Inverters with Different Loads for Ring Oscillators True Random Number Generator Analysis

Noor Alia Nor Hashim
College of Engineering,
Universiti Tenaga Nasional,
Kajang, Selangor, Malaysia
noor_alia@uniten.edu.my

Julius Teo Han Loong
College of Engineering,
Universiti Tenaga Nasional,
Kajang, Selangor, Malaysia
julius.teo@uniten.edu.my

Fazrena Azlee Hamid
College of Engineering,
Universiti Tenaga Nasional,
Kajang, Selangor, Malaysia
fazrena@uniten.edu.my

***Abstract*—There have been a multitude of security issues surfacing in hardware security at the moment. The hardware and software systems are exposed to a lot of multi-level attacks in the cryptography aspect. True random number generator (TRNG) can provide an answer to the issues by producing random and unpredictable keys or numbers that can be used in hardware and the transactions of the network. The way these random output are produced are through physical phenomenon that produces entropies that can be sampled by TRNG. This research provides an idea on how the performance of TRNG can be enhanced by creating a more random output. Nanoelectronics such as memristors have been adopted and explored to tackle the issues. The memristor has been implemented in the TRNG designs to analyze the performance results of the ouput. Different loads such as transistors, resistor and memristor have been used in the TRNG to investigate the effect on the performance of the TRNG. The TRNG design uses complementary metal oxide semiconductor (CMOS) technology of 0.18 µm and is simulated by LT SPICE IV. The TRNG design in 2nd scenario produces the best results and passed 10 out of 12 of the NIST tests compared to other scenarios.**

Keywords—true random number generator; memristor; ring oscillator; hardware security; nanoelectronics

I. INTRODUCTION

The hardware and software operations required high security in order to have safe and secure transactions between users. Cryptography plays an important role in ensuring a secure network is always achieved and maintained [1]. The increasing number of security attacks happening such as Trojans and side-channel assaults is worrying and any solutions should be explored further to tackle the problem. These security attacks can be minimized by updating algorithmic mechanisms adopted in the transactions with latest options that can ensure highest quality in hardware security. Nanoelectronics are one of the latest innovation in the traditional complementary metal oxide semiconductor (CMOS) processes to be developed as the security solutions [2]. True random number generator are widely accepted to be used to generate random outputs that can be used in the cryptography application of the network system [3].

A. True Random Number Generator

Random number generator (RNG) is suitable for cryptography because it generates unpredictable random output bits even though all specifications of the generator is known. There are two types of RNG which are true random number generator (TRNG) and pseudo random number generator (PRNG). TRNG are used in security due to the way it produces random outputs using entropies that exists in the physical processes of its circuits in a nondeterministic solution of generating true unpredictable keys [4, 5]. There are three circuit parts that comprises a TRNG which are called; the entropy source, harvesting mechanism and post processing [1]. Randomness that exists in the physical processes are extracted and the existing entropy in it is defined in the first circuit of the generator which are the entropy source. The entropy is sampled to generate the unique binary output without changing any physical process in the second circuit which are the harvesting mechanism.

B. Memristors

It was presented by Leon Chua that there is an equation that exists to define a relationship consisted of flux-linkage, φ and charge, q. Memristor is the missing component and the fourth basic two-terminal circuit element [6]. The definition of a memristor is that it is a circuit element that are of passive type that explains the link between the time integrals

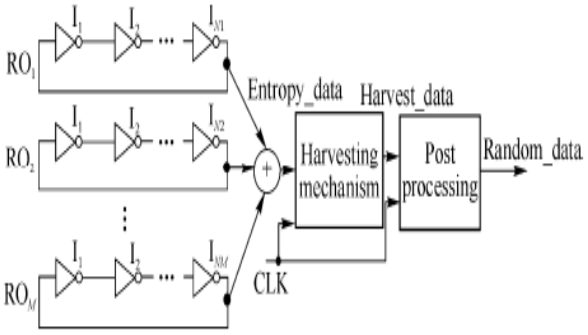

Fig. 1. True Random Number Generator [1]

of current and voltage across a two terminal element. It is one of the nanoelectronics components that are being investigated because it was believed that it has suitable characteristics that can be implemented as a replacement of CMOS technology. It was stated in [7] that it exudes behavior of non-linearity that can be control and having a more random process variations as in comparison with the CMOS processes. Besides that, memristors are constructed from a non-complex crossbar that contains two electrodes that are placed on the sides of an oxide layer. It can also reduces the area usage in the TRNG design due to the smaller size of memristors that requires smaller space and also power usage [8, 9]. . This paper will focus on three different loads to be used in the inverters of the TRNG and memristors represents nanoelectronics that are adopted in the design.

978-1-7281-0460-7/19/$31.00 ©2019 IEEE

II. METHODOLOGY

A. Entropy Source Circuit

This research are based on the TRNG design that was presented in [1] by Ning et.al. that uses a simple method and are all –digital circuits. The TRNG design consisted of inverters with different loads to build the ring oscillators of the entropy source circuit, a binary XOR-tree, harvesting mechanism and post processing circuits. CMOS technology of 0.18 µm was used in the TRNG design and the voltage supply was of 1.8 v. The main changes of the TRNG are in the entropy source circuit. 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 different loads are implemented in the inverters to build the ring oscillators (M-RO). The topology of the circuit is shown in Figure 2.

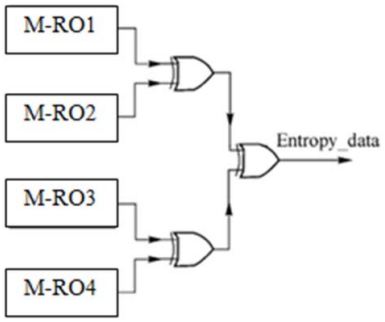

Fig. 2. The composition of the entropy source circuit that adopted memristor based ring oscillators

B. Harvesting Mechanism

The harvesting mechanism consisted of a modest arbiter that uses set/reset (SR) latch concept as shown in Figure 3. The concept of an SR latch contains two steady states that can retain the state information. Signals are applied to the control inputs and the arbiter can control its state and can produce a maximum of two outputs.

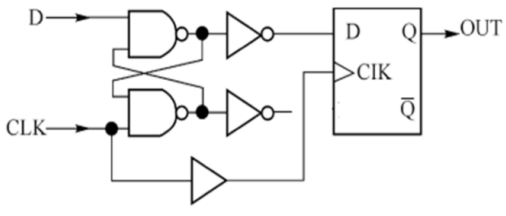

Fig. 3. Simple arbiter of SR latch of harvesting mechanism [1].

C. Post Processing

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 4.

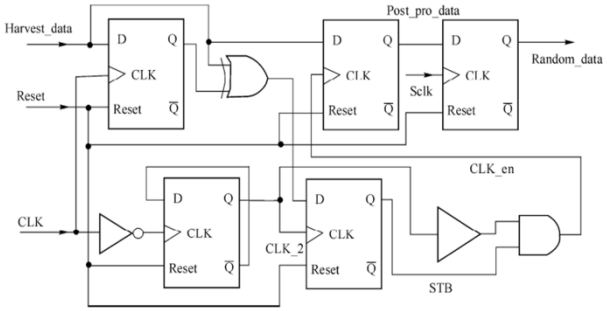

Fig. 4. Simple Von Neumann corrector [1].

Changes were made to the TRNG design to include different loads for the inverters to build the ring oscillators in the entropy source circuit. It is divided to three scenarios which are; 1st scenario: TRNG with inverters of NMOS and PMOS transistors, 2nd scenario: TRNG with common source with resistive load as inverters and 3rd Scenario: TRNG with common source with memristive load as inverters. The performance of the TRNG was evaluated based on the results of the NIST test suite.

D. Simulation Setup

The simulation setup of the TRNG design was by Linear Technology Corporation, LTspice IV and the CMOS technology are based on the Silterra 0.18 µm with a supply voltage of 1.8 v. Each of the scenario generates a maximum length of 10k bits to be compared. The software that was being used is by Microsoft Windows 7 with Intel i5 core operating at 2.67GHz and 4GB RAM. The gate width was set to 4.5 µm and the gate length was set to 1.8 µm.

E. Statistical Tests Evaluation

The performance results for each scenario was evaluated using the National Institute of Standards and Technology (NIST) test suite. In the test suite, it evaluates the binary number of bits that are generated by the TRNG by breaking down the different types of non-randomness that can exist in output bits. There are a total of 15 statistical tests in the test suite. The maximum length of the output bits was only up to 10k, therefore there are three test which are Maurer's "Universal Statistical" Test, Random Excursions Test and Random Excursions Variant Test that are not being used to evaluate the output bits produced. In total, the research will only focus 12 tests of the NIST test suite. The maximum length is a limitation of the computer processor that are only able to generate 10k bits due to the computer RAM of only 4GB.

III. RESULTS AND DISCUSSION

This section compiled the results of the statistical tests for the random output produced by the proposed TRNG design. It is divided to three scenarios which are; 1st scenario: TRNG with inverters of NMOS and PMOS transistors, 2nd scenario: TRNG with common source with resistive load as inverters

and 3rd scenario: TRNG with common source with memristive load as inverters. The statistical tests results are based on the results of NIST test suite.

TABLE I. NIST TESTS RESULTS FOR THE THREE SCENARIOS OF THE PROPOSED TRNG

Scenarios of Proposed TRNG	Total of tests passed									
	1k bits	2k bits	3k bits	4k bits	5k bits	6k bits	7k bits	8k bits	9k bits	10k bits
1st Scenario	6	8	7	7	7	7	7	6	7	7
2nd Scenario	6	10	10	10	10	10	9	9	9	9
3rd Scenario	6	10	10	10	8	7	7	6	5	6

Table 1 showed the NIST tests results for the three scenarios of the proposed TRNG. It can be seen that the best results are produced when the proposed TRNG adopts a common source with resistive load as inverters in 2nd scenario. Foe each scenario, the best results are produced when the output bits are in 2k data size length and the amount of passed tests slowly decreases as the bits become longer. When the data size is in 10k length, the 2nd scenario of the TRNG had the highest amount of passed tests of 9 tests compared to 1st scenario with 7 passed tests and 3rd scenario with 6 passed tests only.

This could be due to the small data size as some of the tests require the data size to be more than 10,000 bits. For each of the tests in the NIST test suite, there is an input requirement that needs to be met in order for all of the conditions of the tests are approved of the output bits. Some of the tests requires the data sizes to be in 1M length in order to be evaluated properly by the tests. The tests that was eliminated from the research required the data size to be larger than the maximum the the proposed TRNG was producing. The tests mentioned are Universal, Random Excursions and Random Excursions Variant. The p-value will be fixed to zero if the test is not valid [10]. Unfortunately the limitations of the computer processor RAM are not able to meet the requirements of all tests. Hence, only 12 tests were being used.

The 2nd scenario has the best results due to the resistive load being used which are considered stable compared to the other scenarios. Future research might consider using memristive load that is stable in order to produce more randomness that is stable in the output. It can be seen that using different loads in the inverters affects the performance results of the TRNG and this gives space for more research to explore the best load that can produce best performance results.

IV. CONCLUSION

This paper presents ring oscillators TRNG design that has been implemented with the 0.18 μm complementary metal oxide semiconductor (CMOS) technology using LT SPICE. Inverters with different loads were implemented in the proposed TRNG design and can be explored further to develop solutions in the security issues that have arised in the hardware and software operations. There are three different scenarios of the TRNG design which are 1st scenario: TRNG with inverters of NMOS and PMOS transistors, 2nd scenario: TRNG with common source with resistive load as inverters and 3rd Scenario: TRNG with common source with memristive load as inverters. The inverters are being used to construct the ring oscillators of the entropy source circuit of the TRNG. The best scenario with the best performance results belongs to 2nd scenario due to a resistive load being used. It is known that resistive load is more stable compared to the other loads and will produce a stable randomness in the output. The research can be further explored to include a more stable memristive load in the design to produce more randomness in the output bits produced.

ACKNOWLEDGMENT

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] 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, pp. 1-6, 2015/08/01 2015.

[2] R. K. J. Rajendran, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, et al., "Nano meets security: Exploring nanoelectronic devices for security applications," *Proceedings of the IEEE,* vol. 103, pp. 822-828, 2015.

[3] B. Valtchanov, V. Fischer, A. Aubert, and F. Bernard, "Characterization of randomness sources in ring oscillator-based true random number generators in FPGAs," in *13th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems*, 2010, pp. 48-53.

[4] M. Stipčević and Ç. K. Koç, "True Random Number Generators," in *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, Ed., ed Cham: Springer International Publishing, 2014, pp. 275-315.

[5] S. Robson, B. Leung, and G. Gong, "Truly Random Number Generator Based on a Ring Oscillator Utilizing Last Passage Time," *IEEE Transactions on Circuits and Systems II: Express Briefs,* vol. 61, pp. 937-941, 2014.

[6] L. Chua, "Memristor-The missing circuit element," *IEEE Transactions on Circuit Theory,* vol. 18, pp. 507-519, 1971.

[7] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *nature,* vol. 453, pp. 80-83, 2008.

[8] M. D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design & Test of Computers,* vol. 27, pp. 48-65, 2010.

[9] A. G. Radwan and M. E. Fouda, "Memristor: Models, Types, and Applications," in *On the Mathematical Modeling of Memristor, Memcapacitor, and Meminductor*, ed: Springer, 2015, pp. 13-49.

[10] M. Sýs, Z. Riha, V. Matyas, K. Marton, and A. Suciu, *On the interpretation of results from the NIST statistical test suite* vol. 18, 2015.