Lightweight hardware fingerprinting solution using inherent memory in off-the-shelf commodity devices

Mohd Syafiq Mispan[1,4,5], Aiman Zakwan Jidin[1,4,5], Muhammad Raihaan Kamaruddin[2,4,5], Haslinah Mohd Nasir[3,4,5]
[1]Micro and Nano Electronics (MiNE), Melaka, Malaysia
[2]Machine Learning and Signal Processing (MLSP), Melaka, Malaysia
[3]Advance Sensors and Embedded Controls System (ASECs), Melaka, Malaysia
[4]Centre for Telecommunication Research and Innovation (CeTRI), Melaka, Malaysia
[5]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Article Info

Article history:

Received Mar 9, 2021
Revised Oct 22, 2021
Accepted Nov 16, 2021

Keywords:

ATMega2560
Hardware security
Physical unclonable function
SRAM-PUF

ABSTRACT

An emerging technology known as Physical unclonable function (PUF) can provide a hardware root-of-trust in building the trusted computing system. PUF exploits the intrinsic process variations during the integrated circuit (IC) fabrication to generate a unique response. This unique response differs from one PUF to the other similar type of PUFs. Static random-access memory PUF (SRAM-PUF) is one of the memory-based PUFs in which the response is generated during the memory power-up process. Non-volatile memory (NVM) architecture like SRAM is available in off-the-shelf microcontroller devices. Exploiting the inherent SRAM as PUF could wide-spread the adoption of PUF. Therefore, in this study, we evaluate the suitability of inherent SRAM available in ATMega2560 microcontroller on Arduino platform as PUF that can provide a unique fingerprint. First, we analyze the start-up values (SUVs) of memory cells and select only the cells that show random values after the power-up process. Subsequently, we statistically analyze the characteristic of fifteen SRAM-PUFs which include uniqueness, reliability, and uniformity. Based on our findings, the SUVs of fifteen on-chip SRAMs achieve 42.64% uniqueness, 97.28% reliability, and 69.16% uniformity. Therefore, we concluded that the available SRAM in off-the-shelf commodity hardware has good quality to be used as PUF.

Corresponding Author:

Mohd Syafiq Mispan
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka
Taman Tasik Utama, 75450 Ayer Keroh, Melaka, Malaysia
Email: syafiq.mispan@utem.edu.my

1. INTRODUCTION

Physical unclonable function (PUF) is a promising technology as a hardware fingerprinting solution for a trusted computing system by providing a root-of-trust. PUF exploits the intrinsic manufacturing process variations during integrated circuit (IC) fabrication. The intrinsic process variations embodied in the silicon chip acts as a random function for a PUF which can uniquely map a set of challenges to a set of responses, known as challenge-response pairs (CRPs). These CRPs are random and show a device-specific property that can be applied in IC identification and authentication, and cryptographic key generation application [1].

Several PUFs have been proposed in the past [2], [3]. Static random-access memory PUF (SRAM-PUF) is one of the previously proposed PUFs and it is categorized as memory-based PUF [4], [5]. Further, SRAM-PUF has been sub-categorized as Weak-PUF due to limitations in its CRPs. The terminology of 'Strong' and 'Weak' PUF is not meant to indicate that one PUF is superior to the other PUFs, rather it is to indicate the corresponding CRPs number of one PUF able to generate [4], [6], [7]. Typical SRAM cells consist of a cross-coupled inverter and two access transistors. The cross-coupled inverter is very susceptible to the process variations, hence lead to the threshold voltage, V_{th} mismatches between n-channel metal-oxide semiconductor (nMOS) and p-channel metal-oxide semiconductor (pMOS) transistors. Due to the V_{th} mismatch, a racing condition to charge the loading capacitances of cross-coupled inverter occurs during the power-up process [8]. An inverter that has a strong pMOS (i.e., low V_{th}) drives more current and turns the nMOS of another inverter to ON state. Eventually, the load capacitance corresponding to the strong pMOS being pulled-up to V_{dd} and another load capacitance being pulled-down to $0V$.

The phenomenon mentioned above causes each SRAM cell to settles at a random start-up value (SUV) either '1' or '0' during the power-up process. The SUVs across different memory blocks within an SRAM and across multiple SRAMs show device-specific and random patterns. Hence, it is suitable to be used as PUF as proposed earlier in [4], [5]. Nevertheless, the question remains is the suitability of on-chip or inherent SRAM in any computing device to be used as a PUF. Exploiting the on-chip SRAM as PUF can further reduce the total cost of building the hardware root-of-trust feature and could wide-spread the adoption of PUF in a computing system [9].

Motivated by the cost reduction and potential wide-spread adoption of PUF in computing systems, the focus of this paper is to analyze and evaluate the suitability of on-chip SRAM as PUF. We used the ATMega2560 microcontroller on the Arduino platform as a case study to evaluate the performance of SRAM-PUF. The main contributions of this work are highlighted below:

i We study the SUVs of on-chip 8kB SRAM in ATMega2560 microcontroller device. We show that the SUVs in the memory address range of 0x0281 to 0x20D0 are random and suitable to be used as PUF.

ii We evaluate the quality of PUF which includes uniqueness, reliability, and uniformity on fifteen on-chip 8kB SRAMs by randomly selecting 4096 bits from the aforementioned memory address range for each SRAM. The on-chip SRAM shows good quality and sufficient entropy of PUF which achieve 42.64%, 97.28%, and 69.16%, respectively for uniqueness, reliability, and uniformity.

The rest of the paper is organized as follows. Section 2 describes the background which related to this work. Section 3 describes the methods used in this study. The experimental analysis and results are presented in section 4. Finally, conclusions are drawn in section 5.

2. RELATED WORK

A dual function of SRAM as memory and PUF has been suggested in the previous studies [10]–[12]. Hoffmann *et al.*, [11], [12] were focused on reusing the on-chip cache as PUF, while Mispan *et al.*, [10] proposed the ageing mitigation technique (i.e., to improve the reliability of SUVs) experiences by the SRAM cells when it is being used as memory and PUF. Other studies have been focusing on using on-chip SRAM as PUF in ARM-based low-end commodity microcontroller devices [13], [14]. These studies show that the inherent SRAM in ARM-based microcontroller contains sufficient entropy to be exploited as PUF. In other studies, Platonov *et al.*, [15] and Aung *et al.*, [16] investigate the entropy of SUVs in an on-chip memory in ATMega1284P and ATMega328P microcontrollers, respectively. The results from both studies show that the SUVs have a good entropy that can uniquely distinguish each chip. Elsewhere, microcontrollers in Arduino platforms have been used for a proof-of-concept of internet-of-things (IoT) device authentication [17]–[19]. Besides, the on-chip SRAM in ATMega328P microcontroller devices have been used as a case study to perform invasive attacks as discussed in [20], [21]. All of the above studies show that the feasibility of using on-chip SRAM in ATMega256 microcontroller on Arduino platform as PUF has never been studied. In our study, we focus on evaluating the PUF entropy of on-chip 8 kB SRAM in an ATMega256 microcontroller device and we specify which memory address can be used to generate a unique identifier.

3. METHODOLOGY

The available on-chip memory of 8 kB SRAM in ATMega2560 microcontroller on the Arduino platform is used in this study. The on-chip SRAM in ATMega2560 is divided into 4 allocations of memories which are the Register File, the I/O memory, Extended I/O memory, and the internal data SRAM [22]. Each address is used to store a byte (i.e., 8-bit) of data. The first 32 locations address the register file, the next 64 locations the standard I/O memory, then 416 locations of extended I/O memory, and the next 8,192 locations address the internal data SRAM. All memory location addresses are analyzed in searching for unique and random patterns of SUVs during the power-up process. To read the SUVs of SRAM-cells, we modified the start-up code (i.e., setup() function) to display the raw SUVs via universal asynchronous receiver-transmitter (UART) (i.e., Arduino on-board USB-to-Serial) before the SRAM gets initialized. The start-up code is essential to every microcontroller as it initializes variables, pin modes, and libraries. To measure the reliability of SUVs under different power-up cycles, five power-up processes have been conducted on each of fifteen devices with a time interval of 5 minutes before the next power-up process takes place to eliminate the effect of data remanence in SRAM cells [23]. It is assumed that the supply voltage and surrounding temperature remain constant during the power-up experiment. All SUVs extracted from the on-chip SRAM are recorded in a CSV file and MATLAB R2016b is used as a post-processing software to evaluate the uniqueness, reliability, and uniformity performances.

4. SIMULATION RESULTS AND ANALYSIS

In this section, the relevant simulation and analysis are discussed based on the described methodology in section 3. First, the randomness of the SUVs in the ATMEGA2560's SRAM is analyzed. Subsequently, the quality of SRAM-PUF such as uniqueness, reliability, and uniformity is evaluated according to the mathematical formulation described in [24], [25].

4.1. Analysis of the ATMEGA2560's SRAM

We evaluated the SUVs patterns of ATMega2560 microcontroller device on Arduino platform that integrates an on-chip 8 kB (i.e., range of address: 0x0000 to 0x21FF) of SRAM. The randomness of SUVs of SRAM cells is assessed using fifteen ATMega2560 devices by extracting the SUVs in each memory location. Figure 1 illustrates the bitmap of SUVs measurement of all the addresses in an 8 kB on-chip SRAM in the ATMega2560 microcontroller. The bitmap has been illustrated such that each row consists of 16-byte of data (i.e., 128-bit). As can be seen in Figure 1, the bitmap indicates that there are repeating patterns in the low address (0x0000 to 0x027F) and high address (0x20D0 to 0x21FF) regions for all fifteen devices.

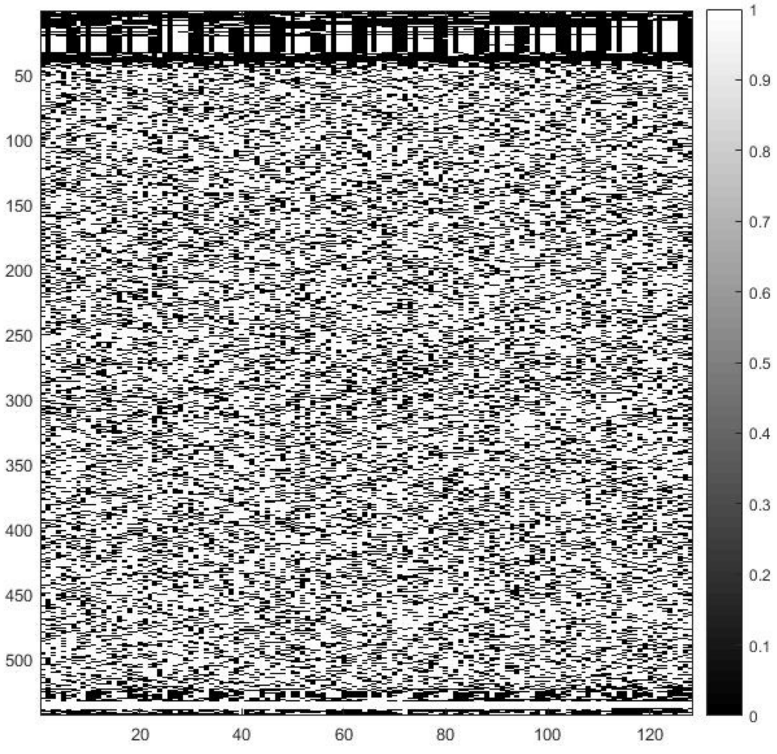

Figure 1. Bitmap of SUVs measurement of an ATMEGA2560 on-chip 8 kB SRAM

As mentioned in section 3 the first 512 locations addressed the register file, the standard I/O memory, and the Extended I/O memory. Therefore, we assume that the observed repeating patterns represent structures used by the on-board ROM code embedded with every Arduino board. Another observation of repeating patterns is at the high address region which corresponding to the address of internal data SRAM that could be caused by the application programming interface (API). The most important observation is the SUVs generated by the SRAM cells within the address region of 0x0280 to 0x20CF which shows randomness and uniqueness characteristics. Hence, the subsequent analysis of PUF quality is based on the SUVs extracted from this address region.

4.2. Uniqueness

Uniqueness measures the ability of a PUF to generate a response that differ from the other responses generated by the other similar types of PUFs when a challenge C is applied. Ideally, the uniqueness should be distributed around 50% with a very small standard deviation. Uniqueness can be evaluated using hamming distance (HD) as defined in (1):

$$\text{Inter–HD} = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{\text{HD}(R_i(n), R_j(n))}{n} \times 100\% \tag{1}$$

where i and j represent two PUF instances under evaluation that generates n-bit of response. m represents the total number of similar types of PUFs.

Based on the findings of random SUVs patterns as discussed in section 4.1, only 4096-bit is selected randomly within the address region of 0x0280 to 0x20CF for each device. Figure 2 depicts the uniqueness for fifteen SRAM-PUF instances with a 4096-bit of response is extracted for each SRAM-PUF. The uniqueness of 0.4264 (42.64%) with a standard deviation of 0.0102 is obtained. The uniqueness and its standard deviation are closed to an ideal value of 50% with a very small standard deviation.

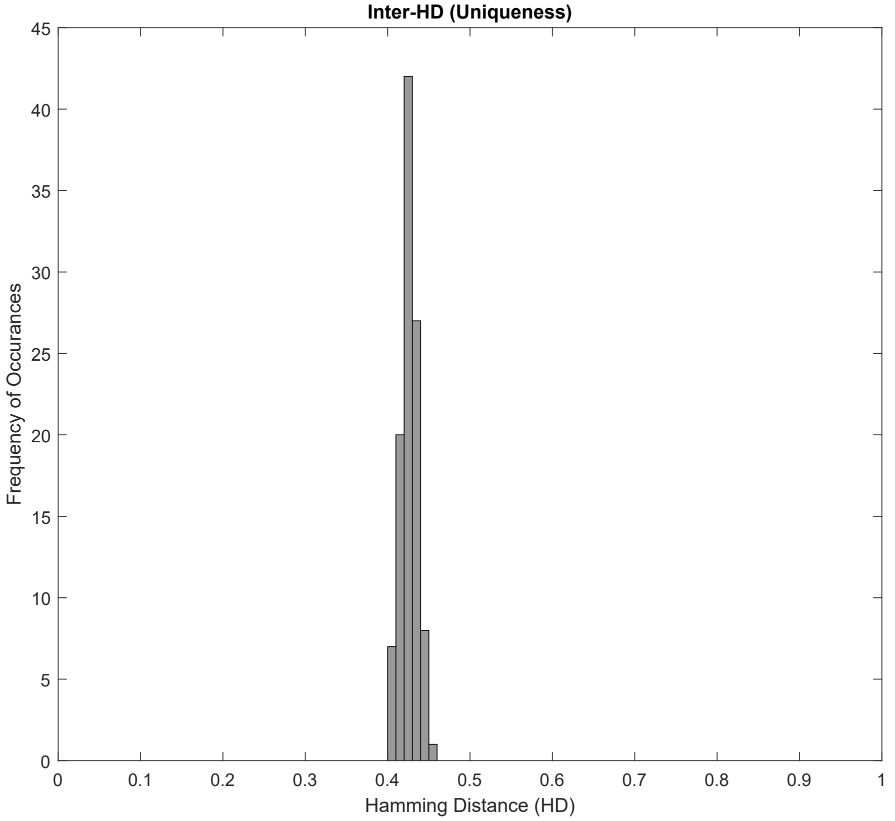

Figure 2. Uniqueness of fifteen SRAM PUF instances

4.3. Reliability

Reliability is a measure of reproducibility of the PUF response. Ideally, a 100% reliability is desired for PUF circuits. However, because of the noise experienced by the PUF circuit, it is not possible to achieve 100% reliability. The SUVs for reliability evaluation have been extracted according to the methodology described in section 3. Subsequently, the reliability is computed using (2), defined as:

$$\text{Reliability} = \left(1 - \frac{1}{m}\sum_{j=1}^{m}\frac{\text{HD}(R_i(n), R'_{i,j}(n))}{n}\right) \times 100\% \tag{2}$$

where i represents PUF under evaluation which generate n-bit response, $R_i(n)$ at reference power-up, $R'_{i,j}(n)$ is the response at different condition (i.e., next power-up process), and m represents the total number of power-up processes. The SUVs which was generated for uniqueness evaluation in Section 4.2. is set as a response at the reference power-up.

Figure 3 depicts the reliability for each of the SRAM-PUFs that has been subjected to five power-up processes. Based on the reliability evaluation, one device shows reliability of 93.29%, lower as compared to the reliability of the other fourteen devices. Despite an outlier, it can be observed that the SRAM-PUFs achieve high reliability under different power-up processes, on average of about 97.28%, close to an ideal value of 100%.

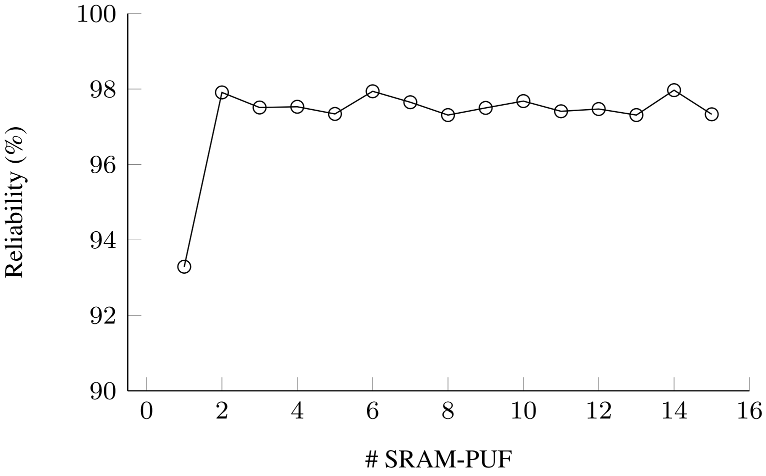

Figure 3. Reliability of fifteen SRAM-PUFs subjected to five power-up processes

4.4. Uniformity

Uniformity measures the number of 1's and 0's distribution in a binary response of a PUF. A balanced distribution of 1's and 0's is required which indicates the randomness in a response. Uniformity can be evaluated using hamming weight (HW) as defined in (3):

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

where $r_{i,j}$ is the j-th binary bit of an n-bit response from a PUF i, for a total of m PUFs. Figure 4 depicts the uniformity distribution of fifteen SRAM-PUFs with 4096-bit extracted from each PUF. The SUVs extracted from fifteen SRAM-PUFs achieve 0.6916 (69.16%) of uniformity with a standard deviation of 0.0182.

The SUVs are skewed towards one, therefore the uniformity value is more than 50% as can be seen in Figure 4 which indicates more 1's than 0's in the PUF responses. A similar observation of a strong bias towards one in another ATMega family is described in [26]. Despite this observation, the uniqueness which has been evaluated earlier in Section 4.2. is closed to an ideal value of 50% (i.e., able to distinguish a PUF from a group of similar PUFs). Hence, on-chip SRAM in the ATMega2560 microcontroller still holds a good quality to be a PUF.

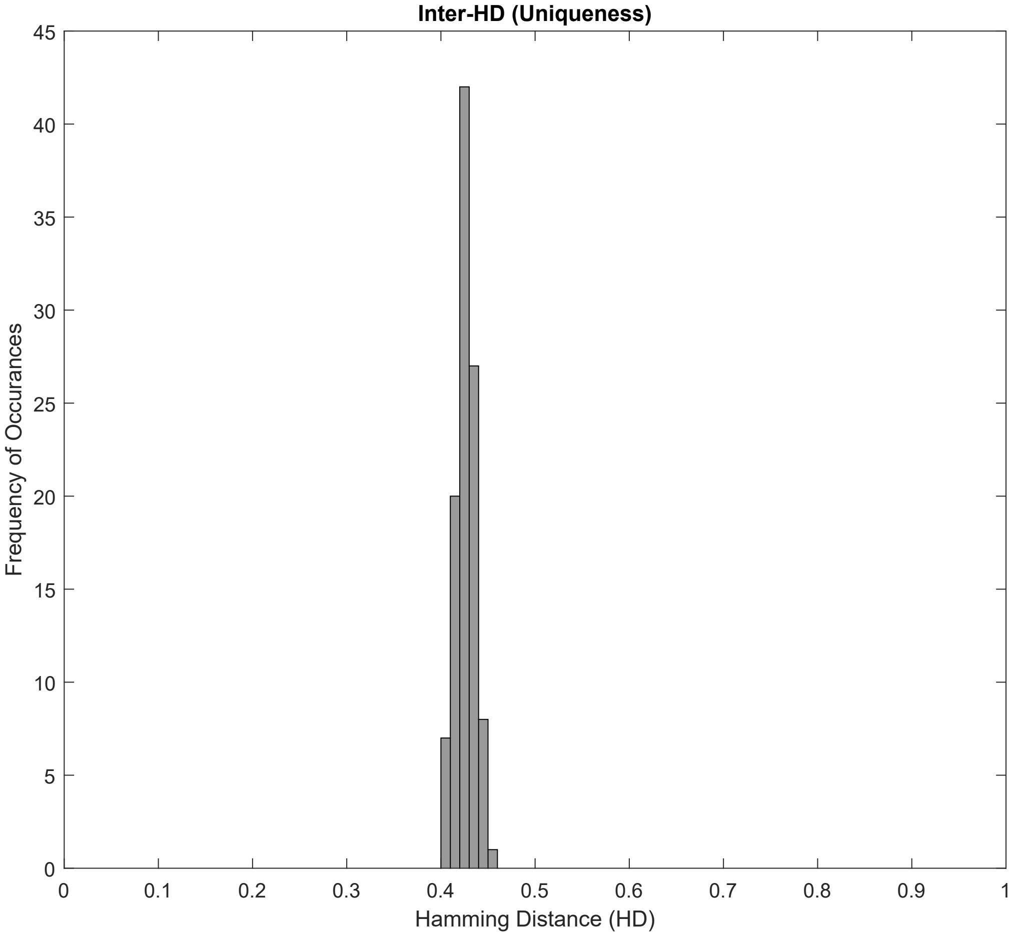

Figure 4. Uniformity of fifteen SRAM PUF instances

5. CONCLUSION

SRAM-PUF is one of the previously proposed memory-based PUFs. SRAM memory is available in any computing system, hence it is interesting to investigate the suitability of using on-chip memory in off-the-shelf commodity devices. In this study, the on-chip memory of 8kB SRAM in ATMega2560 microcontroller on the Arduino platform has been used as a case study. Our findings show that the uniqueness is distributed close to an ideal value of 50% with a small standard deviation. The average reliability of fifteen SRAM-PUFs under five different power-up cycles is approximately about 97.28%. The uniformity of SUVs extracted from fifteen SRAM-PUFs shows biasing towards one whereby the uniformity is distributed around 69.16%. Despite the skewed uniformity, on-chip SRAM in the ATMega2560 microcontroller still showing good uniqueness and reliability. Hence, it can be concluded that the on-chip SRAM in the ATMega2560 microcontroller on the Arduino platform is suitable to be used as a hardware root-of-trust solution known as PUF.

ACKNOWLEDGEMENT

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

REFERENCES

[1] 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.

[2] M. S. Mispan, H. Sarkawi, A. Z. Jidin, R. H. Ramlee, and H. M. Nasir, “Design and implementation of multiplexed and obfuscated physical unclonable function,” *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 9, no. 1, pp. 91–100, 2021, doi: 10.11591/ijeei.v9i1.2664.

[3] M. S. Mispan, B. Halak, and M. Zwolinski, “A survey on the susceptibility of PUFs to invasive, semi-invasive and non-invasive attacks: challenges and opportunities for future directions,” *Journal of Circuits, Systems and Computers*, vol. 30, no. 11, pp. 1–37, 2021, doi: 10.1142/S0218126621300099.

[4] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” in *International Conference on Cryptographic Hardware and Embedded Systems*, 2007, pp. 63–80, doi: 10.1007/978-3-540-74735-2_5.

[5] D. E. Holcomb, W. P. Burleson, and K. Fu, “Power-Up SRAM state as an identifying fingerprint and source of true random numbers,” *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198-1210, 2009, doi: 10.1109/TC.2008.212.

[6] U. Rührmair *et al.*, “PUF modeling attacks on simulated and silicon data,” *IEEE Transactions on Information Forensic and Security*, vol. 8, no. 11, pp. 1876-1891, Nov. 2013, doi: 10.1109/TIFS.2013.2279798.

[7] U. Rührmair, S. Devadas, and F. Koushanfar, “Security Based on Physical Unclonability and Disorder,” in *Introduction to Hardware Security and Trust*, M. Tehranipoor and C. Wang, Eds. 1st, Springer, 2012, pp. 65-102, doi: 10.1007/978-1-4419-8080-9.

[8] M. S. Mispan, M. Zwolinski, and B. Halak, “Ageing mitigation techniques for SRAM memories,” in *Ageing of Integrated Circuits*, B. Halak, Ed. 1st, Springer, Cham, 2020, pp. 91-111, doi: 10.1007/978-3-030-23781-3_4.

[9] T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, “A critical insight into the identity authentication systems on smartphones,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 3, pp. 982-989, 2019, doi: 10.11591/ijeecs.v13.i3.pp982-989.

[10] M. S. Mispan, S. Duan, B. Halak, and M. Zwolinski, “A reliable PUF in a dual function SRAM,” *Integration*, vol. 68, pp. 12-21, 2019, doi: 10.1016/j.vlsi.2019.06.001.

[11] C. Hoffman, M. Cortes, D. F. Aranha, and G. Araujo, “Computer security by hardware-intrinsic authentication,” in *International Conf. on Hardware/Software Codesign and System Synthesis*, 2015, pp. 143-152, doi: 10.1109/CODESISSS.2015.7331377.

[12] A. Bacha and R. Teodorescu, “Authenticache: Harnessing cache ECC for system authentication,” in *International Symposium on Microarchitecture*, 2015, pp. 128-140, doi: 10.1145/2830772.2830814.

[13] A. Schaller, T. Arul, V. Van Der Leest, and S. Katzenbeisser, “Lightweight anti-counterfeiting solution for low-end commodity hardware using inherent PUFs,” in *Trust and Trustworthy Computing*. Springer International Publishing, 2014, pp. 83-100, doi: 10.1007/978-3-319-08593-7_6.

[14] F. Kohnhäuser, A. Schaller, and S. Katzenbeisser, “PUF-based software protection for low-end embedded devices,” in *Trust and Trustworthy Computing*, M. Conti, M. Schunter, and I. Askoxylakis, Eds. Springer International Publishing, 2015, pp. 3-21, doi: 10.1007/978-3-319-22846-4.

[15] M. Platonov, J. Hlavác, and R. Lórencz, “Using power-up SRAM state of Atmel ATmega1284P microcontrollers as physical unclonable function for key generation and chip identification,” *Information Security Journal*, vol. 22, no. 5-6, pp. 244-250, 2013, doi: 10.1080/19393555.2014.891279.

[16] P. P. Aung, K. Mashiko, N. B. Ismail, and O. C. Yee, “Evaluation of SRAM PUF Characteristics and Generation of Stable Bits for IoT Security,” in *Emerging Trends in Intelligent Computing and Informatics*, F. Saeed, F. Mohammed, and N. Gazem, Eds. Springer, Cham, 2020, doi: 10.1007/978-3-030-33582-3_42.

[17] C. Lipps, A. Weinand, D. Krummacker, C. Fischer, and H. D. Schotten, “Proof of concept for IoT device authentication based on SRAM PUFs using ATMEGA 2560-MCU,” in *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, 2018, pp. 36-42, doi: 10.1109/ICDIS.2018.00013.

[18] A. R. Korenda, F. Afghah, B. Cambou, and C. Philabaum, “A proof of concept SRAM-based physically unclonable function (PUF) key generation mechanism for IoT devices,” in *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2019, pp. 1-8, doi: 10.1109/sahcn.2019.8824887.

[19] D. Mukhopadhyay, “PUFs as Promising Tools for Security in Internet of Things,” *IEEE Design & Test*, vol. 33, no. 3, pp. 103-115, 2016, doi: 10.1109/MDAT.2016.2544845.

[20] D. Nedospasov, J. P. Seifert, C. Helfmeier, and C. Boit, “Invasive PUF analysis,” in *Fault Diagnosis and Tolerance in Cryptography*, 2013, pp. 30-38, doi: 10.1109/FDTC.2013.19.

[21] C. Helfmeier, C. Boit, D. Nedospasov, and J. P. Seifert, “Cloning physically unclonable functions,” in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 1-6, doi: 10.1109/HST.2013.6581556.

[22] Microchip, “ATmega640/V-1280/V-1281/V-2560/V-2561/V Datasheet,” pp. 1-427, 2014. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/ATmega640-1280-1281-2560-2561-Datasheet-DS40002211A.pdf (accessed 12/7/2021).

[23] S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A. Sadeghi, “Remanence decay side-channel: The PUF case,” *IEEE Tran. on Information Forensics and Security*, vol. 11, no. 6, pp. 1106-1116, 2016, doi: 10.1109/TIFS.2015.2512534.

[24] A. Maiti, V. Gunreddy, and P. Schaumont, “A systematic method to evaluate and compare the performance of physical unclonable functions,” in *Embedded Systems Design with FPGAs*, P. Athanas, D. Pnevmatikatos, and N. Sklavos, Eds. New York: Springer New York, 2013, pp. 245-267, doi: 10.1007/978-1-4614-1362-2.

[25] A. Maiti and P. Schaumont, “The impact of aging on a physical unclonable function,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 9, pp. 1854-1864, 2014, doi: 10.1109/TVLSI.2013.2279875.

[26] A. V. Herrewege, “Lightweight PUF-based Key and Random Number Generation,” Ph.D. dissertation, KU Leuven, 2015. [Online]. Available: https://www.esat.kuleuven.be/cosic/publications/thesis-254.pdf (accessed 12/7/2021).

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 obtained his M.Eng in Electronic and Microelectronic System Engineering from ESIEE Engineering Paris France in 2011. He has 2 years of working experience in designing digital IC and digital system in FPGA at Altera Corporation Malaysia, before joining Universiti Teknikal Malaysia Melaka as lecturer and researcher, in Electronics and Computer Engineering. His research interests include FPGA Design and Digital System Design. He can be contacted at email: aimanzakwan@utem.edu.my.

Muhammad Raihaan Kamaruddin received the B.Eng (Electronics and Computer Systems) and M.Eng (Electronics and Information Science) degrees from Takushoku University, Japan, He is working toward the PhD degree in Electronics and Computer Engineering with the Universiti Teknikal Malaysia Melaka (UTeM). His PhD is on the Implementation of bio-inspired robotic navigation system using stochastic computing. He has working experience as lecturer in Universiti Teknikal Malaysia Melaka (UTeM) for 10 years (2010-present). His research interest includes machine learning, robotic and stochastic computing. He can be contacted at email: raihaan@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.