Indonesian Journal of Electrical Engineering and Computer Science
Vol. 13, No. 3, March 2019, pp. 892~901
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i3.pp892-901

Ring oscillator physically unclonable function using sequential ring oscillator pairs for more challenge-response-pairs

Julius Han Loong Teo, Noor Alia Nor Hashim, Azrul Ghazali, Fazrena Azlee Hamid
Department of Electrical and Communication Engineering, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Oct 25, 2018
Revised Dec 16, 2018
Accepted Dec 30, 2018

Keywords:

Memristor
Physically unclonable function
Ring oscillator

ABSTRACT

The ring oscillator physically unclonable function (ROPUF) is one of the several types of PUF that has great potential to be used for security purposes. An alternative ROPUF design is proposed with two major differences. Firstly, the memristor is included in the ring oscillators as it is claimed to produce a more random oscillation frequency. Other reasons are its memory-like properties and variable memristance, relative compatibility with CMOS, and small size. Secondly, a different method of generating the response is implemented whereby a sequence of selection of ring oscillator pairs are used to generate a multiple bit response, rather than using only one ring oscillator pair to generate a single bit response. This method significantly expands the set of challenge-response pairs. The proposed memristor-based ROPUF shows 48.57%, 51.43%, and 51.43% for uniqueness, uniformity, and bit-aliasing, respectively. Also, modelling by support vector machine (SVM) on the proposed memristor-based ROPUF only shows 61.95% accuracy, thereby indicating strong resistance against SVM.

Corresponding Author:

Julius Han Loong Teo,
Department of Electrical and Communication Engineering,
Universiti Tenaga Nasional,
Jalan IKRAM-UNITEN, 43001 Kajang, Selangor, Malaysia.
Email: juliusteo@live.com.my

1. INTRODUCTION

1.1. Physically Unclonable Function

The Physically Unclonable Function (PUF) is a circuit that has been regarded as an alternative to current for security measures [1-3]. PUFs are said to have its own unique and inherent property, analogous to humans having a unique set of fingerprints, from which security keys can be extracted and used for security purposes, such as the identification and authentication of an electronic device. This so-called unique and inherent property of the PUF is due to random and uncontrollable variations in the manufacturing process [4, 5]. Often, these variations are unwanted, particularly in the fabrication of chips, but the PUFs exploit these variations to have a circuit property that is unique from other circuits of the same type. With the security key being unique to and inherent within the PUF, the PUF can be used as an alternative to the storing of these keys in nonvolatile memory that can be easily attacked [6]. Also, tampering the PUF will very likely damage the circuit and its security key [7], rendering invasive attacks futile.

The input and output of a PUF are respectively termed as ‘challenge’ and ‘response’. A challenge sent to a PUF results in a response from the PUF, which is termed as challenge-response pair (CRP). The set of CRPs is considered as the unique property that distinguishes itself from other PUFs [1-3]. To date, there are a several PUF types being researched like the bistable ring PUF [8], the arbiter PUF [1-3], the SRAM PUF [9-11], crossbar array PUF [12-15], and the ring oscillator PUF (ROPUF) [5, 16-19], which is the type of PUF taken into discussion for this research.

1.2. Memory Resistor

Meanwhile, the memristor, short for "memory resistor", is said to be the fourth fundamental passive circuit element; the first three being the resistor, capacitor, and inductor. The idea of the memristor falls on one of the six possible pairwise relationships among four fundamental circuit variables, namely current i, voltage v, charge q, and flux linkage Φ. Chua, in 1971, claimed that the relationship between charge and flux linkage to be memristance [20-22]. Chua made this postulation for the sake of completeness because, at the time, the relationship between charge and flux linkage was the only pairwise relationship left that was not yet firmly understood. These pairwise relationships are visualized in Figure 1.

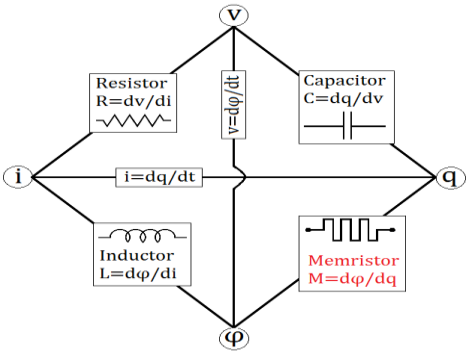

Figure 1. Mapping of the pairwise relationship of circuit variables

However, the actual physical memristor was only discovered in 2008 by a team of researchers in HP Labs [23, 24]. Their memristor structure simply consists of only two titanium dioxide, TiO_2 layers: undoped and doped with oxygen vacancies, denoted as TiO_{2-x} which are sandwiched between platinum electrodes. The structure of the memristor is shown in Figure 2, in which the length of the doped layer is labelled w, whereas the length of the memristor is labelled D. As a schematic, the memristor is represented as two series-connected variable resistors, as shown in Figure 3. The expression for the equivalent memristance, M is shown in (1), whereby memristance is simply resistance but only specifically for memristors. M_{ON} and M_{OFF} are the memristance at ON state or low resistance state (LRS) and OFF state or high resistance state (LRS), respectively. Simply put, M_{ON} and M_{OFF} are the maximum and minimum resistances, respectively.

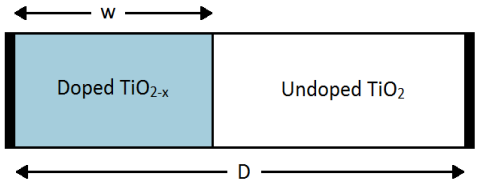

Figure 2. Structure of the HP memristor

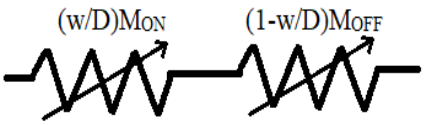

Figure 3. Circuit equivalent of the HP memristor

The memristance changes over time with respect to the polarity of the excitation signal, until it approaches M_{ON} or M_{OFF}. Furthermore, the memristance in retained once the excitation signal it is removed. This memory-like characteristic is where the name memory resistor comes from, and it is the most prominent characteristic that distinguishes itself from other circuit components.

The memory and varying memristance are due to the movement of the oxygen vacancies that are found in the doped titanium dioxide layer, TiO_{2-x}. The oxygen vacancies move, depending on the polarity of the excitation signal, and change the thickness of the doped titanium dioxide layer, w, which consequently change the overall memristance as expressed in (1) earlier. When the excitation is removed, w is no longer affected and is unchanged, and hence, the memristance is retained [23-27].

The change in memristance with respect to the excitation is nonlinear. In fact, the I-V plot of the memristor exhibits a hysteresis loop pinched at the origin when excited by a bipolar periodic signal, like a sinusoid, as shown in Figure 4. The pinched hysteresis loop reduces in area with increasing excitation frequency, until it reduces into a straight line [23-27].

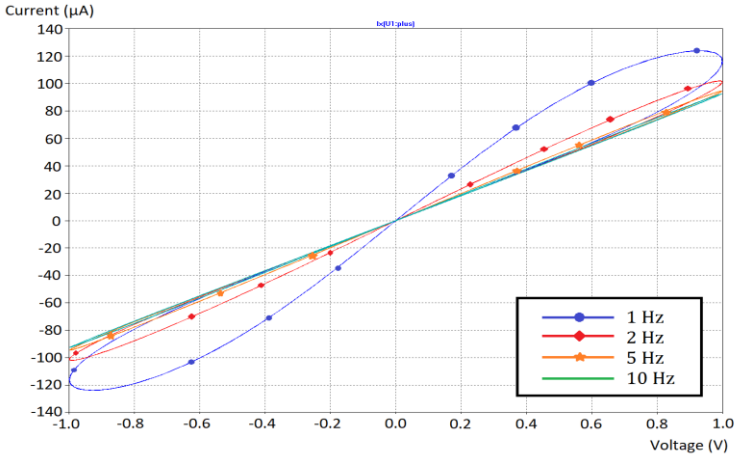

Figure 4. I-V plot of the memristor at various frequencies

The reasons for incorporating the memristor in the ROPUF are the memory-like property and variable memresistance. Also, the memristor manufacturing technology is said to be relatively compatible with the modern CMOS fabrication standards [28]. In addition, the memristor-based PUFs are said to be more resistant to modelling attacks than purely CMOS-based PUFs because memristors are bidirectional devices as compared to MOSFETs which are unidirectional [29]. Furthermore, the memristor length is typically in the tens of nanometers, which is much smaller than most CMOS components and can reduce ROPUF circuit area. For these reasons, research efforts have been made to include the memristor into different types of PUFs to enhance its performance as a hardware security device [28-34].

1.3. Ring Oscillator Physically Unclonable Function

The classical ring oscillator Physically Unclonable Function (ROPUF) was introduced by Suh and Devadas [5], as shown in Figure 5. The idea of the ROPUF is the comparison of the frequency between a selected pair of identical ROs to generate a response bit. Due to random and uncontrollable manufacturing process variations, there is a discrepancy in the delays of each inverting unit in the RO, consequently causing discrepancy in the oscillating frequency among identical ROs.

Generally, the ROPUF consists of k ROs, two k-to-1 multiplexers, two counters, and one comparator. The operation of the ROPUF can be simplified as follows. The challenge to the PUF is taken as the select inputs to both k-to-1 multiplexers, which selects a pair of ROs to be directed to the respective counters. The counters count the pulses within a certain duration, and finally the comparator compares both counter values with one another to generate a response bit. If one count value is higher than the other, then the response bit is logic-0, and vice versa.

There are ${}^{k}C_{2}$ possible pairs of ROs to generate ${}^{k}C_{2}$ single-bit responses. However, due to the occurrence of correlated response bits, the 1-out-of-p masking scheme was proposed. In this scheme, only one response bit is generated from a group of p ROs, where the two ROs that has the largest difference in oscillation frequency are compared [5]. Thus, the actual number of response bits is then calculated by k/p. While this scheme addresses the issue of correlated bits, it reduces the number of CRPs at the cost of increased hardware overhead.

Much research effort has been made to improve the ROPUF in terms of performance metrics, namely uniqueness, uniformity, bit-aliasing, and reliability; to increase the number of CRPs; or to simply reduce the size of the circuit. One example is the configurable ROPUF [16, 36-38] whereby the ROs can be configured by selecting the desired inverters in them. This method is done to improve performance metrics, particularly uniqueness and reliability, as well as to avoid using the 1-out-of-p masking scheme. The main drawback, however, is the increased overhead as a 2-to-1 multiplexer is required in every stage, or in other words, after every inverter in each RO.

Another ROPUF example is the design that has ROs with configurable duty cycles [17]. The duty cycle of the RO is configured by controlling the transistor width ratio and the number of stages. The comparison between two ROs can then be made from different nodes within the RO since the resultant oscillation frequency is now different due to altered duty cycles. The purpose of this design is to increase the

number of CRPs. However, this design increases hardware overhead as it requires two more m-to-1 multiplexers, where m is the number of stages in each RO.

The waveform ROPUF [18] uses another RO to sample the PUF's RO, because it has higher frequency (and sampling rate) than conventional clocks. Thus, response generation is sped up and power consumption is reduced. Meanwhile the random telegraphic noise (RTN) induced ROPUF improves reliability [19]. However, both ROPUFs have uniqueness values that are relatively low.

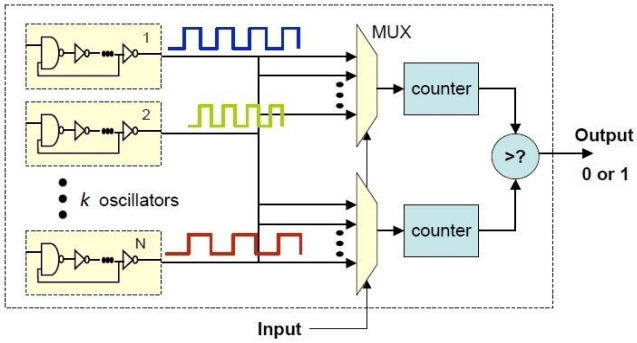

Figure 5. ROPUF by Suh and Devadas [5]

In this paper, the memristor is introduced in the inverting units of the ring oscillators (ROs) as it causes a more random oscillating frequency [35]. Furthermore, a different method in generating a response is proposed that significantly expands the CRP set with only a small number of ROs. It is also shown that the proposed method has good performance metrics and strong resistance to modelling attacks by support vector machine (SVM), which is one of the widely used machine learning algorithms today.

2. RESEARCH METHOD

2.1. Memristor in Ring Oscillator

The basic ring oscillator (RO) consists of an odd number of inverters or NOT gates that are looped in a ring, as its name suggests. In this paper, rather than using inverters (usually static CMOS) are replaced with common-source amplifiers with memristive load, as shown in Figure 6. The reasons for using this configuration are its relatively small size compared to CMOS components and more random oscillation frequency [35].

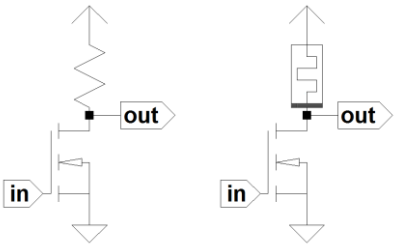

Figure 6. MOSFET common-source amplifier with resistive load (left) and memristive load (right)

2.2. Sequential Ring Oscillator Pairs

The generation of on response bit is made from the comparison of one pair of ROs. In addition, to overcome the issue of correlated bits, several methods have been proposed but at the cost of increased hardware overhead, while others do not significantly improve the performance metrics values.

In this research, it is proposed that the generation of the response is done by a sequence of selection of RO pair. In other words, the output bit from every RO pair, is arranged to form one ROPUF response. In this research, the number of ROs used in the simulation is eight i.e. k = 8 ROs. There are then ${}^{8}C_{2} = 28$ RO

pairs and thus, 28 output bits. These 28 output bits can be arranged in 28! ways, or roughly 3×10^{29} responses, which is an extremely large number. The challenge is then $\lceil \log_2(28!) \rceil = 98$ bits. An interfacing circuitry receives the challenge and then sequentially selects pairs of ROs for the generation of a 28-bit response. Therefore, with a small number of ROs, the number of CRPs is significantly large. Also, with a multiple-bit response as compared to a single-bit response, the difficulty in predicting a response is increased exponentially from 2 to 2^n.

2.3. Simulation Setup

The proposed memristor-based ROPUF, as shown in Figure 7, uses k = 8 ROs, where each RO consists of five stages, and each stage is the common-source amplifier with memristive load as described in Section III-A. The ROs are sent to a pair of 8-to-1 multiplexers. Each multiplexer output is sent to a counter. Both counter outputs are then sent to the comparator for the response bit generation.

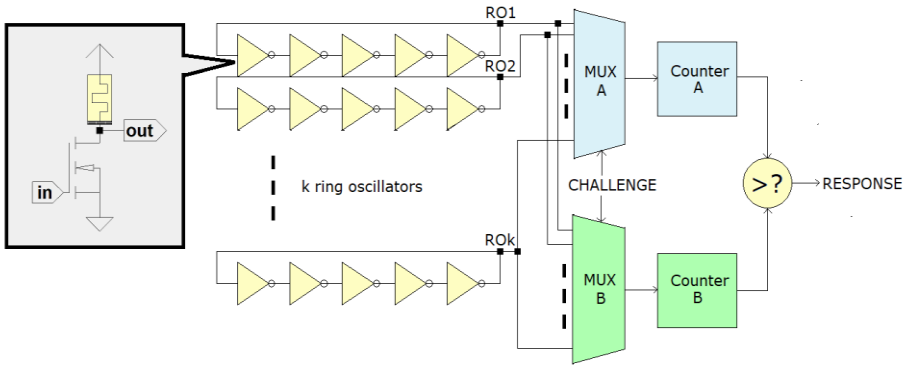

Figure 7. Proposed memristor-based ROPUF

Circuit simulations were performed on two SPICE simulators, namely LTspice IV by Linear Technology Corporation and Design Architect-IC (DA-IC) by Mentor Graphics Incorporated. For LTspice IV, SilTerra 180nm CMOS process with 1.8V supply voltage was used. As for DA-IC, SilTerra 130nm CMOS process with 1.2V supply voltage was used.

The memristor model used in the simulation is prepared by Biolek et al. as a SPICE subcircuit for transient analysis [39]. The memristor SPICE subcircuit was adapted where the memristor device parameters are shown in Table 1. To simulate the random and uncontrollable variations in the manufacturing process, 20% Monte Carlo variation was injected into the initial memresistance, M_{INIT}, and length of memristor, D.

Table 1. Memristor Parameters

Memristor parameter		Value
Resistance at ON state	M_{ON}	100 kΩ
Resistance at OFF state	M_{OFF}	16 kΩ
Initial resistance	M_{INIT}	11kΩ (±20%)
Length of memristor	D	10nm (±20%)
Migration coefficient	μ	$10fm^2/(V\cdot s)$
Boundary control parameter	p	10

2.4. ROPUF Evaluation Criteria

Detection of bias: There are a few aspects used to detect bias [40-42], but three commonly used metrics are taken into discussion, namely uniqueness, uniformity, and bit-aliasing, which have been derived by Maiti et al. [42]. The computation of these performance metrics was performed using MATLAB. To calculate these metrics, the following parameters are needed.

a) x – the number of PUF circuits in the set|
b) n – the number of bits in the PUF response
c) $HD(R_i,R_j)$ – the Hamming distance between two responses, R_i and R_j, which are of the same length

In general, Hamming distance between two strings is the number of positions that have different symbols or characters. It can only be applied between two strings that are of the same length. In the context

of this research, Hamming distance between two response stings is specifically the number of bit-positions that do not have the same bit.

Uniqueness estimates the ability of a PUF type to uniquely distinguish one circuit from another. In other research literature, uniqueness is termed as inter-chip variation or inter-chip Hamming Distance (inter-HD). Uniqueness is calculated by averaging all Hamming distances of all possible pairs of responses for the same applied challenge. The expression for calculating uniqueness is shown in (2). The ideal value is 50%.

$$\text{Uniqueness} = \frac{1}{\binom{x}{2}} \sum_{i=1}^{x-1} \sum_{j=i+1}^{x} \frac{HD(R_i, R_j)}{n} \times 100\% \quad (2)$$

Uniformity measures the proportion of logic-0s and logic-1s in a response of each PUF. This metric indicates whether there is bias within the response. For the same applied challenge, let $r_{i,j}$ be the j^{th} bit of the i^{th} response (R_i) that is n bits long, then the mathematical expression for calculating uniformity of the i^{th} PUF circuit is given by (3). The ideal value is also 50%; a result that is less than 50% indicates a higher proportion of logic-0s whereas a result that is more than 50% indicates a higher proportion of logic-1s for that response. The overall uniformity of the PUF type can be obtained by simply averaging each uniformity value over the number of responses, x.

$$\text{Uniformity} = \frac{1}{n} \sum_{j=1}^{n} r_{i,j} \times 100\% \quad (3)$$

Bit-aliasing estimates the tendency of the PUFs to generate identical responses, which is an unwanted effect. In other words, bit-aliasing measures the affinity of a bit position in a response towards either logic-0 or logic-1. By letting $r_{i,j}$ be the j^{th} bit of the i^{th} response (R_i) that is n bits long, the mathematical expression for calculating the bit-aliasing at the j^{th} bit position is shown in (4). Like uniformity, the ideal value is 50% where a result that is less than 50% indicates a higher proportion of logic-0s and a result that is greater than 50% indicates a higher proportion on logic-1s for that bit position. The overall bit-aliasing of the PUF type can be obtained by simply averaging each bit-aliasing value over the number of response bits, n.

$$\text{Bit-aliasing} = \frac{1}{x} \sum_{i=1}^{x} r_{i,j} \times 100\% \quad (4)$$

Resistance to SVM: Another criterion to evaluate the PUF is regarding its ability to resist modelling attacks, particularly by machine learning algorithms. In this research, the machine learning algorithm that was taken into consideration is SVM. The training and testing of the CRPs were performed using the LIBSVM package in MATLAB, which is made available online [43]. Although the CRP set of the proposed ROPUF is significantly large, training and testing the whole set would take a considerably long time. Hence, due to this computational constraint, only 1024 CRPs are used, which were taken from the first ten challenge bits. The training set sizes used are 20% and 50% of the CRP subset. Then, the rest of the CRP subset is used for testing. Similarly, the CRP pairs to be trained are chosen at random. The expected modelling accuracy is 50%, which is the probability of obtaining one out of two equally possible outcomes, like a fair coin toss. In the context of this research, the two outcomes are simply logic-0 and logic-1.

3. RESULTS AND ANALYSIS

3.1. Detection of Bias

Table 2 shows the results of the proposed memristor-based ROPUF in terms of uniqueness, uniformity, and bit-aliasing, in comparison with a few other ROPUF design in the literature. Take note that some information, particularly on performance metric values are not applicable or not available in the respective literature, and thus are labelled 'N/A'. This is because their primary aspect of evaluation of their ROPUFs is on uniqueness or inter-HD.

The results for both 180nm at 1.8 V and 130nm at 1.2V show performance metric values that are very close to one another, indicating consistency regardless of the circuit simulator, CMOS process, and supply voltage used. More importantly, the performance metric values for both circuit simulators are very close to the ideal 50% value. Thus, the proposed memristor-based ROPUF show good performance, implying that it is a well-functioning PUF.

In contrast to most of the other ROPUF designs, the proposed memristor-based ROPUF show better performance metric results than [5, 16, 18, 19] especially in terms of uniqueness. In contrast to [17], the results are comparable to another. Most of the other research efforts improve certain aspects but forgo

others, such as improving performance speed and reliability against voltage changes but at the expense of reducing uniqueness [18, 19].

The primary advantage of this design is that it only uses very few ROs to produce a very large number of CRPs. The idea is that a sequence of all the possible pairs of ROs is used to generate a multiple-bit response, rather than using one pair of ROs for a single-bit response. Nevertheless, it is also possible to use only a subset of the possible pairs of ROs, especially when the number of ROs used is large. While there are other methods that have been proposed to increase the CRP set and improve uniqueness, it is not as effective as the method proposed in this paper.

Table 2. Performance Metric Results

ROPUF	Number of ROs	Number of CRPs	Performance metric (%)		
			Uniqueness	Uniformity	Bit-aliasing
Classical [5]	1024	128	46.15	N/A	N/A
Gao et al. [16]	32	16	46.79	N/A	N/A
Agustin et al. [17]	128	2048	49.41	48.13	52.10
Tanamoto [18]	24	N/A	42.20	46.74	N/A
Yoshinaga et al. [19]	256	128	48	N/A	N/A
Proposed (180nm, 1.8V)	8	3×10^{29}	48.57	51.43	51.43
Proposed (130nm, 1.2V)	8	3×10^{29}	51.36	49.49	48.81

3.2. Resistance to SVM

Table 3 shows the modelling accuracy by SVM on the proposed memristor-based ROPUF. Although the modelling accuracy is not very close to the ideal 50%, the values are acceptable as the SVM is still unable to accurately predict the responses for both 20% and 50% training sizes. In addition, this result is comparable to a previous research effort on the ROPUF that was also tested with SVM, whereby the highest prediction accuracy obtained was only 60.9% [44]. In fact, the results are much better in contrast to the classical arbiter PUF, a different type of PUF, which showed up to 99% modeling accuracy [45-48], and thus indicate high vulnerability to modelling attacks. Therefore, the results indicate that the proposed memristor-based ROPUF is resistant to attacks by SVM.

Table 3. SVM Modelling Accuracy

Training size (%)	20	50
Modelling accuracy (%)	61.95	58.59

4. CONCLUSION

In short, two main changes on the ROPUF are proposed. The first change is the inclusion of the memristor in the inverting units of the RO. This is because the memristor is smaller than most CMOS components, thereby reducing circuit size and power consumption. Furthermore, it is claimed that the memristor is relatively compatible with CMOS fabrication standards. The second change is the method of generating the response of the PUF. In other ROPUF designs, one pair of RO generates one response bit; but in the proposed memristor-based ROPUF, one sequence of RO pairs generates one multibit response. This method significantly expands the CRP set list without extensive circuit overhead. The results in terms of uniqueness, uniformity, and bit-aliasing show that the proposed memristor-based ROPUF have little bias in the response. Also, SVM is unable to accurately model the behavior of the proposed memristor-based ROPUF, thereby the ROPUF is resistant to attacks by SVM. In conclusion, the proposed memristor-based ROPUF is a simple yet robust PUF design.

As for future research plans, the proposed memristor-based ROPUF is to undergo further testing and validation, such as voltage and temperature reliability, randomness test like the NIST test suite, and modeling attacks using other machine learning algorithms. Eventually, the ROPUF is to be fabricated and implemented as an actual physical hardware device for security purposes.

ACKNOWLEDGEMENTS

This research is supported by the Fundamental Research Grant Scheme (FRGS) under the project code FRGS/1/2015/TK04/UNITEN/02/2, which has been awarded by the Ministry of Higher Education, Malaysia, and by the Universiti Tenaga Nasional (UNITEN) Internal Grant under the project code J510050761. Also, many thanks to all colleagues in UNITEN for their insight and support.

REFERENCES

[1] B. Gassend, D. Clarke, M. v. Dijk, and S. Devadas, "Silicon physical random functions," presented at the Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, 2002.

[2] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, 2004, pp. 176-179.

[3] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. v. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, pp. 1200-1205, 2005.

[4] U. Ruhrmair and D. E. Holcomb, "PUFs at a glance," presented at the Proceedings of the conference on Design, Automation & Test in Europe, Dresden, Germany, 2014.

[5] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," presented at the Proceedings of the 44th annual Design Automation Conference, San Diego, California, 2007.

[6] R. J. Anderson, *Security Engineering: A guide to building dependable and distributed systems*, John Wiley and Sons, 2001.

[7] L. Feiten, J. Oesterle, T. Martin, M. Sauer, and B. Becker, "Systemic Frequency Biases in Ring Oscillator PUFs on FPGAs," *IEEE Transactions on Multi-Scale Computing Systems*, vol. PP, pp. 1-1, 2016.

[8] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair, "The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, 2011, pp. 134-141.

[9] J. W. Jang and S. Ghosh, "Design and analysis of novel SRAM PUFs with embedded latch for robustness," in *Sixteenth International Symposium on Quality Electronic Design*, 2015, pp. 298-302.

[10] L. Kusters, T. Ignatenko, F. M. J. Willems, R. Maes, E. v. d. Sluis, and G. Selimis, "Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios," in *2017 IEEE International Symposium on Information Theory (ISIT)*, 2017, pp. 1803-1807.

[11] E. I. Vatajelu, G. D. Natale, and P. Prinetto, "Towards a highly reliable SRAM-based PUFs," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2016, pp. 273-276.

[12] G. S. Rose and C. A. Meade, "Performance analysis of a memristive crossbar PUF design," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6.

[13] M. Uddin, M. B. Majumder, G. S. Rose, K. Beckmann, H. Manem, Z. Alamgir, *et al.*, "Techniques for Improved Reliability in Memristive Crossbar PUF Circuits," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2016, pp. 212-217.

[14] M. Uddin, M. B. Majumder, and G. S. Rose, "Robustness Analysis of a Memristive Crossbar PUF Against Modeling Attacks," *IEEE Transactions on Nanotechnology*, vol. 16, pp. 396-405, 2017.

[15] G. S. Rose, M. B. Majumder, and M. Uddin, "Exploiting Memristive Crossbar Memories as Dual-Use Security Primitives in IoT Devices," in *2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2017, pp. 615-620.

[16] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014, pp. 1-6.

[17] J. Agustin and M. L. Lopez-Vallejo, "A temperature-independent PUF with a configurable duty cycle of CMOS ring oscillators," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 2471-2474.

[18] T. Tanamoto, S. Yasuda, S. Takaya, and S. Fujita, "Physically Unclonable Function using Initial Waveform of Ring Oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. PP, pp. 1-1, 2016.

[19] M. Yoshinaga, H. Awano, M. Hiromoto, and T. Sato, "Physically unclonable function using RTN-induced delay fluctuation in ring oscillators," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 2619-2622.

[20] L. O. Chua, "Memristor - the missing circuit element," *IEEE Trans. Circuit Theory*, vol. 18, pp. 507-519, // 1971.

[21] L. O. Chua and S. M. Kang, "Memristive devices and systems," *Proc. IEEE*, vol. 64, pp. 209-223, // 1976.

[22] L. Chua, "Resistance switching memories are memristors," *Applied Physics A*, vol. 102, pp. 765-783, 2011.

[23] R. S. Williams, "How We Found The Missing Memristor," *IEEE Spectrum*, vol. 45, pp. 28-35, 2008.

[24] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, pp. 80-83, 05/01/print 2008.

[25] 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.

[26] P. Mazumder, S.-M. Kang, and R. Waser, "Memristors: devices, models, and applications," *Proceedings of the IEEE*, vol. 100, pp. 1911-1919, 2012.

[27] T. Prodromakis and C. Toumazou, "A review on memristive devices and applications," in Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on, 2010, pp. 934-937.

[28] G. S. Rose, N. McDonald, L. K. Yan, B. Wysocki, and K. Xu, "Foundations of memristor based PUF architectures," in *2013 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, 2013, pp. 52-57.

[29] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan, "A novel memristor based physically unclonable function," Integr. VLSI J., vol. 51, pp. 37-45, 2015.

[30] G. S. Rose, N. McDonald, L. K. Yan, and B. Wysocki, "A write-time based memristive PUF for hardware security applications," in 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013, pp. 830-833.

[31] M. Uddin, M. B. Majumder, G. S. Rose, K. Beckmann, H. Manem, Z. Alamgir, et al., "Techniques for Improved Reliability in Memristive Crossbar PUF Circuits," in 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016, pp. 212-217.
[32] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, "Nano-PPUF: A memristor-based security primitive," in *2012 IEEE Computer Society Annual Symposium on VLSI*, 2012, pp. 84-87.
[33] A. Mazady, M. T. Rahman, D. Forte, and M. Anwar, "Memristor puf—a security primitive: Theory and experiment," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, pp. 222-229, 2015.
[34] Koeberl, P., et al. (2013). Memristor PUFs: A new generation of memory-based Physically Unclonable Functions. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013.
[35] N. A. N. Hashim, J. H. L. Teo, M. S. Hamid, and F. A. Hamid, "Analysis of Memristor-based Ring Oscillator Random Number Generator," presented at the 12th IEEE International Conference on Semiconductor Electronics (ICSE), Kuala Lumpur, 2016.
[36] X. Xin, J.-P. Kaps, and K. Gaj, "A Configurable Ring-Oscillator-Based PUF for Xilinx FPGAs," presented at the Proceedings of the 2011 14th Euromicro Conference on Digital System Design, 2011.
[37] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *2009 International Conference on Field Programmable Logic and Applications*, 2009, pp. 703-707.
[38] M. Choudhury, N. Pundir, M. Niamat, and M. Mustapa, "Analysis of a novel stage configurable ROPUF design," in *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2017, pp. 942-945.
[39] Z. Biolek, V. Biolkova, and D. Biolek, "SPICE model of memristor with nonlinear dopant drift," *Radioengineering*, 2009.
[40] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing techniques for hardware security," in 2008 IEEE International Test Conference, 2008, pp. 1-10.
[41] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in 2010 International Conference on Reconfigurable Computing and FPGAs, 2010, pp. 298-303.
[42] A. Maiti, V. Gunreddy, and P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," *IACR ePrint*, vol. 657, 2011.
[43] C.-C. Chang and C.-J. Lin, "LIBSVM: A Library for support vector machines," *ACM Trans. Intelligent Systems and Technology*, vol. 2, pp. 27:1-27:27, 2011.
[44] M. Mustapa, "PUF based FPGAs for hardware security and trust," Doctor of Philosophy, University of Toledo, 2015.
[45] J. Delvaux and I. Verbauwhede, "Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise," in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, 2013, pp. 137-142.
[46] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237-249.
[47] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 37-42.
[48] U. Chatterjee, R. S. Chakraborty, H. Kapoor, and D. Mukhopadhyay, "Theory and Application of Delay Constraints in Arbiter PUF," *ACM Trans. Embed. Comput. Syst.*, vol. 15, pp. 1-20, 2016.

BIOGRAPHIES OF AUTHORS

Julius Han Loong Teo received the B.Eng in Electrical and Electronics engineering from Universiti Tenaga Nasional, Malaysia in 2016 and subsequently the M.Eng degree in 2018 in the same university. He was a research assistant with the Electronics and Communication Engineering Department in Universiti Tenaga Nasional. His research interests include memristor application and IC design.

Noor Alia Nor Hashim was born in Kuala Lumpur, Malaysia in 1986. She received her B.Eng in electrical and electronics engineering from Universiti Tenaga Nasional, Malaysia in 2009. She is also currently pursuing the M.Eng degree in the same university.
She is currently with the Electronics and Communication Engineering Department in Universiti Tenaga Nasional as a research assistant. Her research involves memristors and random number generators.

	Azrul Ghazali received the B.Eng in electrical engineering from Vanderbilt University, USA in 1998 and the M.Sc in Microelectronics from Universiti Kebangsaan Malaysia, Malaysia in 2003. He is currently a senior lecturer in the Electronics and Communication Engineering Department in Universiti Tenaga Nasional, Malaysia. His reseach interests include IC design, VLSI, and microelectronics.
	Fazrena Azlee Hamid received the B.Tech diploma in engineering from Coventry Technical College, UK in 1996, followed with the B.Eng and Ph.D degrees in electronics engineering from University of Southampton, UK in 1999 and 2004, respectively. She is working as a senior lecturer with the Electronics and Communication Engineering Department in Universiti Tenaga Nasional, Malaysia. Her research is currently funded by the Ministry of Higher Education. Her research interests include IC design and optimization as well as memristor modelling and applications for hardware security.