Bulletin of Electrical Engineering and Informatics
Vol. 8, No. 1, March 2019, pp. 74~82
ISSN: 2302-9285, DOI: 10.11591/eei.v8i1.1401

Configurations of memristor-based APUF for improved performance

Julius Han Loong Teo, Noor Alia Noor Hashim, Azrul Ghazali, Fazrena Azlee Hamid
Electronics and Communication Department, College of Engineering, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Oct 14, 2018
Revised Nov 16, 2018
Accepted Dec 18, 2018

Keywords:

Arbiter
Memristor
Physically unclonable function

ABSTRACT

The memristor-based arbiter PUF (APUF) has great potential to be used for hardware security purposes. Its advantage is in its challenge-dependent delays, which cannot be modeled by machine learning algorithms. In this paper, further improvement is proposed, which are circuit configurations to the memristor-based APUF. Two configuration aspects were introduced namely varying the number of memristor per transistor, and the number of challenge and response bits. The purpose of the configurations is to introduce additional variation to the PUF, thereby improve PUF performance in terms of uniqueness, uniformity, and bit-aliasing; as well as resistance against support vector machine (SVM). Monte Carlo simulations were carried out on 180 nm and 130 nm, where both CMOS technologies have produced uniqueness, uniformity, and bit-aliasing values close to the ideal 50%; as well as SVM prediction accuracies no higher than 52.3%, therefore indicating excellent PUF performance.

Corresponding Author:

Julius Han Loong Teo,
Electronics and Communication Department,
College of Engineering, Universiti Tenaga Nasional,
Jalan Ikram-Uniten, 43001 Kajang, Selangor, Malaysia.
Email: juliusteo@live.com.my

1. INTRODUCTION

1.1. Memory resistor

The memristor, short for "memory resistor", is 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: current i, voltage v, charge q, and flux linkage Φ. Chua, in 1971, claimed that the q–Φ relationship is memristance, M [1-3] because, at the time, it was the only pairwise relationship left that was not yet firmly understood. These pairwise relationships are visualized in Figure 1 (left). Memristance, M, is simply resistance specifically for memristors, and is measured in ohms, Ω.

However, the actual memristor was only found in 2008 by HP Labs in their research for a suitable switch in their crossbar array [4, 5]. Their discovered memristor is made up of two layers of titanium dioxide, TiO2, where one layer is doped with oxygen vacancies, denoted as TiO2-x. The length of the doped layer is labelled w, whereas the length of the memristor is labelled D, where D is typically 10 nm. The structure of the memristor is shown in Figure 1 (right).

The memristor, as the name suggests, is a resistor with memory. Once the voltage across it is removed, the memristance at that time instance is retained. Also, the memristance increases over time until the maximum memristance, MOFF when connected at one polarity; and until the minimum memristance, MON at reverse polarity. The applied signal causes the oxygen vacancies in TiO2-x to move, whose direction depends on the polarity. Consequently, w changes and causes M to change as well. When the signal is removed, w is unchanged, and hence, M is retained [1-8]. The current-voltage i-v plot of the memristor

exhibits a pinched hysteresis loop when a sine signal is applied, as shown in Figure 2. The loop area shrinks with increasing frequency, and eventually reduces into a line as the frequency approaches infinity [1-8].

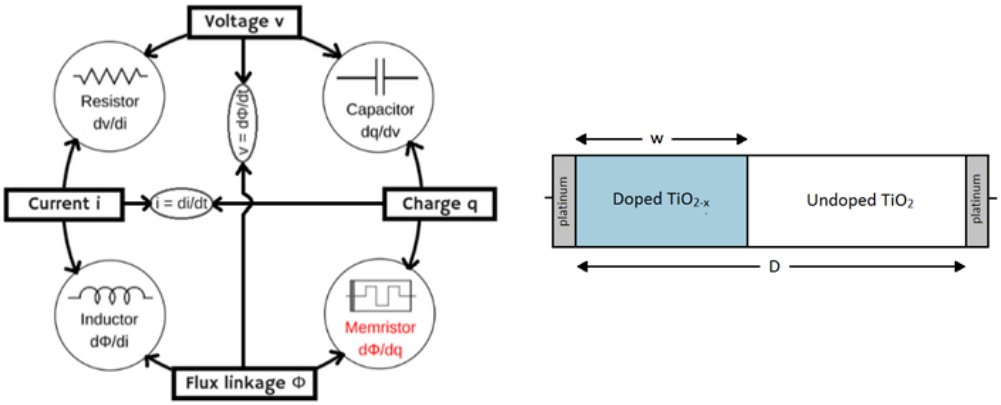

Figure 1. Pairwise relationship of the four circuit variables (left) and structure of HP memristor (right)

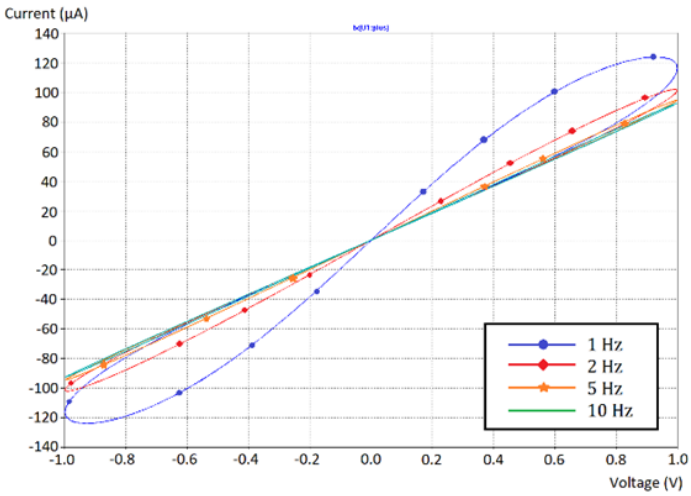

Figure 2. I-V plot of the memristor

The memristor is incorporated in PUF designs because of its memory-like properties and ability to change its memresistance which creates additional variation. Also, the memristor manufacturing technology is said to be relatively compatible with the modern CMOS fabrication standards [9]. In addition, the memristor-based PUFs have been conjectured to be more resistant to model building attacks than purely CMOS-based PUFs, because memristors are bidirectional devices as compared to the unidirectional MOSFET [10]. The memristor, roughly tens of nanometers long, is much smaller than most CMOS components and thus, reduces the area of the PUF. Hence, besides the APUF, other research efforts have been made to incorporate the memristor into different types of PUFs to enhance its performance [9-15].

1.2. Memristor based arbiter PUF

The Physically Unclonable Function (PUF) was introduced for hardware security purposes [16-18]. The name PUF suggests that it is a physical circuit, which cannot be perfectly duplicated, that uniquely maps inputs to outputs. The input and output are termed as “challenge” and “response”, respectively. One mapping of a challenge to a response is termed as “challenge-response pair” (CRP). The PUF exploits manufacturing variations to have CRPs that are unpredictable (but repeatable), which are like unique “fingerprints”. This

unique “fingerprint” is inherent in the PUF circuitry and needs not be stored in memory. Hence, the PUF is used as an alternative to storing keys in nonvolatile memory in security applications like the identification and authentication of a device [19-21].

One PUF example is the memristor-based arbiter PUF (APUF), which was initially introduced by Mathew et al. [22] in Figure 3 (left). The advantage of this APUF over the traditional APUF is its challenge-dependent path delays which makes modelling by machine learning algorithms like SVM and LR infeasible [22]. The traditional APUF showed vulnerability such attacks up to 99% prediction accuracy [23-25].

Although the circuit design by Mathew et al. is resistant to attacks by machine learning algorithms, it was found to be susceptible to attacks by cryptanalysis, which was pointed out and circumvented by Chatterjee et al. by changing the transistor connection in the delay paths [26], as shown in Figure 3. Thus, the newer design has all its memristors affected in the challenge application stage, unlike the previous design where, depending on the challenge, only a subset of the memristors are affected.

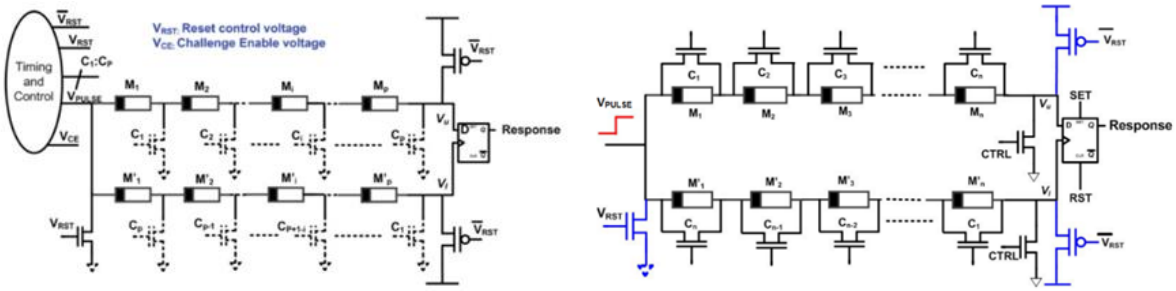

Figure 3. Memristor-based APUF by mathew et al. [22] (left) and by chatterjee et al. [26] (right)

Teo et al. made two modifications on the circuit design, which are adding arbiters to increase the number of response bits and replacing the D flip-flop with a SR NAND latch as the arbiter [27], as shown in Figure 4. The first modification is done because the SR NAND latch, compared to the D flip-flop has better input-to-output path symmetry, which reduces bias in the response generation. Also, the SR NAND latch is a simpler and smaller circuit component than the D flip-flop. As for the second modification, adding more response bits makes computing the response of the APUF more difficult, or at the very least, more time-consuming. Increasing the number of response bits from 1 to n results in the increase of the number of possible responses from 2 to 2n.

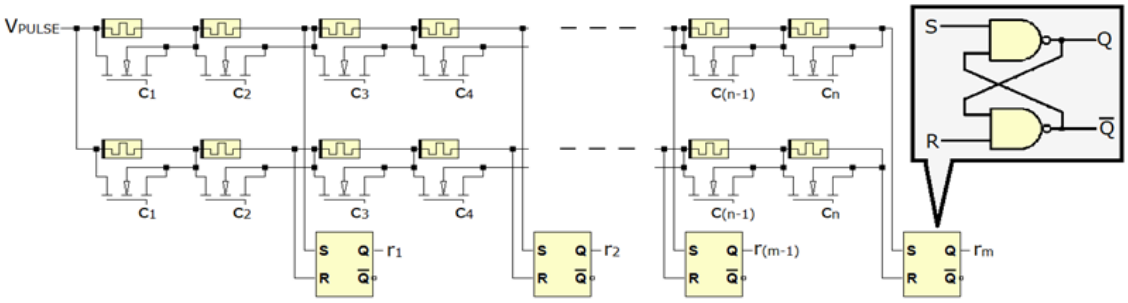

Figure 4. Memristor-based APUF by Teo et al. [27]

The operation of the memristor-based APUF can be briefly described in four stages [22, 26-27].

a. Reset: A reset signal, VRST, is set to 1. VRST is applied across all memristors to cause each memristor to be in its random initial memristance, which is dependent on the variations inherited in the manufacturing process.
b. Challenge application: VRST is set to 0. A pulse signal, VPULSE, and the challenge voltages are set to 1. Each memristor’s memristance is altered in such a way that it is dependent on the applied challenge.

Also, a control signal, VCTRL, is set to 1 to prevent the voltage at the input of the arbiters to rise and generate a false response bit.

c. Signal propagation: After a sufficient period, VCTRL is set to 0 to allow VPULSE to propagate to the arbiters.

d. Response generation: Depending on which of the two delay paths does the signal propagate faster, the output of the arbiter either maintains at 1 or toggles to 0, which is taken as the PUF response.

Based on the previous memristor-based APUF designs, further modifications can be made on the memristor-based APUF. Therefore, in this paper, circuit configurations are proposed as a means for increased variation and thereby, improve its performance in terms of uniqueness, uniformity, and bit-aliasing as well as resistance to SVM.

2. RESEARCH METHOD

2.1. Memristor-based APUF configurations

Configurations on the circuit of the memristor-based APUF are proposed simply to increase variation, thereby improve uniqueness and increase difficulty in duplication. The circuit designer may set the circuit of the memristor-based APUF to any desired, or even random, configuration so that it will be even more difficult for an adversary to duplicate the APUF without discovering the actual configuration. Take for example two APUFs that are both designed to be m-bit challenge and n-bit response. However, one of the APUFs may have more memristors per transistor, which has longer path delays than the other. Thus, both APUFs are more distinct from one another, besides already having variations due to the manufacturing process variations. In this paper, two configurations were made on the memristor-based APUF from two variables, which are number of memristors per transistor, and number of challenge and response bits.

The first configuration is varying the number of memristors per transistor. In other words, additional memristors are included in series between the source and drain terminals of each transistor. The memristor-based APUF was simulated from one to five memristors per transistor, where five memristors per transistor is shown in Figure 5. Each memristor added is subjected to manufacturing variations and thus, uniqueness can be improved.

As for the second configuration, the number of challenge bits is varied at 8, 16, and 32 bits, whereas the number of response bits is varied at 4 and 8 bits. Thus, there are a total of six possible combinations of challenge bits to response bits. The placement of the arbiters is spread out evenly along the delay paths. The position of the arbiters can be determined by simply dividing the number of challenge bits by the number of response bits. As an example, for 32 challenge bits and 4 response bits, the arbiters are placed on the delay paths after every eight transistors, as shown in Figure 6. For simulations in configuration 2, the number of memristor per transistor was fixed at one.

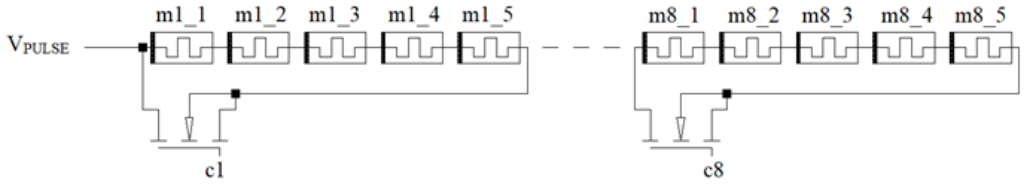

Figure 5. Example of configuration 1: 5 memristor per transistor

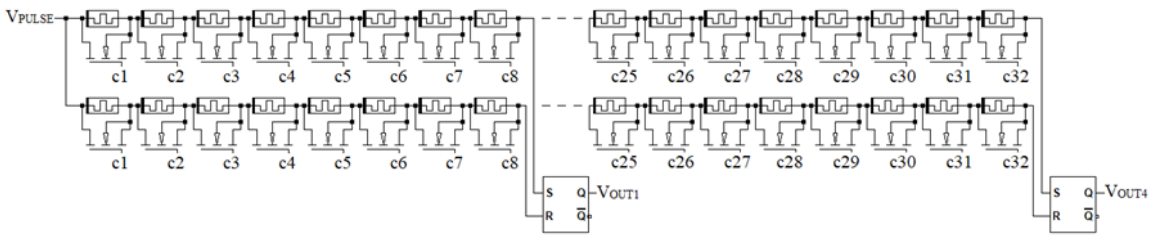

Figure 6. Example of configuration 2: 32-bit challenge, 4-bit response

2.2. Simulation setup

The circuit simulations were performed using SilTerra's 180nm at 1.8V and 130nm at 1.2V to observe any effect on the APUF performance. The memristor-based APUF circuit is based on Teo et al. [27]. The memristor SPICE circuit used is by Biolek et al. [28] with parameters shown in Table 1. The initial memresistance, MINIT, and the length of the memristor, D, were chosen as sources of manufacturing variation, set at 20% Monte Carlo variation of 5000 runs, similar to that performed in [22, 26, 27].

Table 1. Memristor simulation 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

2.3. PUF performance metrics

The performance of the proposed memristor-based APUF is evaluated on uniqueness, uniformity, and bit-aliasing, which are metrics that have been derived by Maiti et al. [29]. The metrics were computed in MATLAB, where the following parameters are used.

a. x: number of PUF circuits tested
b. n: number of response bits
c. HD (Ri,Rj): Hamming distance of responses, Ri and Rj (where i and j are indexes)

Uniqueness estimates the ability of a PUF type to uniquely distinguish one circuit from another. Uniqueness is calculated by averaging all Hamming distances of all possible pairs of responses for the same applied challenge. The equation for uniqueness is shown in (1). The ideal value is 50% [29].

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

Uniformity measures the proportion of 0s and 1s of a PUF response, which indicates the presence of bias within the response. For the same applied challenge, let ri, j be the jth bit of the ith n-bit response (Ri), then the equation for calculating uniformity of the ith PUF circuit is given by (2). The ideal value is 50% to show a balanced proportion of 0s and 1s for one response [29].

$$Uniformity = \frac{1}{n} \sum_{j=1}^{n} r_{i,j} \times 100\% \quad (2)$$

Bit-aliasing measures the proportion of 0s and 1s for one bit-position of the responses. By letting ri, j be the jth bit of the ith n-bit response (Ri), the equation for calculating the bit-aliasing at the jth bit position is given by (2). The ideal value is 50% to show a balanced proportion of 0s and 1s for one bit position [29].

$$Bit - aliasing = \frac{1}{x} \sum_{i=1}^{x} r_{i,j} \times 100\% \quad (3)$$

2.4. Support Vector Machine (SVM)

Support vector machine (SVM), one of the widely used machine learning algorithms, is generally used to classify data. In the context of this research, SVM attempts to model the behavior of the memristor-based APUF. The SVM trains on a given subset of the CRPs, and then runs tests by predicting the rest of the CRPs. A good PUF should be able to resist being accurately predicted by any modeling attacks, and thus the desired outcome is 50% prediction accuracy, indicating that the SVM appears to be randomly guessing between 0 and 1, which is a sign that it cannot model the APUF. The training and testing of the CRPs were performed using the LIBSVM package [30]. The training set size was 50% of the CRP set, which were chosen at random and then, the rest of the CRP set is used for testing.

3. RESULTS AND ANALYSIS

3.1. Performance metrics

The simulation results of the memristor-based APUF for Configuration 1 on 180nm at 1.8V and 130nm at 1.2V are shown in Tables 2 and 3., respectively.

Table 2. Simulation results for configuration 1 on 180nm at 1.8V

No. of memristor per transistor	Performance metric (%)		
	Uniqueness	Uniformity	Bit-aliasing
1	49.998	49.940	49.938
2	50.008	49.795	49.900
3	49.995	50.310	50.344
4	46.886	50.335	50.388
5	50.011	49.905	50.088

Table 3. Simulation results for configuration 1 on 130nm at 1.2V

No. of memristor per transistor	Performance metric (%)		
	Uniqueness	Uniformity	Bit-aliasing
1	49.991	50.650	50.663
2	49.834	47.251	47.263
3	49.619	46.302	46.313
4	49.945	50.512	50.513
5	49.215	54.560	54.763

For both circuit simulators, the performance of the memristor-based APUF have shown improvement, that is the values of the performance metrics are much closer to 50% as compared to the results of other memristor-based APUFs in [26, 27]. Comparing between the results from both circuit simulators, 180 nm at 1.8 V presents a more favorable result. The discrepancy may be due to the difference in the CMOS technology used. Nevertheless, the results when the 130 nm at 1.2 V is used are still acceptable, which is within the ±5% range from the ideal 50%.

The simulation results for the configuration 2, which is varying the number of challenge and response bits are shown in Tables 4 and 5., for 180 nm at 1.8 V and 130 nm at 1.2V, respectively. The memristor-based APUF shows excellent performance regardless of the combination of the number of challenge bits or response bits used, especially for the simulation set using 180 nm at 1.8 V. However, there is a slight discrepancy for the case of 32 challenge bits and 4 response bits when using 130 nm at 1.2 V. Nevertheless, for the rest of the combinations, the results are still satisfactory.

Table 4. Simulation results for configuration 2 on 180nm at 1.8V

No. of challenge bits	Performance metric (%)					
	4 response bits			8 response bits		
	Uniqueness	Uniformity	Bit-aliasing	Uniqueness	Uniformity	Bit-aliasing
8	49.998	49.940	49.938	49.987	49.902	49.894
16	50.008	49.960	49.963	50.006	49.795	49.800
32	49.990	49.575	49.631	49.995	49.790	49.809

Table 5. Simulation results for configuration 2 on 120nm at 1.2V

No. of challenge bits	Performance metric (%)					
	4 response bits			8 response bits		
	Uniqueness	Uniformity	Bit-aliasing	Uniqueness	Uniformity	Bit-aliasing
8	49.991	50.650	50.663	49.719	47.376	47.375
16	49.338	44.903	44.875	49.695	47.889	47.881
32	42.460	66.692	66.700	48.775	56.833	56.838

The proposed configurations of the memristor-based APUF show favorable results in terms of the performance metric values, especially in the case of uniqueness for almost all configurations. These results show that the memristor-based APUF is more unique, or in simple terms, the PUF responses are not alike and predictable, and appear random. With that said, it is harder to observe a pattern or repeatability in the response bits to predict the response. Furthermore, the results are consistent regardless of the configuration used. Therefore, the memristor-based APUF maintains its resistance to possible attacks.

With configurations, the circuit designer has the freedom to set the memristor-based APUF into any desired, or even random, configuration, since there is no fixed rule on the configurations. It can be designed

in such a way that both types of configurations discussed are applied. Therefore, it is more difficult for an adversary to duplicate a particular APUF without discovering the actual circuit design. In short, the memristor-based APUF, besides having improved performance in terms of uniqueness, uniformity, and bit-aliasing, also has better reliability in the sense that the performance is unchanged with changing configurations.

3.2. SVM prediction accuracy

Tables 6 and 7 shows the accuracy of the SVM on configurations 1 and 2, respectively. The expected result is 50%, which is the probability of obtaining one out of two equally possible outcomes, like a fair coin toss. The results in Tables 6 and 7 shows very close to desired values for even a large training set. Therefore, the results indicate that the proposed configurations on the memristor-based APUF have strong resistance against attacks by SVM, which is one of the widely used machine learning algorithms.

Table 6. SVM prediction accuracy for configuration 1

No. of memristor per transistor	SVM prediction accuracy (%)
1	49.940
2	42.188
3	50.672
4	49.609
5	49.024

Table 7. SVM prediction accuracy for configuration 2

No. of challenge bits	SVM prediction accuracy (%)	
	4 response bits	8 response bits
8	51.913	52.344
16	50.586	48.731
32	49.024	48.731

4. CONCLUSION

In this paper, configurations on the memristor-based APUF are proposed to increase variations and thereby further improving the PUF performance in terms of uniqueness, uniformity, and bit-aliasing; as well as resistance to attacks by SVM. Also, it is to make it more difficult or time-consuming for an adversary to duplicate the circuit design. The configurations made are 1) varying the number of memristor per transistor, and 2) varying the number of challenge and response bits. The results show excellent performance as well as strong resistance against attacks by SVM. In addition, the results are consistent among configurations. The memristor-based APUF shows excellent simulation results for all configurations for both CMOS technologies. In conclusion, configurations can be used in the implementation of the memristor-based APUF as a device for hardware security.

Future research efforts will be focused on additional tests such as randomness using NIST test suite as well as using other machine learning algorithms like linear regression or artificial neural network. Eventually, the actual hardware implementation will be done.

ACKNOWLEDGEMENTS

This research is supported by the Fundamental Research Grant Scheme (FRGS) under the project code FRGS/1/2015/TK04/UNITEN/02/2, awarded by the Ministry of Higher Education, Malaysia, and by the Universiti Tenaga Nasional (UNITEN) Internal Grant under the project code J510050761.

REFERENCES

[1] L. O. Chua, "Memristor - the missing circuit element," *IEEE Trans. Circuit Theory*, vol. 18, pp. 507-519, 1971.
[2] L. O. Chua and S. M. Kang, "Memristive devices and systems," *Proc. IEEE*, vol. 64, pp. 209-223, 1976.
[3] L. Chua, "Resistance switching memories are memristors," *Applied Physics A*, vol. 102, pp. 765-783, 2011.
[4] R. S. Williams, "How We Found The Missing Memristor," *IEEE Spectrum*, vol. 45, pp. 28-35, 2008.
[5] D. B. Strukov et al., "The missing memristor found," *Nature*, vol. 453, pp. 80-83, 05/01/print 2008.
[6] 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.
[7] P. Mazumder, S.-M. Kang, and R. Waser, "Memristors: devices, models, and applications," *Proceedings of the IEEE*, vol. 100, pp. 1911-1919, 2012.

[8] T. Prodromakis and C. Toumazou, "A review on memristive devices and applications," *2010 17th IEEE International Conference on Electronics, Circuits and Systems*, Athens, 2010, pp. 934-937.
[9] 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.
[10] J.Mathew et al. "A novel memristor based physically unclonable function," *Integr. VLSI J.*, vol. 51, pp. 37-45, 2015.
[11] G. S. Rose, N. McDonald, L. Yan and B. Wysocki, "A write-time based memristive PUF for hardware security applications," *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, 2013, pp. 830-833.
[12] M. Uddin *et al*., "Techniques for Improved Reliability in Memristive Crossbar PUF Circuits," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, 2016, pp. 212-217.
[13] 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.
[14] 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.
[15] P. Koeberl, Ü. Kocabaş and A. Sadeghi, "Memristor PUFs: A new generation of memory-based Physically Unclonable Functions," *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, 2013, pp. 428-431.
[16] 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.
[17] J. W. Lee et al., "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.
[18] Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200-1205, Oct. 2005.
[19] U. Rührmair and D. E. Holcomb, "PUFs at a glance," *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, 2014, pp. 1-6.
[20] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, 2007, pp. 9-14.
[21] G. S. Rose and C. A. Meade, "Performance analysis of a memristive crossbar PUF design," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, 2015, pp. 1-6.
[22] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan, "A Novel Memristor-Based Hardware Security Primitive," *ACM Trans. Embed. Comput. Syst.*, vol. 14, pp. 1-20, 2015.
[23] U. Rührmair, et al., "*Modeling attacks on physical unclonable functions*," in Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 237-249.
[24] G. Hospodar, et al., "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability," *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 37-42
[25] U. Chatterjee et al., "Theory and Application of Delay Constraints in Arbiter PUF," *ACM Trans. Embed. Comput. Syst.*, vol. 15, pp. 1-20, 2016.
[26] U. Chatterjee, R. S. Chakraborty, J. Mathew and D. K. Pradhan, "Memristor Based Arbiter PUF: Cryptanalysis Threat and Its Mitigation," *2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID)*, Kolkata, 2016, pp. 535-540.
[27] JJ. T. H. Loong, N. A. Nor Hashim and F. A. Hamid, "Memristor-based arbiter Physically Unclonable Function (APUF) with multiple response bits," *2016 IEEE Student Conference on Research and Development (SCOReD)*, Kuala Lumpur, 2016, pp. 1-5.
[28] Z. Biolek et al., "SPICE model of memristor with nonlinear dopant drift," *Radioengineering*, 2009.
[29] 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.
[30] 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.

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.