Modeling arbiter-PUF in NodeMCU ESP8266 using artificial neural network

Mohd Syafiq Mispan[1, 3, 4], Aiman Zakwan Jidin[1, 3, 4], Haslinah Mohd Nasir[2, 3, 4], Noor Mohd Ariff Brahin[1, 3, 4], Illani Mohd Nawi[5]

[1]Micro and Nano Electronics (MiNE), Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Malaysia
[2]Advance Sensors and Embedded Controls System (ASECs), Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Malaysia
[3]Centre for Telecommunication Research and Innovation (CeTRI), Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Malaysia
[4]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Malaysia
[5]Jabatan Kejuruteraan Elektrik dan Elektronik, Fakulti Kejuruteraan, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia

Article Info

Article history:

Received Jun 29, 2022
Revised Aug 7, 2022
Accepted Aug 26, 2022

Keywords:

Computational model
Hardware fingerprinting
Lightweight authentication
Machine learning
Physical unclonable function

ABSTRACT

A hardware fingerprinting primitive known as physical unclonable function (PUF) has a huge potential for secret-key cryptography and identification/authentication applications. The hardware fingerprint is manifested by the random and unique binary strings extracted from the integrated circuit (IC) which exist due to inherent process variations during its fabrication. PUF technology has a huge potential to be used for device identification and authentication in resource-constrained internet of things (IoT) applications such as wireless sensor networks (WSN). A secret computational model of PUF is suggested to be stored in the verifier's database as an alternative to challenge and response pairs (CRPs) to reduce area consumption. Therefore, in this paper, the design steps to build a PUF model in NodeMCU ESP8266 using an artificial neural network (ANN) are presented. Arbiter-PUF is used in our study and NodeMCU ESP8266 is chosen because it is suitable to be used as a sensor node or sink in WSN applications. ANN with a resilient back-propagation training algorithm is used as it can model the non-linearity with high accuracy. The results show that ANN can model the arbiter-PUF with approximately 99.5% prediction accuracy and the PUF model only consumes 309,889 bytes of memory space.

Corresponding Author:

Mohd Syafiq Mispan
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya street, 76100 Durian Tunggal, Melaka, Malaysia
Email: syafiq.mispan@utem.edu.my

1. INTRODUCTION

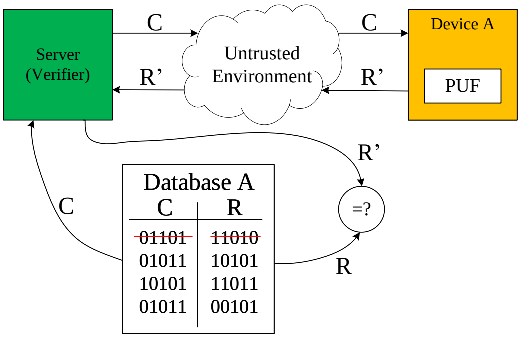
In recent years, the energy efficiency and security of the resource-constrained internet of things (IoT) systems become a crucial issue and a major challenge. With the evolving security and privacy threats, software-level security provides no guarantee to protect the system [1], [2]. Hence, hardware-level security technology is required to enhance the system protection and ensure only the authenticated device or hardware can proceed to the software or application launch. Nevertheless, providing another layer (i.e., hardware) of security level is challenging especially for resource-constrained IoT systems.

The emergence of physical unclonable function (PUF) as hardware fingerprinting technology could provide an intrinsic secret key or unique device-identifier by exploiting the inherent process variations during integrated circuits (ICs) fabrication. The input-output of the PUF is known as challenge and response pairs (CRPs). The unique and random corresponding responses are generated when challenges are applied to a PUF. The PUF response is uniquely different from one challenge to the other challenges. Additionally, when the same challenge is applied to two similar PUFs, each PUF generates a uniquely different response (i.e., device specific response). PUF design shows a few advantages such as low area and energy consumption, low fabrication cost, device-specific response, and non-human key programming which reduce the potential threat from untrusted parties in the interest to compromise the key [3].

Nevertheless, when considering the PUF application for resource-constrained device authentication, one of the primary drawbacks is the establishment of the secret CRPs table in the verifier database [4], [5]. During the authentication, the server is securely communicating with the PUF by sending the challenge and retrieving the PUF response as depicted in Figure 1. The authentication passes if the retrieved response is matched with the stored response. To avoid replay attacks, the used CRPs must be discarded from the verifier database and only unused CRPs are used for the next authentication process. Hence, the server must collect a huge number of CRPs before the field application and store them secretly [6], [7]. For applications with thousands (or could be millions) of PUF clients, this corresponds to an enormous amount of required secret storage.

To overcome the limitation of the huge database in the verifier, the researchers explored the feasibility of using a secret computational model of PUFs. In the early exploration, PUF-based authentication protocols have been proposed in which the underlying PUFs need to be derived during the enrollment phase. The example includes secure re-configurable PUF, time-bounded PUF, Slender PUF, noise bifurcation architecture, and statistical delay-based PUF [8]-[12]. In a study, Kong *et al.* [13] proposed a PUF-based remote attestation by binding the software-based attestation protocol to intrinsic device characteristics. Arithmetic and logic unit (ALU) PUF is used as a PUF basic building based on the delay difference in two different ALUs caused by the manufacturing variations. Moreover, the emulation-based approach is also proposed to overcome the huge CRPs storage. The ALU PUF is emulated by extracting its gate-level delay and the delay additions. However, during the read-out of the gate-level delays by a trusted party, the protected interface must be used. This protected interface must not be used by the user when the device is deployed in the field. Hence, it is suggested to provide a protected interface that can be permanently disabled by, e.g., using fuses.

In a recent study, Yilmaz *et al.* [14] proposed a lightweight authentication for resource-constrained IoT devices in which the PUF model is stored in the verifier's database. The proposed authentication scheme has been implemented on Zolertia Zoul devices based on server-client configuration. Elsewhere, Aghaie *et al.* [15] proposed a fast and novel method to build the PUF model for delay-based PUFs implemented on FPGA with only a few CRPs. The delay sensor is deployed as a readout circuit to characterize the delay of signals traversing through the PUF components. The readout circuit is only present in the FPGA design at the trusted party. The FPGA design shipped to the customer is not included with the readout circuit. Therefore, the design released to the customers is secured as no direct readout mechanism attach to it. All the above studies show that using a computational secret model of PUF for authentication protocol is feasible and it is getting attention in the PUF research community.



Database A

C	R
~~01101~~	~~11010~~
01011	10101
10101	11011
01011	00101

Figure 1. Authentication process using PUF technology

One of the potential resource-constrained applications that suit the PUF computational model is wireless sensor networks (WSN) [16], [17]. WSN is a technology used within an IoT system to sense and process sensitive data [18]. Figure 2 illustrates the WSN which consists of a sink and sensor nodes. All the collected data at the sensor nodes are forwarded to a sink node. Hence, before the exchange messages occur, the sensor nodes must be authenticated by the sink to ensure their authenticity. WSN can be developed using NodeMCU ESP8266 devices [19], [20]. Therefore, in this study, we design a computational model of PUF in NodeMCU ESP8266 using an artificial neural network (ANN) to enable the lightweight authentication protocol development in WSN. 32-bit arbiter-PUF is used as our case study for PUF computational model development.

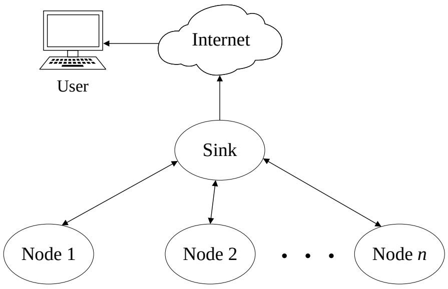


Figure 2. Sink and sensor nodes concept in WSN

2. METHOD

Arbiter-PUF was proposed in [21], [22] which consists of k switching component and one arbiter block as illustrated in Figure 3. The development of the arbiter-PUF computational model in NodeMCU ESP8266 is divided into three major design steps. First, 32-bit arbiter-PUF architecture was constructed in Cadence using 65-nm of CMOS technology node. Subsequently, the arbiter-PUF is simulated at 25 °C (room temperature) and supply voltage of 1.2 V (nominal value). The inherent process variations are modeled using Monte Carlo simulations within the Cadence environment. A total of 32000 CRPs have been collected for building the computational model of arbiter-PUF using ANN.

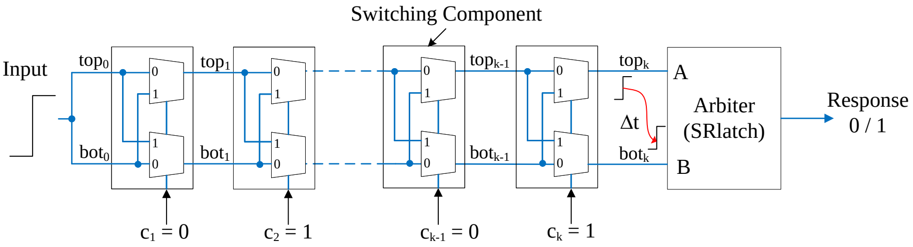


Figure 3. 32-bit arbiter-PUF architecture (k=32)

The second design step is the characterization of collected CRPs using the ANN technique in a MATLAB environment. The architecture of ANN used in our study is made-up of one input layer, one hidden layer, and one output layer. 32 neurons are placed in the hidden layer and tan-sigmoid is used as the activation function which is given as $f(x) = \frac{2}{1+e^{-2x}} - 1$. Whereas the linear activation function is used at the output layer. Figure 4 depicts the ANN architecture as described above. Following [23], [24], the training algorithm which has the optimum prediction accuracy, fast convergence time, and consistency is chosen, known as the resilient back-propagation algorithm. 30,000 CRPs are chosen randomly to be used as a training data set and the remaining 2,000 CRPs are used as the test data set. The weights and biases are extracted during the CRPs characterization to be used in the third design step.

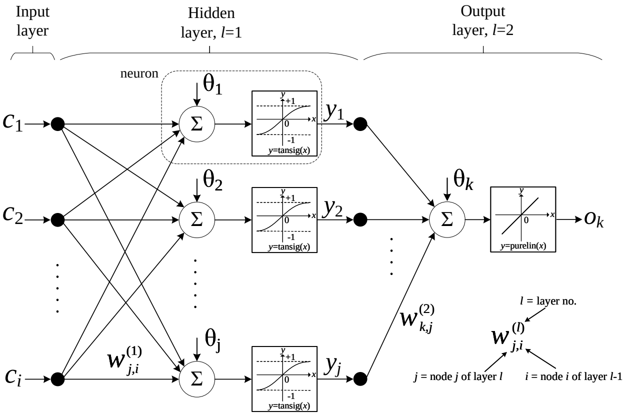


Figure 4. 3-layer of ANN archicture

For the third design step, an exact ANN architecture as simulated in MATLAB is designed in NodeMCU ESP8266 and the extracted weights and biases are stored in the memory. Subsequently, the predictability of the built ANN architecture is tested by using a similar 2,000 CRPs test data set. Its prediction result is compared against simulated predictability in the MATLAB environment, and it is expected to be similar.

3. RESULTS AND DISCUSSION

3.1. Arbiter-PUF characterization

As mentioned in section 1, PUF generates the random responses by exploiting the inherent process variations. The process variations are manifested in random delays in the IC. In our study, the random delay is modeled using Monte Carlo simulation. As a result, each switching component in Figure 3 has its own unique and random delay, which is also experienced by all the routing. When a rising pulse is applied at the input and propagates to the final output, it is subjected to all these random delays. For c_i=0, the paths for a rising pulse is straight, while for c_i=1 they are crossed. The accumulated delays at top_{32} and bot_{32} are evaluated using SR-latch (i.e., an arbiter). Figure 5 represents the random delays of top and bottom paths generated by two arbiter-PUFs in which both instances were applied with the same challenge. If $top_{32} < bot_{32}$, a binary response '1' is generated. Otherwise, a binary response '0' is generated. Based on delays in Figure 4, the corresponding random response of '1' and '0' is generated respectively for PUF instances A and B. The results indicate that the process variations are successfully modeled in arbiter-PUF using Monte Carlo simulation.

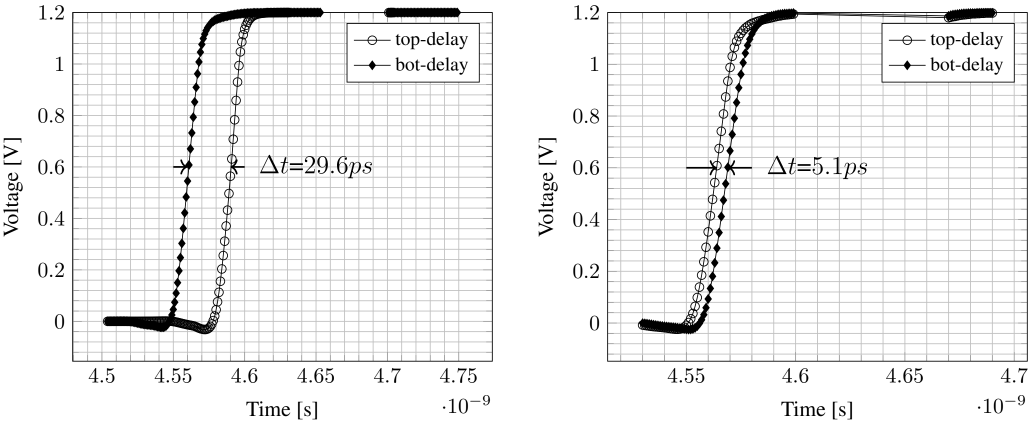


Figure 5. Rising pulses of two Arbiter-PUF instances (before the SR-latch) when applied with the same challenge

3.2. Modeling accuracy

Based on the arbiter-PUF which was designed in section 3.1, 32,000 CRPs are collected for building its computational model. An ANN technique is deployed for model-building as it can solve non-linear problems [25]. Figure 6 depicts the prediction accuracy of the 32-bit arbiter-PUF computational model. When a training set is small (i.e., 1,000 and below), the prediction accuracy is $\approx$90%. As the training set starts to increase larger than 1,000 CRPs, the prediction accuracy improves and achieved $\approx$99.5% accuracy. The result shows that a computational model of 32-bit arbiter-PUF is successfully built using the ANN technique. Subsequently, the weights and biases are extracted for the computational model development in the NodeMCU ESP8266.

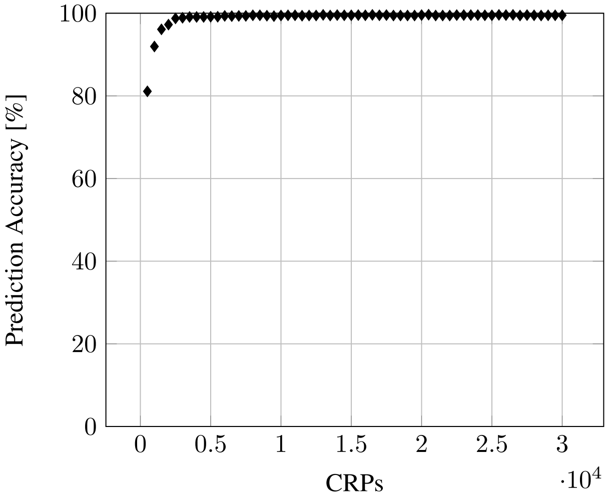


Figure 6. Prediction accuracy of 32-bit Arbiter-PUF modeled using ANN technique

3.3. Estimation of memory usage

The usage of memory for 32-bit arbiter-PUF model implementation in the NodeMCU ESP8266 device has been analyzed and summarized in Table 1. 7.1% of flash memory was occupied which consists of 5,200 bytes and 277,681 bytes, respectively for data and code. Whereas for SRAM, 50.3% was occupied which represents about 32,208 bytes. Note that in this study, only a set of weights and biases assuming for one sensor node has been stored in the memory. The NodeMCU ESP8266 device which has a database, DB to store the weights and biases represents a sink or verifier used to authenticate the nodes. In practice, the DB should consist of several sets of weights and biases for the identification and authentication process of sensor nodes in the WSN application.

Table 1. Memory usage (in byte) of the 32-bit arbiter-PUF model

.text	.data	.bss	Flash	SRAM	Total
277,681	5,200	27,008	282,881	32,208	309,889

4. CONCLUSION

PUF is a promising technology in the applications of identification/authentication and secret key generation. Although the PUF itself is a low-cost architecture, the deployment of the PUF in the authentication application requires a huge database of CRPs. An increase in the area consumption could deter the prevalent adoption of PUF, especially in resource-constrained systems. In this study, a computational model of Arbiter PUF is developed by using the ANN technique. Our findings show that 32-bit arbiter-PUF can be modeled with a very high accuracy of approximately 99.5%. Moreover, the computational model can be programmed in the NodeMCU ESP8266 device. The programmed device can be used as a verifier or sink in the WSN application for the sensor nodes authentication. Above all, this study gives insight into the design steps to build the PUF model in any microcontroller by using available machine learning techniques to enable lightweight authentication protocol development.

ACKNOWLEDGEMENT

The authors would like to thank the Ministry of Higher Education Malaysia and Universiti Teknikal Malaysia Melaka for the financial funding to complete this project. Grant No. FRGS/1/2020/TK0/UTEM/02/56.

REFERENCES

[1] S. Bhunia and M. Tehranipoor, "Introduction to hardware security," in *Hardware Security*, S. Bhunia and M. Tehranipoor, Ed. Elsevier, 2019, pp. 1–20.

[2] M. Malik, M. Dutta, and J. Granjal, "A survey of key bootstrapping protocols based on public key cryptography in the internet of things," *IEEE Access*, vol. 7, pp. 27443-27464, 2019, doi: 10.1109/ACCESS.2019.2900957.

[3] M. S. Mispan, B. Halak, and M. Zwolinski, "A survey on the susceptibility of PUFs to invasive, semi-invasive and noninvasive attacks: challenges and opportunities for future directions," *Journal of Circuits, Systems and Computers*, vol. 30, no. 11, p. 2130009, 2021, doi: 10.1142/S0218126621300099.

[4] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Computing Surveys*, vol. 48, no. 2, pp. 1–42, 2015, doi: 10.1145/2818186.

[5] U. Chatterjee *et al.*, "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424-437, 2019, doi: 10.1109/TDSC.2018.2832201.

[6] S. Sutar, S. Member, and A. Raha, "Memory-based combination PUFs for device authentication in embedded systems," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 793-810, 2018, doi: 10.1109/TMSCS.2018.2885758.

[7] M. S. Mispan and B. Halak, "Physical unclonable function: a hardware fingerprinting solution," in *Authentication of Embedded Devices*, B. Halak, Ed. Cham: Springer, 2021, pp. 29–51.

[8] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 2, no. 1, pp. 1-33, 2009, doi: 10.1145/1502781.1502786.

[9] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based PUF," *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, 2011, pp. 2071-2074, doi: 10.1109/ISCAS.2011.5938005.

[10] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," *2012 IEEE Symposium on Security and Privacy Workshops*, 2012, pp. 33-44, doi: 10.1109/SPW.2012.30.

[11] M. D. Mandel Yu, D. M'Raihi, I. Verbauwhede, and S. Devadas, "A noise bifurcation architecture for linear additive physical functions," *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2014, pp. 124-129, doi: 10.1109/HST.2014.6855582.

[12] T. Xu, D. Li, and M. Potkonjak, "Adaptive characterization and emulation of delay-based physical unclonable functions using statistical models," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6, doi: 10.1145/2744769.2744791.

[13] J. Kong, F. Koushanfar, P. K. Pendyala, A. R. Sadeghi, and C. Wachsmann, "PUFatt: embedded platform attestation based on novel processor-based PUFs," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*,2014, pp. 1-6, doi: 10.1145/2593069.2593192.

[14] Y. Yilmaz, L. Aniello, and B. Halak, "ASSURE: a hardware-based security protocol for resource-constrained IoT systems," *Journal of Hardware and Systems Security*, vol. 5, no. 1, pp. 1-18, 2021, doi: 10.1007/s41635-020-00102-0.

[15] A. Aghaie, M. Ender, and A. Moradi, "PUFs physical learning: Accelerating the enrollment via delay-based model extraction," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 3, pp. 1621-1632, 2022, doi: 10.1109/TETC.2021.3115176.

[16] M. H. Mahalat, D. Karmakar, A. Mondal, and B. Sen, "PUF based secure and lightweight authentication and key-sharing scheme for wireless sensor network," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 18, no. 1, pp. 1-23, 2022, doi: 10.1145/3466682.

[17] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-k. R. Choo, "PUF-based authentication and key agreement comprehensive survey," *IEEE Internet of Things Journal*, vvol. 9, no. 11, pp. 8205-8228, 2022, doi: 10.1109/JIOT.2022.3142084.

[18] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," in *Wireless Sensor Networks-Technology and Protocols*, M. A. Matin, Ed. IntechOpen, 2012, pp. 3–24.

[19] M. S. Mispan, A. Z. Jidin, M. R. Kamaruddin, and H. M. Nasir, "Proof of concept for lightweight PUF-based authentication protocol using NodeMCU ESP8266," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 24, no. 3, pp. 1392-1398, 2021, doi: 10.11591/ijeecs.v24.i3.pp1392-1398.

[20] X. Bajrami and I. Murturi, "An efficient approach to monitoring environmental conditions using a wireless sensor network and NodeMCU," *Elektrotechnik und Informationstechnik*, vol. 135, no. 3, pp. 294-301, 2018, doi: 10.1007/s00502-018-0612-9.

[21] D. Lim, "Extracting secret keys from integrated circuits," M.S. thesis, Massachusetts Institute of Technology, Cambridge, United States, 2004.

[22] 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," *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, 2004, pp. 176-179, doi: 10.1109/VLSIC.2004.1346548.

[23] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan, "A novel memristor-based hardware security primitive," *ACM Transactions on Embedded Computing Systems*, vol. 14, no. 3, pp. 1-20, 2015, doi: 10.1145/2736285.

[24] M. H. Ishak, M. S. Mispan, W. Y. Chiew, M. R. Kamaruddin, and M. Korobkov, "Secure lightweight obfuscated delay-based physical unclonable function design on FPGA," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 2, pp. 1075-1083, 2022, doi: 10.11591/eei.v11i2.3265.

[25] J. Heaton, *Introduction to neural networks for Java*, 2nd ed. Heaton Research, Inc., 2008.

BIOGRAPHIES OF AUTHORS

Mohd Syafiq Mispan received B.Eng Electrical (Electronics) and M.Eng Electrical (Computer and Microelectronic System) from Universiti Teknologi Malaysia, Malaysia in 2007 and 2010 respectively. He had experienced working in semiconductor industries from 2007 until 2014 before pursuing his Ph.D. degree. He obtained his Ph.D. degree in Electronics and Electrical Engineering from University of Southampton, United Kingdom in 2018. He is currently a senior lecturer in Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka. His current research interests include hardware security, CMOS reliability, VLSI design, and Electronic Systems Design. He can be contacted at email: syafiq.mispan@utem.edu.my.

Aiman Zakwan Jidin is currently a Ph.D. candidate at Universiti Malaysia Perlis, Malaysia. His research topic is focusing on optimizing memory testing algorithm efficiency for improving fault coverage. Previously, he obtained his MEng in Electronic and Microelectronic System from ESIEE Engineering Paris, France in 2011, before working as FPGA IP Core Design Engineer at Altera Corporation Malaysia (now part of Intel). He is a full-time lecturer and researcher at Universiti Teknikal Malaysia Melaka (UTeM), in Electronic and Computer Engineering. His research interests include DFT, VLSI, and FPGA system design. He can be contacted at email: aimanzakwan@utem.edu.my.

Haslinah Mohd Nasir received her Bachelor Degree in Electrical-Electronic Engineering (2008) from Universiti Teknologi Malaysia (UTM), MSc (2016) and PhD (2019) in Electronic Engineering from Universiti Teknikal Malaysia Melaka (UTeM). She had 5 years (2008-2013) experience working in industry and currently a lecturer in UTeM. Her research interest includes microelectronics, artificial intelligence and biomedical. She can be contacted at email: haslinah@utem.edu.my.

Noor Mohd Ariff Brahin received B.Eng Electrical (Electronics) from Universiti Teknologi Malaysia, Malaysia in 2008. He had experienced working in semiconductor industries from 2008 until 2013. He is currently a Teaching Engineer in Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka. His research interest include artificial intelligence and VLSI design. He can be contacted at email: mohdariff@utem.edu.my.

Illani Mohd Nawi received the B.Eng. degree (Hons.) from the Universiti Teknologi PETRONAS in 2002, and the M.Sc. degree in microelectronics systems design and the Ph.D. degree in electrical and electronic engineering from the University of Southampton, Southampton, U.K., in 2004 and 2018, respectively. She is currently a lecturer in Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Teknologi PETRONAS. Her research interests ranges from microelectronics systems design, robotics and automations, automotive-mems, bio-mems, and reliability in IC design. She can be contacted at email: illani.nawi@utp.edu.my.