era. In a cryptographic implementation where ultimate security is crucial, randomness quality of key generated by a random number generator (RNG) is required [1] and essential. Ultimate security of an encryption system will rely on randomness level (unpredictable and irreproducible) of keys generated by RNG [2]. Therefore many methods have been proposed to realize truly random number generators (TRNG) as replacing pseudo RNG which has a repetitive occurance and pattern at a certain time [3].

The use of true random number generators (TRNG) seems to be crucial in cryptography. To design an ultimate secured encryption system of quantum cryptography, it demands a true random number generator to produce random key, which increases complexity and resistant to the attackers to crack it. One-time pad (OTP) encryption is an encryption method, as considered the most secured cryptography application, requires high-speed random bit. However, the realization of a hardware-based RNG in these applications is not matured yet, due to its bigger size, sensitive to environment and low output rate [4].

This paper discusses on designing a quantum random number generator (QRNG) which has a potential for encryption application of internet of thing (IoT) ecosystem. Furthermore the method can be integrated into the existing hardware for miniaturization.

In this design of photonic-based RNG comprises optical components, analog-digital electronic systems, and asynchronous transmitter, and utilizes Verilog firmware to integrate the system. The electronic system will convert analog signals produced by an optical componet to digital signals and the system was designed using a FPGA RC10 that consists of three modules; acquisition, whitening, and LFSR module.

II. QUANTUM RANDOM NUMBER GENERATOR

Randomness is events that have no a pattern and cannot be modelled or predicted. Randomness has been used in many applications for simulation, art, statistic, gamings, gambling and especially in cryptography that will be discussed in this paper. Random number generator is methods in generating randomness [5]. Many methods have been proposed to generate randomness such pseudo random generator (PRNG), hardware-based random number generator and true random number generator (TRNG), and quantum random number generator (QRNG) which is considered as hardware-based TRNG. PRNG generates sequence of random numbers based on a deterministic algorithm using a computer. The sequence has repetitive occurances and patterns at a long of certain time and it can be predicted if the initial condition and algorithm are known.

III. DESIGNING OF QUANTUM RANDOM NUMBER GENERATOR

QRNG is one of quantum technologies that can generate keys with many alternative methods [6], and this paper will be focusing on designing of photonic-based random number generator that utilizes a light source to generate random analog signals and a single-photon detection to detect the signals as previously implemented by N. M. Thamrin et. al [7]. Fig. 1 shows behavioral process of data processing module in optical-based QRNG wherein the module has three stages to produce the string of non-deterministic random bits. Starting with data

978-1-5090-5864-8/17/$31.00 ©2017 IEEE

acquisition, by getting the input signals from the optical component, the signals are then processed in whitening module to eliminate all the unwanted non-random aspect in the data. Later, the data will be XOR-ed with the LFSR (Linear Feedback Shift Register) to produce 8 bit random data with good uniformity distribution criteria to liaise with the requirement of NIST (National Institute of Standard & Technology) statistical test. UART (Universal Asyncronous Receiver/transmitter) is then used in the last stage to serialize the 8-bit digital data.

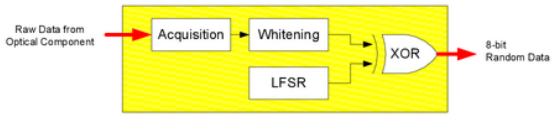

Fig. 1. Data processing (Analog to Digital) in optical-based QRNG.

A. Data Acquisition Module

In a cryptographic application, the generated keys must be resistant to attacks and cryptographically secure. The acquisition module as shown in Fig. 3 is utilized to receive the raw data from the optical component, which is pulses detection of a single photon. This module converts the single photon signals into digital raw random data. A comparator will determine the value of bit 1's and 0's based on the threshold value comparison. Setting of the threshold value will give an effect in the probability of generating bit 1 and bit 0. If the threshold value is set too high, the probability of generating less bit 1's is high, and if it is set too low, the chances of producing more bit 1's is low. The generated raw random bits are bias and correlated to each other. This defect can fault and jeopardize the whole cryptographic system. Therefore, it must be removed from the raw random bits.

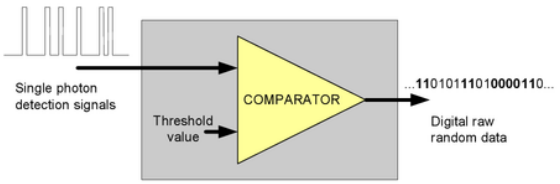

Fig. 2. Data acquisition module in optical-based QRNG.

B. Whitening Module

Whitening module is functioned to eliminate the bias and correlate between raw random bits. This module only accepts sequence of "10" or "01" and will eliminate sequence contained consecutive bit 1's and 0's such as "11" and "00". The biasness and autocorrelation effects can be reduced with this method and thus resulting a better random bit.

C. LFSR Module

Linear Feedback Shift Register (LFSR) is frequently used to produce pseudo random number with goodly statistical properties. An LFSR is of maximal length when the generated sequence passes through all possible 2^{n-1} values, and certain combinations of taps will produce a maximal length LFSR [8]. A LFSR comprises of shift registers with feedback as algorithm wherein each of the squares labelled $S0, S1, \ldots, Sn+1$, is a binary storage component, which could be a memory element, a delay element, or a bistable flip-flop [3]. These n binary storage components are usually called states of the register. At any given time, their contents are defined its state. A shift register that has n stages will consist of 2^n possible states.

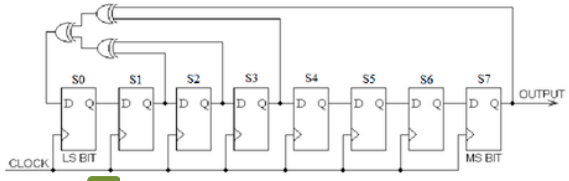

Fig. 3. 8-bit Linear Feedback Shift Register.

LFSR is not considered as a cryptographically secure of system but its construction has decreased the area consumption in the embedded circuit. Fig. 3 shows a block circuit diagram of 8-bit LFSR used in this QRNG design.

D. UART as Asynchronous Transmitter

Fig. 4 describes an asynchronous transmitter which is a single UART that has a parallel-to-serial converter. The asynchronous transmitter (UART) has four inputs i.e. TxD_data, TxD_start, Clock (clk), Reset (rst), and two outputs i.e. busy signal and a serial output TxD_1.

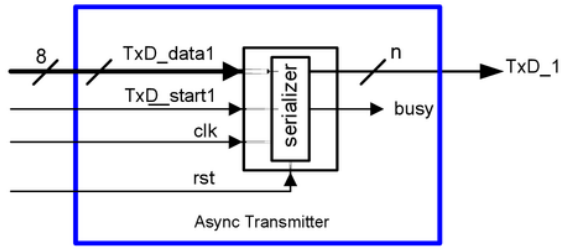

Fig. 4. Asynchronous Transmitter (UART).

UART will start to take an 8-bits data (TxD_data) when the "TxD_start" signal is asserted, and the data will be serialized through some processes i.e. state machine or finite state machine (FSM) and the m-to-n converter, and finally the serial data will be sent into the output "TxD". The "busy" signal will be asserted and the "TxD_start" signal will be ignored while a transmission occurs during that time. So UART actually generates three

signals; the data bits, the start bit signal and the stop bit ("busy" signal) by using a state machine inside.

If a "BaudTick" signal is available, and stated with 921600 times a second. The state machine will start right when "TxD_start" was asserted, but only advances when "BaudTick" was asserted and then the "TxD_1" will generate serial output through the m-to-n converter inside the UART.

IV. Random Number Generator Tests

Several test packages are already available and could be used to calculate randomness of binary data sequence statistically [1], and randomness test in this discussion uses NIST statistical test suite which has sixteen statistical parameters of randomness. The NIST test suite consists of sixteen test criterias that were built to test the randomnes level of binary data sequence generated by either software or hardware based on an existing event such as chaostic events, light source, noise, quantum or pseudorandom number generators. The statistical parameters used in this test will identify the existing of non-randomness aspects in a binary data sequence. Final report of the test will summarize statistical analysis results of a binary sequence in linearity diagrams and decide the level randomnes of the sequence.

V. Discussion

RNGs used to generate key for an encryption process should be considered as a crucial part of the cryptographic application. Weaknesses of randomness quality of key produced by the RNG can cause a complete failure of the entire system. Therefore, the generated random sequences for keys in the encryption applications must verified and tested using standard of statistical tests.

Testing and verification of the randomness quality is very important matter in cryptography system since any practical RNG implementations will behave as a key generator and the generator sometimes produces unrandom bits which might be caused by supply voltage variations, gain errors, circuit saturation, temperature, cabling and grounding problems [3].

A. Converting Process of Analog to Digital

Light signals outputed from the optical component as shown in Fig. 5 is processed to be serial digital signals (digital bit sequence). Measurement and analysis of a single bit of digital sequence was done using Tektronic DPO4000 / Agilent MS07054A Mixed Signal Oscilloscopes. The digital sequence data is then collected by Realterm™ software as shown in Fig. 6, and its randomness will be analyzed using NIST statistical test. Histogram and scatter analysis also will be conducted using Origin™ software in order to see its pattern.

Randomness testing of the QRNG which is designed using a LFSR with primitive polynomial $1+x^4+x^5+x^6+x^7$ was conducted at baud rate 80 Kcps (character per second). Since a character consists of 8 bits data, this output is equivalent to 640 Kbps. In order for miniaturization purpose, the designed photon-based RNG was implemented on a Complex Programmable Logic Devices (CPLD).

Fig. 5. Process of converting analog signals to be digital signals.

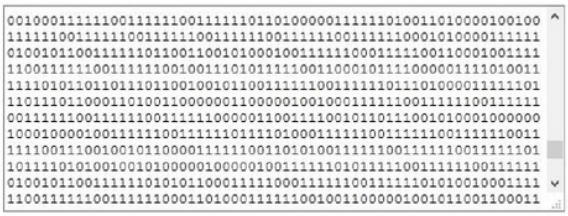

Fig. 6. The digital data sequence collected by realterm.

B. Randomness Testing

The sixteen statistical criterias of randomness which are determined by NIST test standard and were described in this paper are as the following; frequency (monobit), frequency within a block, cumulative sums, runs, longest run of ones in a block, random binary matrix rank, discrete Fourier transform (spectral), non-overlapping (a-periodic) template matching, overlapping (periodic) template matching, Maurer's universal statistical, approximate entropy, random excursions, random excursions variant, serial, Lempel-Ziv complexity and linear complexity.

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.978228 for a sample size = 643 binary sequences, and the minimum pass rate for the random excursion (variant) test is approximately 0.975521 for a sample size = 425 binary sequences. Table I shows randomness test results of a single output photonic-based random number generator using NIST. In this NIST testing, value of 100 is used for frequency and block frequency setting, and 5 for serial and entropy parameters, 643 for bit stream number, and 1000000 for the length of bit stream [9].

The statistical test is utilized to calculate a *P-value* with different methods that summarizes the strength of the witness against the null hypothesis. In this test, a *P-value* is the probability that an ideal random number generator would have generated binary sequences less random than the sequences that were tested, given the type of unrandomness quantified by the statistical test. Perfect randomness will occur if a *P-value* is equal to 1, and *P-value* is equal to zero will indicate that the binary sequence is completely non-random [8].

A significance grade (α) could be chosen for the test modul. The null hypothesis will be accepted if $P\text{-}value \geq \alpha$; whereas the binary sequence will appear to be random. If value of $P\text{-}value < \alpha$, the null hypothesis will be rejected, meaning that the binary sequence is not random. The parameter α indicates the probability of the type I error whereas typically the range of α is between 0.001 to 0.01. An α of 0.01 denotes that one will expect 1 sequence of 100 sequences will be rejected.

TABLE I. NIST STATISTICAL TESTS: P-VALUE & PROPORTION

Statistical Tests	UART Output	
	P-Value	Proportion
Frequency	0.706682	0.9844
Block-frequency	0.881521	0.9907
Cumulative-sums	0.957089	0.9891
Runs	0.554739	0.9922
Longest-runs of Ones	0.415927	0.9876
Rank	0.784272	0.9907
FFT	0.026695	0.9969
Non-periodic-templates	0.504527	0.9829
Overlapping-templates	0.444517	0.9907
Universal	0.963672	0.9876
Approximate entropy	0.793156	0.9938
Random-excursions	0.169882	0.9870
Random-excursions Variant	0.062613	0.9922
Serial	0.159103	0.9891
Lempel-Ziv Complexity	0.033231	0.9891
Linear Complexity	0.101292	0.9891

[a] Statistical test results using NIST test, only *P-value* and *Proportion* parameters

A $P\text{-}value \geq 0.01$ will determine that the binary sequence is random with a confidence level of 99 %, otherwise if $P\text{-}value < 0.01$ will define that the binary sequence is not random with the same of a confidence level. In this test result as shown in TABLE 1, all values of *P-value* calculated by using different statistical methods of NIST test are more than 0.01. These results indicate that output sequence of this QRNG design is considered truly random with a confidence level of 99 %.

C. Comparison Pseudorandom and QRNG

The random pattern analysis i.e. scatter and histogram analysis are utilized to make a comparison of digital sequence data generated by pseudorandom and the designed quantum random number generator.

The scatter and histogram analysis were conducted using Origin™ software. As shown in Fig. 7, scatter analysis of the pseudorandom data has the same patterns and repetitive occurences per period. This pattern becomes a limitation of pseudorandom dan could be a vulnerable for attackers to crack a message if pseudorandom data are used as key to encrypt the message. Fig. 8 shows scatter analysis of the designed photonic-based random number generator which has no patterns. This result could be an evidence that the digital sequence data produced by QRNG are truly random.

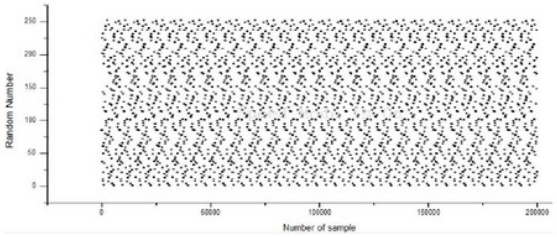

Fig. 7. Scatter analysis of pseudorandom.

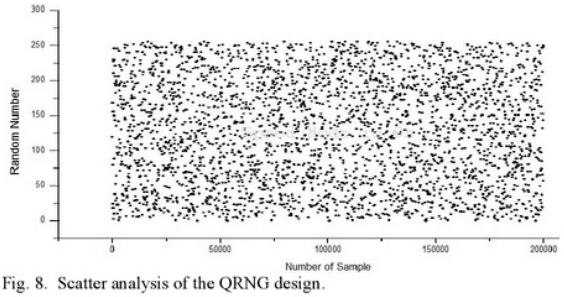

Fig. 8. Scatter analysis of the QRNG design.

Histogram analysis of the digital sequence data generated by pseudorandom is shown in Fig. 9. As can be seen in the Fig., the histogram bars pattern of pseudorandom data are platted, and have consistent frequencies.

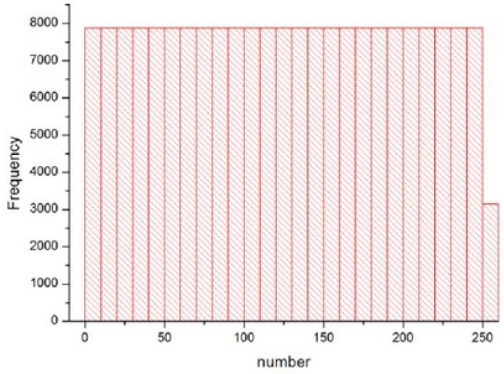

Fig. 9. Histogram analysis of pseudorandom.

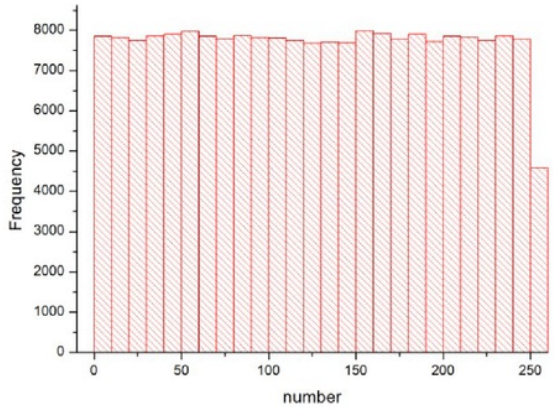

Fig.10. Histogram analysis of the designed QRNG.

It is clearly different with histogram bars patterns of the designed QRNG that are not platted with inconsistency of frequencies as shown in Fig. 10.

VI. CONCLUSIONS

In this paper, a design of quantum random number generator (QRNG) which is photonic-based random number generator has succesfully implemented. Randomness test was conducted to the QRNG's output using NIST statistical test. The statistic test is utilized to determine values of *P-value* that summarize the strength of the evidence contrary to the null hypothesis. The binary sequence will be perfect random if *P-value* is equal to 1, and *P-value* of zero denotes that the binary sequence is completely nonrandom. Results of the test show that all values of *P-value* are more than 0.01 that indicate output sequences of the QRNG design are random with a confidence level of 99 %. Scatter and histogram analysis for pattern comparison of digital sequence data produced by the QRNG and pseudorandom were also conducted. Scatter analysis of the pseudorandom shows the existence of a pattern in the certain time which is disappeared in the QRNG. Histogram analysis of the pseudorandom shows a platted pattern with consistent frequencies, it is clearly different with the designed QRNG that has no a pattern with inconsistency of frequencies. In the future works, designing a parallel QRNG will be conducted to enhance random bit speed significantly. Parallel QRNG must be developed to fullfil OTP (One-Time Pad) encryption requirement that requires a high-speed random bit.

ACKNOWLEDGMENT

The authors would like to thank to State Polytechnic of Jember especially to Renewable Energy Engineering Department, Engineering Faculty, for providing facilities to join the conference.

REFERENCES

[1] M. Drutarovsky, P. Galajda, "A robust chaos-based the random number generator embedded in reconfigurable switched-capacitor hardware," RadioEngineering, Vol. 16, No.3, September 2007.

[2] K. Uchida, T. Tanamoto, and S. Fujita, "Single-electron randomnumber generator (RNG) for highly secure ubiquitous computing applications," *ScienceDirect Solid-State Electronics*, vol. 50, pp.1552–1557, 2007.

[3] M. Siswanto, G. Witjaksono, M. Soeheila and Z. Hamdan, "Study on the effects of characteristic polynomial in LFSR for randomness quality," *Proceeding of the International Conference on Advanced Science, Engineering and Information Technology (ICASEIT 2011)*, Malaysia 14-15 Jan 2011.

[4] M. Siswanto, G. Witjaksono, and W. Firdaus. Hj. Yaakob, "Quantum random number generator (QRNG) with multi random source (MRS) processor," World International Property Organization (WIPO), International Publication Number WO 2012/064174 A1, 18 May 2012.

[5] A.A. Thomas and V. Paul, "Random Number Generator Methods a Survey," *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, vol. 6, pp.556–559, Jan 2016.

[6] M.H. Collantes, J.C.G.-Escartin, "Quantum Random Number Generators, " Instituto Nacional de Ciberseguridad, Avenida Jose Aguado, 41, Edificio INCIBE 24005, Leon, Spain, Oct. 2016.

[7] N.M. Thamrin, G. Witjaksono, A. Nuruddin, and M. S. Abdullah, "A Photonic-based random number for cryptographic application," IEEE Computer Society, pp. 356–361, 2008.

[8] Linear Feedback Shift Registers, 31 January 2017, http://www.oocities.org/siliconvalley/screen/2257/vhdl/lfsr/lfsr.html

[9] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, & S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Speed Publication 800-22 (with revisions date, May 15, 2001).

Design of Quantum

ORIGINALITY REPORT

19%	15%	15%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	insightsociety.org Internet Source	3%
2	nvlpubs.nist.gov Internet Source	2%
3	eprint.iacr.org Internet Source	2%
4	www.scilit.net Internet Source	1%
5	ftp.fourmilab.ch Internet Source	1%
6	Shuqin Zhu, Congxu Zhu, Huanqing Cui, Wenhong Wang. "A Class of Quadratic Polynomial Chaotic Maps and Its Application in Cryptography", IEEE Access, 2019 Publication	1%
7	webpages.uncc.edu Internet Source	1%
8	Alessandro Sorniotti. "Efficient Access Control for Wireless Sensor Data", International	1%

	Journal of Wireless Information Networks, 09/2009 Publication	
9	N.M. Thamrin. "An Enhanced Hardware-based Hybrid Random Number Generator for Cryptosystem", 2009 International Conference on Information Management and Engineering, 04/2009 Publication	1%
10	media.neliti.com Internet Source	1%
11	Submitted to Rochester Institute of Technology Student Paper	<1%
12	www.ijcee.org Internet Source	<1%
13	M.S. Abdullah. "A Photonic-based Random Number Generator for Cryptographic Application", 2008 Ninth ACIS International Conference on Software Engineering Artificial Intelligence Networking and Parallel/Distributed Computing, 08/2008 Publication	<1%
14	"Table of contents", 2017 3rd International Conference on Science in Information Technology (ICSITech), 2017 Publication	<1%

15	Tong, X.. "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, 200904 Publication	<1%
16	chinacissp.com Internet Source	<1%
17	Nathalie Bochard, Florent Bernard, Viktor Fischer. "Observing the Randomness in RO-Based TRNG", 2009 International Conference on Reconfigurable Computing and FPGAs, 2009 Publication	<1%
18	Celal Erbay, Salih Ergin. "Random Number Generator Based on Hydrogen Gas Sensor for Security Applications", 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018 Publication	<1%
19	Xiamu Niu, Yongting Wang, Di Wu. "A Method to Generate Random Number for Cryptographic Application", 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014 Publication	<1%
	etd.lib.metu.edu.tr	

20	Internet Source	<1%
21	Chen, Fu Long, Zhao Xia Zhu, and Xiao Ya Fan. "FPGA-Based In-Circuit Verification of Digital Systems", Advanced Materials Research, 2011. Publication	<1%
22	documents.mx Internet Source	<1%
23	AFSHIN AKHSHANI. "PSEUDO RANDOM NUMBER GENERATOR BASED ON SYNCHRONIZED CHAOTIC MAPS", International Journal of Modern Physics C, 2010 Publication	<1%
24	arxiv.org Internet Source	<1%
25	ee.usyd.edu.au Internet Source	<1%
26	"Foundations and Practice of Security", Springer Nature America, Inc, 2013 Publication	<1%

Exclude quotes	Off	Exclude matches	Off

Exclude bibliography On