Performance of Memristor Based Ring Oscillators True Random Number Generator for Energy Technology

N A N Hashim, J T H Loong, F A Hamid

Abstract: ***We are living in an era where everything is trying to be more connected in terms of the different physical entities and its surrounding environment. This new concept that is developing called the Internet of Things (IoT) has garnered a lot of attention [Bodei, 2019 #45]. There are various of applications and smart objects associates with the IoT and this leads to an increase in security challenges. IoT security is very important but getting harder to achieve. One example of utilization of IoT is in the smart grid infrastructure and this in turn increases the need for network security. An integrated internet-based smart grid and energy resources also called Energy Internet (EI) has a lot of security challenges that comes with the current smart grid. Smart grid infrastructure and any means of energy that implements the internet system also known as Energy Internet (EI) has many security challenges that come with the current smart grid. A memristor based ring oscillator True Random Number Generator design has been proposed in this research as a solution that can combat security challenges that existed in the hardware implementation of devices. Inputs based on non-deterministic methods are being used in TRNGs to generate outputs that possessed randomness characteristics in applications of IoT that makes it secure. Complementary metal oxide semiconductor (CMOS) technology of 0.18 µm are being used in the TRNG design and a software of LT SPICE IV helps to realized it.The proposed TRNG design produced output that passed 10 out of the 15 NIST tests, therefore showed that the TRNG produce a fairly random output.***

Keywords: True Random Number Generator; Memristor; Ring Oscillator; Hardware Security; Nanoelectronics.

I. INTRODUCTION

The world is evolving where internet is a part of our daily lives and is heading towards a new paradigm called Internet of Things (IoT). IoT is a connection of the network to reality by having physical objects in connection with its surroundings. The 'smart' devices contained sensors that gather datas, keeps them on memory 'clouds' and through actuators connects with the surrounding. These devices made it possible for users to communicate with each other and work towards a common goal. By having this new revolution of technology, there are new prospects in terms of economically and socially due to its effects on future planning of cities, industrial plants, landscaping and emerging infrastructure [1].

Revised Manuscript Received on December 15, 2019.

N A N Hashim, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.

J T H Loong, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.

F A Hamid, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.

There are many advantages that come with the IoT technology and the possibilities are endless in various capacities but a huge part of its development relies on the hardware security and its sturdiness. The IoT applications are vast such as smart grid infrastructure, healthcare monitoring and Energy Internet but are considered complex and sensitive [2].

Although this concept of IoT contains a lot of benefits, it also comes with a lot more security requirements due to the fact that the processes is exposed in a network that was used to be much more private when it was manually executed and now are more prone towards security attacks and cyber dangers. Although various type of application will have its own security requirements, basic security apparatuses are still required to safeguard the network system and also maintain a secure communication of trading datas and protecting the privacy of the process [1].

The IoT is very important and has been associated with the energy industry in terms of recognizing and realizing the main components of a lot of devices to ensure there are improvements in the operational and communication productivities. One of the most prominent examples of IoT application that relates to the energy technology is the smart grid infrastructure. Within the past years, there has been a rise in the security outbreaks that threatened the safety of the application. These occurrences have contributed losses in the economy and also affected the environment. There is a need to develop a more secure infrastructure for the smart grid and tackle any security concerns that have risen [2]. Security services are basically realized on a main system that consists of encryption or decryption and signature or verification processes. These processes are premeditated to ensure that there is a high security level that can be achieved [3].

In the majority of modern security systems, random number generator (RNGs) is the central of it. These systems have been developed to ensure a high security level but maintaining low effect on the user's communication and output. This showed that the application of RNGs is crucial in order to have safe transactions of the network. There are two types of RNGs which are pseudo random number generator (PRNG) and true random number generator (TRNG). The PRNG is considered the most type implemented but it uses deterministic algorithm that produces output with a sequence of bits that repeats overtime [4]. A TRNG can produce a truly random and unique output each time. Hardware security solutions can deliver a safe building blocks that consist of having a unique

physical feature for circuits and equipments that produce high quality performance using low energy.

A TRNG is emerging as a technology in hardware security that is normally founded by its physical characteristics such as a quantum phenomenon [5, 6].

Technology development has introduces a lot of nanoelectronics technology that can be implemented in the traditional CMOS fabrication technologies and provide solutions to all of security challenges [7, 8]. By introducing these nanoelectronics in the fabrication, it can present an extensive alternative approach of the operation and execute nonlinear functions [9, 10]. One of an example of nanoelectronics are memristors. Memristors based TRNG is believed to have the potential solution to be more resilient towards security attacks and offer alternatives for research and development.

This research will explore the application and advantages of memristor and the randomness traits of the output of the TRNG design. The memristor model of the design is based on the Prodromakis window function. The simulations were executed using Silterra 180 nm CMOS process with a voltage supply of 1.8v. The purpose of the implementation is to introduce additional variation to the TRNG and improved randomness in an output.

True Random Number Generator

Random number generator (RNG) are categorise into two main categories which are the pseudo random number generator (PRNG) and the true random number generator (TRNG). PRNG produces deterministic output by using algorithm whereas TRNG produces non-deterministic outputs that are based on entropy sources realized in hardware. The entropy can be extracted from hardware in a lot of ways and an example of it is by occurrence that are physically-based such as thermal noise and clock jitter [11].

True random number generators (TRNGs) are a device used to generate outputs of sequences that are in a randomly manner of binary numbers that are unique and unpredictable. When the device functions, a random occurrence will happen and be used in the hardware TRNGs which in turn will produce sequences that are in random order and unpredictable. Examples of the physical sources that can be extracted as the initial value are thermal noise, shot noise and clock jitter. These sources produce noises that are irregular and this makes it difficult for attackers to guess the output produced. TRNGs produces output of binary sequences that are irregular and non-deterministic which makes the output sequences unable to repeat its patterns although the attackers is aware of the internal structure of the hardware [12].

This research paper presents a design of TRNG that implements memristor based ring oscillators (MRO) as the entropy source. Using ring oscillators as the entropy sources is common for the RNGs. In the paper [13], the basic idea of implementing ROs with TRNGs was presented and how the inverters processed the delay that happens between logi gates and is in a ring connection of frequency/phase instability from a clock jitter. Flip-flops and latches will extract the jitter to be used as its sampled entropy source for the hardware. The randomness characteristics are more prominent in the outputs when nanoelectronic TRNGs are being used. There have been more TRNGs adopting these different nanoelectronics in the past years such as contact resistive random-access memory [10], nanoscale diode [14], memristor [15, 16], magnetic-tunnel junction [17, 18], and carbon nanotube field-effect transistor [19].

Memristor

In 1971, Leon Chua discovered a connection existed between charge, q and flux-linkage, φ in the electrical elements relationships. He defined that the memristor is the missing relationship and the circuit element of two-terminal of the basic electrical relationships [20]. The term ‘memristor’ comes from the wording of ‘memory resistor’ which means a circuit element that is in the passive category that retains the connection of the time integrals between the current and voltage throughout the two-terminal circuit element.

Chua presented his proposal of the existence of memristor and this sparked the interests on the memristor [21]. There are six possible relationships of the four variables. Among the relationships, five of them are well-known which are current that describes the time integral of charge, voltage that is described as flux linkage’s time integral, resistor which is a connection of current and voltage, capacitor which is the connection of voltage and charge and lastly the inductor which is the connection of current and flux linkage. Figure 1 showed a diagram of the combination of the six relationships.

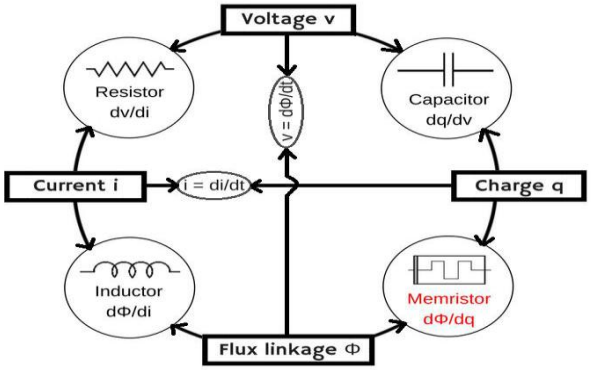

Fig. 1 Diagram of the relationships of the four variables [22]

In 1976, Chua and Kang presented the theory of memristor and was explored in more depth towards the devices that have the memristor properties and systems [23]. The memristor is believed to not only be confined to a single, particular device but possessed characteristics that can adapt in different entities and systems. Memristors or memristance can behave similarly as a resistor where the electrical components can possess internal resistance but the memristor is not deliberately created as a resistor. There are plenty of examples of devices and systems that possessed the memristors properties such as thermistors and discharge tubes.

The actual, physical memristor was realized much later on in 2008. A group of academics in Hewlett-Packard (HP) laboratories was the one who discovered the memristor

when they were researching on an appropriate electrical switch to be adopted in their crossbar memory research.

The memristor was fabricated by having two films of titanium dioxide, TiO_2 and one of the film consisted of the oxygen vacancies that also reacts as the charge transporters. The layers of titanium dioxide is normally called TiO_{2-x} and by having the '2-x' only signals doping instead of the mathematical formula and the amount of electrons are smaller compared to the steady TiO_2 molecule. There are two platinum electrodes that are constructed to sandwich the two layers of titanium dioxide [9, 24]. Figure 2 showed the composition of the memristors that were created by HP Labs.

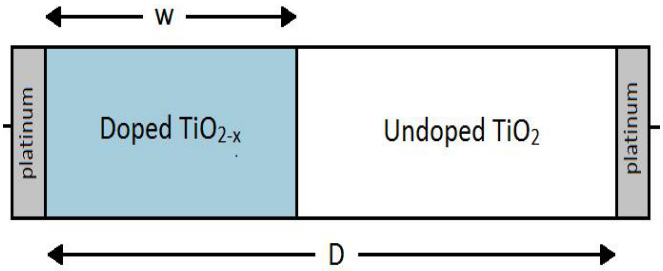

Fig. 2 Physical structure of the memristor [9]

Whenever a high frequency signal is supplied to a memristor, the change in memristance does not acts linearly. One of the characteristic of a memristor is that when it is supplied with a periodic signal, the graph of I-V relationship of the component will reflect a hysteresis circle that is decreased towards the starting point. Figure 3 showed the graph of I-V relationship of the memristor when it is supplied with a sinusoidal signal. The higher the applied signal's frequency is the shape of the hysteresis circle decreases towards the starting point slowly. The hysteresis circle eventually changes to a straight line as depicted in the graph of I-V relationship of a resistor as the frequency becomes higher. As a whole, it was concluded that the memristor acts linearly when excited with high frequency signal and vice versa when excited with low frequency signal [23].

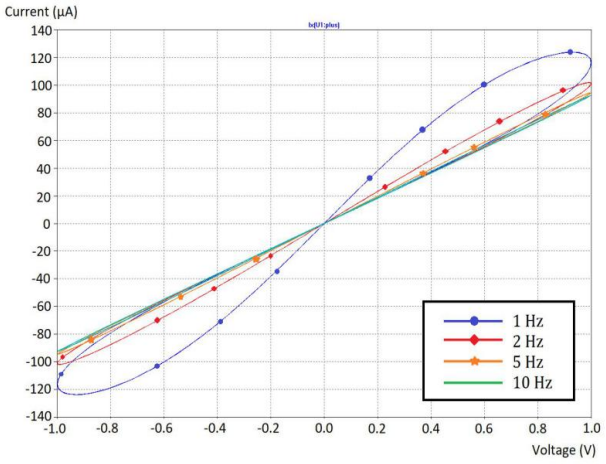

Fig. 3 I-V plot of memristor [23]

II. METHODOLOGY

Design of Memristor Based Ring Oscillators TRNG

There are three circuits that composed the design of the proposed memristor based ring oscillators TRNG which are the entropy source, harvesting mechanism and post processing. The TRNG design are modified from the paper of Ning et al. [25]. In the paper, a high speed TRNG with a wide-ranging of voltage supply constructed using various prime numbers of inverters that assembled ring oscillators were fabricated. The output's randomness characteristics were enhanced by having a third circuit of Von Neumann corrector in the topology of the TRNG. Our proposed TRNG design is different from the Ning et.al. Design in terms of the inverters are constructed using the common source stage that adopts a load of resistor and eventually been replaced by the memristor component. The memristor based ring oscillators are adopted in the entropy source circuit to be included in the TRNG design.

Entropy Source Circuit

The entropy source circuit is crucial in the TRNG design. The various prime numbers of inverters are incorporated to build the memristor based ring oscillators. The phase noise are collected and being used as the sampled entropy as the source of randomness of the input. There are four categories of ring oscillators with various prime numbers of inverters consisted of 13, 17, 23, 31 inverters and each RO are attached to three XORs. The memristor are implemented in the inverters to build the memristor ring oscillators (M-RO). The topology of the circuit is shown in Figure 4. The prime number of inverters is adopted to lessen any intersections that happen in the transition zones but at the same time it can intensify the amount of entropy of the circuit. It was designed in such that each ring oscillator contains a memristor to replace the resistor part in the common source stage that has resistor as its load.

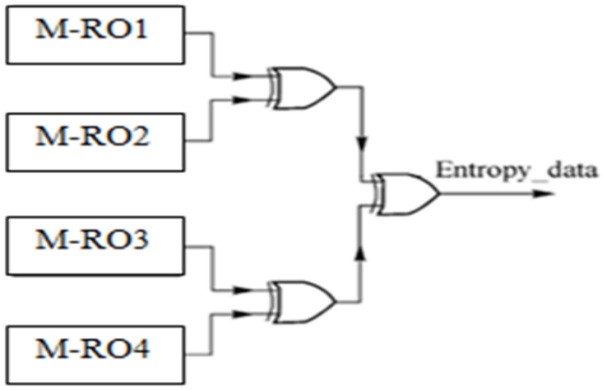

Fig. 4 Entropy source circuit using memristor based RO

Figure 5 shows the composition of the entropy source circuit. Each ring oscillators were build using the memristor based ring oscillators (M-RO) that adopts the concept of a common source. Different window functions was adopted by the memristor model to investigate any changes in behavior and the performance results of the output produced.

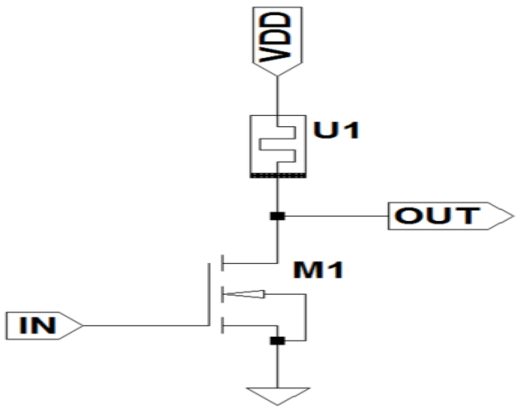

Fig. 5 The composition of the entropy source circuit that adopted memristor based ring oscillators

Harvesting Mechanism

The harvesting mechanism consisted of a modest arbiter that uses set/reset (SR) latch concept as shown in Figure 6. The concept of an SR latch contains two steady states that can retain the state information. It is also called a flip-flop. Signals are applied to the control inputs and the arbiter can control its state and can produce a maximum of two outputs. The SR latch has a design that is cross-coupled and this can decrease bias of up to 2 ps compared to traditional arbiter. Besides that, random and systemic variations can be decreased in the circuits which lead to less input bias. This is due to its layout and the components used to construct it.

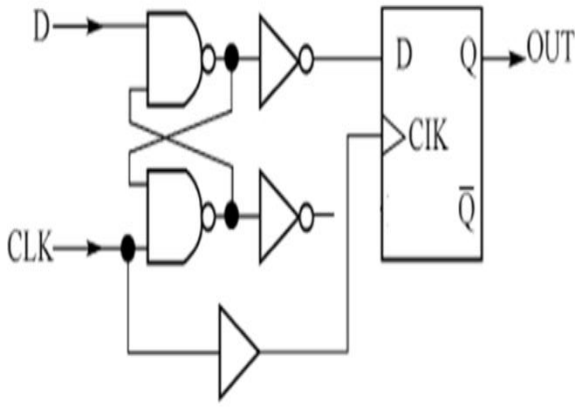

Fig. 6 Simple arbiter of SR latch of harvesting mechanism [25]

Post Processing

Post processing is not a compulsory circuit to have in a TRNG but it can enhance the quality of randomness in an output. Von Neumann corrector is used to construct the circuit of the TRNG. The Von Neumann corrector is constructed by having a few logic gates as shown in Figure 7. From an output of four bits, it will be decreased to an output of 1 bit which is compacted by a factor of four. Any sequences with an output bits of '00' and '11' will be extracted from the sequences and '01' turns to '1' and '10' turns to '0'.

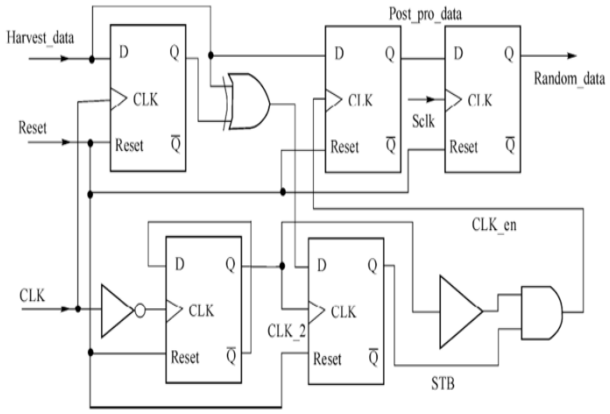

Fig. 7 Simple Von Neumann corrector [25]

III. SIMULATION SETUP

A Linear Technology Corporation software of LTspice IV was used to design the TRNG design and the transistors was used by CMOS technology of SilTerra 180nm and with a voltage supply of 1.8v. The TRNG generated a maximum length of 10000 bits to be analyzed in the research. This was the maximum data size that the proposed TRNG design can produced due to the computer system processor. All of the simulations were conducted the Microsoft Windows 7 system that has an operating core of Intel i5 at 2.67GHz with 4GB memory RAM. The W/L for the MOSFET transistors was set to 2.5 to ensure a continuous oscillation and to maintain all of the transistors to be in saturation. The gate width was set to 4.5 µm and the gate length was set to 1.8 µm.

The memristor SPICE model adopted for the memristor-based ring oscillators TRNG was based on the linear ion drift model and has a window function by Prodromakis. The linear ion drift model has an easier implementation for the TRNG and has fewer time simulation and power compared to the nonlinear ion drift model. . The SPICE subcircuit was used to make any changes to the memristor model and attached in the appendix. The default values below are extracted from Prodromakis et.al. and are commonly used for any simulations conducted. The settings of the memristor parameters are displayed below;

- Resistance in ON state, $R_{ON} = 100\Omega$
- Resistance in OFF state, $R_{OFF} = 16k\Omega$
- Resistance at T = 0, $R_{INIT} = 11k\Omega$
- Width of the thin film, D = 10nm
- Ion drift migration coefficient, $\mu = 10fm2/(V{\cdot}s)$
- Parameter of the WINDOW-function for modeling nonlinear boundary conditions, p = 10

Statistical Tests Evaluation

The randomness of the output are verified using a common test suite used is by National Institute of Standards and Technology (NIST) that can tests for specific randomness characteristics. The NIST test suite consists of 15 statistical tests [26]. The NIST test suite consists of various randomness tests that were created to test binary sequences that resulted from true random number generator

(TRNG) or pseudorandom number generator (PRNG) [26]. The different aspects of randomness that exists in a stream of continuous bits can be analyzed using this test suite as the tests looked at different characteristics that can make the output be considered not random. There are various non-randomness characteristics that can appear in an output and the tests breakdown the different types in 15 statistical tests. There are subtests in some tests that can be considered as one test such as the cumulative sum test. The Cumulative Sums Test are divided to two subsets of reverse and forward but are considered as one test. Below are the 15 statistical tests that exists in the test suite: [26]

The Frequency (Monobit) Test

- Frequency Test within a Block
- The Runs Test
- Tests for the Longest-Run-of-Ones in a Block
- Binary Matrix Rank Test
- The Discrete Fourier Transform (Spectral) Test
- The Non-overlapping Template Matching Test
- The Overlapping Template Matching Test
- Maurer's "Universal Statistical" Test
- Linear Complexity Test
- The Serial Test
- The Approximate Entropy Test
- The Cumulative Sums (Cusum) Test
- Random Excursions Test
- Random Excursions Variant Test

For each of the tested stream of binary numbers there will be a probability value (P-value) for the hypothesis of null that will be generated. In order to pass each statistical test, the value of the P-value needs to exceed 0.01. This research will consider 12 of the 15 tests. The input requirements of each of the tests are different and require certain number of lengths. Three of the tests which are Maurer's "Universal Statistical" Test, Random Excursions Test and Random Excursions Variant Test are excluded due to the input size recommendation that needs a minimum of 10^6 bits to be tested. Since the proposed TRNG design are only able to produce until 10 000 bits, the three tests are removed. The TRNG design was only competent to produce a maximum of 10 000 bits due to the computer processor limitations of 4GB RAM.

IV. RESULTS AND DISCUSSIONS

The NIST tests results for the TRNG is shown in Table 1 for data size between 1000 to 10000 number of bits.

Table. 1 NIST test results for different number of bits of proposed TRNG

Statistical Test	P-value (1000 bits)	P-value (2000 bits)	P-value (3000 bits)	P-value (4000 bits)	P-value (5000 bits)	P-value (6000 bits)	P-value (7000 bits)	P-value (8000 bits)	P-value (9000 bits)	P-value (10000 bits)
Approximate entropy	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Block Frequency	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Cusum-Forward	Pass	Pass	Pass	Pass	Fail	Fail	Fail	Fail	Fail	Fail
Cusum-Reverse	Pass	Pass	Pass	Pass	Fail	Fail	Fail	Fail	Fail	Fail
Spectral DFT	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail
Frequency	Pass	Pass	Pass	Fail	Pass	Fail	Fail	Fail	Fail	Fail
Linear Complexity	Fail	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Long Runs of Ones	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Non Overlapping Templates	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Overlapping Template	Fail	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Random Excursions	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Random Excursions Variant	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Rank	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Runs	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Serial	Fail	Pass	Pass	Pass	Fail	Fail	Pass	Pass	Pass	Pass
Universal	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Total of tests passed	6	10	10	10	7	7	8	8	8	7
Success rate (%)	50.0	83.3	83.3	83.3	58.3	58.3	66.7	66.7	66.7	58.3

Table 1 showed the results of the TRNG after the binary numbers from the random output produced were verified using the NIST. The NIST test suite was run for sets of amount of bits to analyze the pattern of number of tests that it will passed in the NIST. Based on the results of the table, the proposed TRNG has the best randomness characteristics when produced 2000 to 4000 bits. It passes 10 out of 12 of the NIST test suite. The total tests passed maintained as the TRNG produces more output bits and started to decrease after producing 4000 and more bits. This proved that the TRNG are only able to generate an output that only passed 10 of the tests.

The two tests that the TRNG consistently failed were approximate entropy and runs test. The approximate entropy, $A_pE_n(m)$ test analyze if there are any patterns of bits that are in repetition in the sequence of the output. It calculates the logarithmic frequency of the blocks that has m sequence that are near each other and that remains so for blocks that are in one position ahead. Failing this test indicated that the $A_pE_n(m)$ have a pattern that is consistent in the sequence.

The other failed test is the runs test that measures if there is a pattern of logic '1' or '0' that is in consistent and the oscillation that exists among the pattern of strings are fast enough. The amount of runs for '*n*' bits, V_n is used to measure the distribution of the amount of runs and failing the test indicated that the V_n has small values which means the change of the output bits was too little to be considered to have this random characteristic [26].

The proposed memristor based ring oscillators TRNG showed best randomness characteristics when data size is 2000 to 4000 bits in terms of NIST tests values. This showed that there might be a repetition in the output bits sequences as the data size increases more than 4000 bits. The frequency test started to fail when data size increases and this indicated that the proportion of logic '1' and '0' is not consistent with a random behaviour of a stream of bits. All following tests are subjected to the result of this test and by failing it might be the reason the results started to decrease. Besides that, some of the tests that failed might indicate that the data is not in compliance with the criterias [26]. The results indicated that the TRNG has the potential to produce an output that possessed randomness characteristics and can be used for research and development solutions for security attacks.

V. CONCLUSIONS

In summary, our TRNG design was designed in such way that it can generate an output that possessed traits that are considered random for research and development of hardware security solutions against attacks. This solution can lead to safe networking transactions for the energy technologies and devices that are involved. The topology of the design comprised of three main circuits; entropy source, harvesting mechanism and post processing. The entropy source circuit has been modified by having memristor replaced the resistors of common source stage for each ring oscillators. All of the simulation setup of the TRNG design was presented and the performance results of the output were evaluated using the NIST test suite. It was discovered that the output has the best performance results when the data size is 2000 bits which passed 10 out of the chosen 12 tests. The output generated by the TRNG is able to show traits that are considered random and can be explored further to provide a solution to the security challenges that the technologies in energy and environment industry are facing.

Future research development can be directed towards increasing the data size of the output bits produced in accordance to the input size recommendation of the statistical tests and incorporating more memristors or other nanoelectronics to the TRNG design. The hardware implementation of the TRNG design can also be developed.

ACKNOWLEDGMENTS

The UNITEN internal grant for project J510050827 had funded and supported this study. A token of appreciation for all of the inputs and knowledge provided by my project leader and colleagues from Universiti Tenaga Nasional.

REFERENCES

1. C. Bodei, S. Chessa, and L. Galletta. Measuring security in IoT communications, Theoretical Computer Science, vol. 764, 100-124, 2019/04/11/ 2019.
2. A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong. Cyber security framework for Internet of Things-based Energy Internet, Future Generation Computer Systems, vol. 93, 849-859, 2019/04/01/ 2019.
3. H. Hellaoui, M. Koudil, and A. Bouabdallah. Energy-efficient mechanisms in security of the internet of things: A survey, Computer Networks, vol. 127, 173-189, 2017/11/09/ 2017.
4. S. Hedayatpour and S. Chuprat. Random Number Generator Based on Transformed Image Data Source, in Advances in Computer, Communication, Control and Automation, Berlin, Heidelberg, 457-464, 2012.
5. D. E. Holcomb, W. Burleson, and K. Fu. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers, vol. 58, 2009.
6. D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. v. Dijk, and S. Devadas. Extracting secret keys from integrated circuits, IEEE Trans. Very Large Scale Integr. Syst., vol. 13, 1200-1205, 2005.
7. J. Hutchby, G. I. Bourianoff, V. V. Zhirnov, and J. E. Brewer. Extending the road beyond CMOS vol. 18, 2002.
8. D. J. Frank and Y. Taur. Design considerations for CMOS near the limits of scaling, vol. 46, 2002.
9. R. S. Williams. How We Found The Missing Memristor, IEEE Spectrum, vol. 45, 28-35, 2008.
10. C. Huang, W. C. Shen, Y. Tseng, Y. King, and C. Lin. A Contact-Resistive Random-Access-Memory-Based True Random Number Generator," IEEE Electron Device Letters, vol. 33, 1108-1110, 2012.
11. S. Buchovecká, R. Lórencz, F. Kodýtek, and J. Buček. True random number generator based on ring oscillator PUF circuit, Microprocessors and Microsystems, vol. 53, 33-41, 2017/08/01/ 2017.
12. M. M. Abutaleb. A novel true random number generator based on QCA nanocomputing, Nano Communication Networks, vol. 17, 14-20, 2018/09/01/ 2018.
13. B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer. Modeling and observing the jitter in ring oscillators implemented in FPGAs, in 2008 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and System, 1-6 2008.
14. U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba. Applications of High-Capacity Crossbar Memories in Cryptography, IEEE Transactions on Nanotechnology, vol. 10, 489-498, 2011.
15. Y. T. Chiu. A memristor true random-number generator, IEEE Spectrum, 2012.
16. T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, et al. High-speed true random number generation based on paired memristors for security electronics, Nanotechnology, vol. 28, 455202, 2017/10/17 2017.
17. Y. Qu, J. Han, B. F. Cockburn, W. Pedrycz, Y. Zhang, and W. Zhao. A true random number generator based on parallel STT-MTJs, in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017,606-609.
18. Y. Wang, H. Cai, L. A. B. Naviner, J. Klein, Y. Jianlei, and W. Zhao. A novel circuit design of true random number generator using magnetic tunnel junction, in 2016 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH),123-128 2016.
19. W. A. Gaviria Rojas, J. J. McMorrow, M. L. Geier, Q. Tang, C. H. Kim, T. J. Marks, et al. Solution-Processed Carbon Nanotube True Random Number Generator, Nano Letters, vol. 17, 4976-4981, 2017/08/09 2017.
20. L. Chua. Resistance switching memories are memristors, Applied Physics A, vol. 102, 765-783, 2011/03/01 2011.
21. L. Chua. Memristor-The missing circuit element, IEEE Transactions on Circuit Theory, vol. 18, 507-519, 1971.
22. M. A. Trefzer. Memristor in a Nutshell, in Guide to Unconventional Computing for Music, E. R. Miranda, Ed., ed Cham: Springer International Publishing, 2017, pp. 159-180.
23. L. O. Chua and K. Sung Mo. Memristive devices and systems, Proceedings of the IEEE, vol. 64, 209-223, 1976.

24. D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams. The missing memristor found, Nature, vol. 453, 80, 05/01/online 2008.
25. L. Ning, J. Ding, B. Chuang, and Z. Xuecheng. Design and validation of high speed true random number generators based on prime-length ring oscillators, The Journal of China Universities of Posts and Telecommunications, vol. 22, 1-6, 2015/08/01/ 2015.
26. A. R. e. al. 2010. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.
27. M. M. a. B. Sarkar. Ring oscillators: Characteristics and applications, Indian Journal of Pure and Applied Physics, vol. vol. 48, pp. 136-145, February 2010.
28. E. Zhou, L. Fang, and B. Yang. A general method to describe forgetting effect of memristors, Physics Letters A, vol. 383, 942-948, 2019/03/11/ 2019.
29. S. Hu, J. Yue, C. Jiang, X. Tang, X. Huang, Z. Du, et al. Resistive switching behavior and mechanism in flexible TiO2@Cf memristor crossbars, Ceramics International, 2019/02/12/ 2019.
30. S. Wen, X. Xie, Z. Yan, T. Huang, and Z. Zeng. General memristor with applications in multilayer neural networks, Neural Networks, vol. 103, 142-149, 2018/07/01/ 2018.

AUTHORS PROFILE

N A N Hashim, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.

J T H Loong, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.

F A Hamid, College of Engineering, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia.