Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 9, No. 1, March 2021, pp. 91~100
ISSN: 2089-3272, DOI: 10.11591/ijeei.v9i1.2664

Design and Implementation of Multiplexed and Obfuscated Physical Unclonable Function

Mohd Syafiq Mispan[1], Hafez Sarkawi[2], Aiman Zakwan Jidin[3], Radi Husin Ramlee[4], Haslinah Mohd Nasir[5]
[1,3]Micro and Nano Electronics (MiNE), Malaysia
[2,5]Advanced Sensors and Embedded Control Systems (ASECs), Malaysia
[4]Machine Learning and Signal Processing (MLSP), Malaysia
[1,2,3,4,5]Centre for Telecommunication Research and Innovation (CeTRI), Malaysia
[1,2,3,4,5]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received , Aug 14, 2020
Revised , Mar 9, 2021
Accepted , Mar 16, 2021

Keywords:

Physical Unclonable Function
Process variation
Machine learning
Model-building
Hardware security

ABSTRACT

Model building attack on Physical Unclonable Functions (PUFs) by using machine learning (ML) techniques has been a focus in the PUF research area. PUF is a hardware security primitive which can extract unique hardware characteristics (i.e., device-specific) by exploiting the intrinsic manufacturing process variations during integrated circuit (IC) fabrication. The nature of the manufacturing process variations which is random and complex makes a PUF realistically and physically impossible to clone atom-by-atom. Nevertheless, its function is vulnerable to model-building attacks by using ML techniques. Arbiter-PUF is one of the earliest proposed delay-based PUFs which is vulnerable to ML-attack. In the past, several techniques have been proposed to increase its resiliency, but often has to sacrifice the reproducibility of the Arbiter-PUF response. In this paper, we propose a new derivative of Arbiter-PUF which is called Mixed Arbiter-PUF (MA-PUF). Four Arbiter-PUFs are combined and their outputs are multiplexed to generate the final response. We show that MA-PUF has good properties of uniqueness, reliability, and uniformity. Moreover, the resilient of MA-PUF against ML-attack is 15% better than a conventional Arbiter-PUF. The predictability of MA-PUF close to 65% could be achieved when combining with challenge permutation technique.

Corresponding Author:

Mohd Syafiq Mispan,
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik,
Universiti Teknikal Malaysia Melaka, Malaysia.
Email: syafiq.mispan@utem.edu.my

1. INTRODUCTION

Nowadays, trusted and secured computing solutions are crucially demanding especially with the emergence of the Internet of Things (IoT). Generally, any computing systems can be represented as hardware, firmware, software (i.e., operating system, application, etc.) and data layers. For any computing systems which dealing with sensitive and user-specific data, the trustworthiness of the whole computing system is very important to avoid loss of privacy which can be realized by providing root-of-trust from the hardware layer.

Physical Unclonable Function (PUF) is an innovative technology that able to extract hardware characteristics and manifest them as device-specific responses that can be used as root-of-trust in trusted computing. The intrinsic manufacturing process variations during integrated circuit (IC) fabrication are exploited by PUF such that it can map a set of challenges to a set of responses, uniquely for each PUF instance. The challenge to response mapping or known as challenge-response pairs (CRPs) represents the characteristic of particular hardware. As PUFs can generate unique CRPs based on hardware characteristics, hence PUFs can be used to provide a secure, reliable and trustworthy root-of-trust to any computing systems.

Guajardo *et al*., [1] and Rührmair *et al*., [2] classified PUFs into Strong-PUFs and Weak-PUFs. Strong-PUFs are PUFs that have an exponential number of CRPs, given as 2^k where k is the number of challenge bits. Meanwhile, Weak-PUFs are the types of PUFs which have a limited number of CRPs, predetermined challenges, and in the extreme case with just only a single challenge. Example of Weak PUFs such as SRAM-PUF [1, 3], D Flip-Flop PUF [4], Buttery-PUF [5], Buskeeper-PUF [6], and SR-NOR latch PUF [7]. The terms of 'Strong' and 'Weak' are not meant to indicate the superiority of one PUF to another but merely to classify the PUFs based on their CRPs nature.

In the early development of PUFs, a delay-based PUF known as Arbiter-PUF, fabricated on silicon using TSMC 180-nm technology node was proposed [8, 9]. Arbiter-PUF is a type of Strong-PUFs which has k-bit challenge and a total of 2^k CRPs. The functionality of Arbiter-PUF is based on the linearly additive delay which can be easily modelled using machine learning (ML) techniques. The susceptibility of Arbiter-PUF to ML-attack, therefore, has raised concern within the research community of hardware security [2, 10]. Several studies in the past have focused on the techniques to increase the resiliency of Arbiter-PUF against MLattack [10, 11, 12, 13, 14]. Most of the techniques are using the XOR obfuscation technique which successfully increases the resilience of Arbiter-PUF against ML-attack. However, the XOR technique degrades the reliability of the PUF response.

In this paper, a new derivative of Arbiter-PUF which is called Mixed Arbiter-PUF (MA-PUF) is proposed. Four Arbiter-PUFs are combined and their outputs are multiplexed to generate the final response. The multiplexing technique is applied in MA-PUF instead of the XOR technique to reduce the degradation impact on the PUF reliability. Based on our analysis, MA-PUF has shown good properties of uniqueness, reliability, and uniformity. Moreover, the MA-PUF exhibits resiliency against ML-attack. The main contributions of this work are highlighted below:

1. We propose a new derivative of Arbiter-PUF known as MA-PUF which has good properties of uniqueness and uniformity, close to an ideal value of 50%. The MA-PUF achieves good reliability of about 96%.
2. The proposed MA-PUF has 15% better resiliency against ML-attack as compared to a conventional Arbiter-PUF. A combination of MA-PUF with challenge permutation further increases its resilience against ML-attack. The predictability of the MA-PUF reduces to ≈65% with a challenge permutation technique.

The rest of the paper is organized as follows. Section 2 describes the background which related to this work. The architecture of the proposed MA-PUF is discussed in Section 3. Section 4 describes the methods to construct the MA-PUF and to quantify its performance. The analysis of MA-PUF performance and its ML-attack resistance is presented in Section 5. Finally, conclusions are drawn in Section 6.

2. BACKGROUND

2.1. Arbiter-PUF

Lee *et al*., [8] proposed an Arbiter-PUF which was designed and implemented on silicon using the process technology of TSMC 180-nm. The proposed architecture of k-bit Arbiter-PUF as illustrated in Figure 1. Arbiter-PUF exploits the logic delay and interconnects variations due to limitations during IC fabrication processes. Arbiter-PUF consists of k switching components and an arbiter. Typically, SR-latch is used as an arbiter since it offers fair arbitration from its symmetric circuit topology [15].

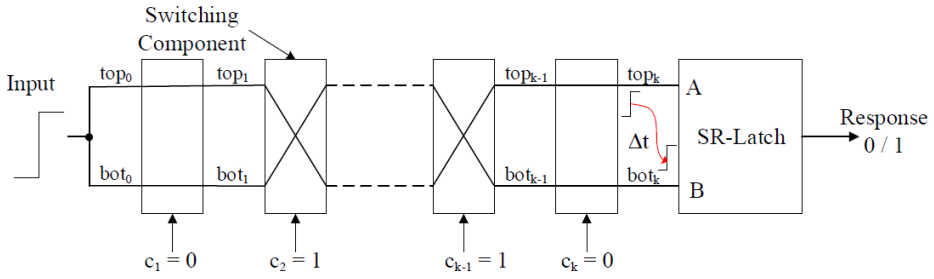

Figure 1. Structure of k-bit Arbiter-PUF [8]

The switching components can be constructed using two-to-one (2-to-1) multiplexer using logic gates or transmission gates. A rising pulse is applied at the input and propagated through two nominally identical delay paths. The switching component controls the propagation delay paths of the input pulse by setting the bits of the challenge, $C = \{c_1, c_2, \ldots, c_k\}$. For $c_k = 0$, the path go straight through, while for $c_k = 1$, they are crossed. Due to process variations, each switching component and the interconnect wire exhibits a unique delay. As the rising pulse passes through until k-th switching component, there is a delay difference between the two rising pulses which represented as Δt. A random response, '0' or '1', is generated by the arbiter (i.e., SR-latch) depending on the difference in arrival times.

2.2. Related Work

The Arbiter-PUF discussed in the previous section was constructed based on the linear characteristics of the additive delays caused by the switching components in each stage. Hence, there is a possibility that the adversaries could model the Arbiter-PUF by using ML techniques. A successful model-building attacked on Arbiter-PUF has been described in [9] by using an ML technique known as support vector machine (SVM). To increase the non-linearity in Arbiter-PUF, other derivatives or Arbiter-PUF are proposed such as Feed-Forward Arbiter-PUF [16], XOR-Arbiter-PUF [17] and Lightweight-PUF [18]. These techniques mainly using the XOR technique to obfuscate the challenges and/or responses. Nevertheless, all the aforementioned PUFs are successfully attacked using ML techniques as described in [2]. An important finding as described by Rührmair *et al*., [2], as the challenge bit length k and the number of XOR increase, the difficulty of an ML to model the PUF increases.

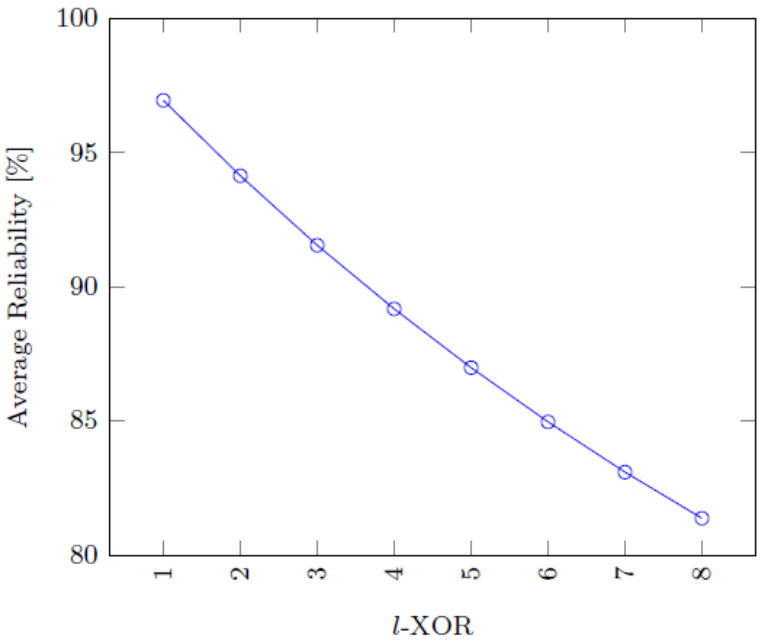

Figure 2. l-XOR Arbiter-PUF, $k = 32$ [19]

In recent works, Ye *et al*., [20] proposed obfuscated PUF by combining the XOR technique and the random start-up values (SUVs) generated by the SRAM cells after the power-up process. However, the susceptibility of the proposed obfuscated PUF against ML-attack has not been presented in [20]. The following work by Ye *et al*., [12] was a randomized PUF (RPUF) based on the obfuscation of the Arbiter-PUF challenges by using random number generator (RNG). Nevertheless, the number of CRPs used for ML training is too small to have a conclusive finding on its ML-attack resiliency. Machida *et al*., [21] proposed Double Arbiter-PUF (DA-PUF) which was constructed based on XOR Arbiter-PUF. XOR Arbiter-PUF consists of l number of Arbiter-PUF as in Figure 1 and the final response is generated by XORing l responses. Unlike the XOR Arbiter-PUF, the DA-PUF obfuscated the $top_{k,i}$ and $bot_{k,i}$ for $i = 1, 2, \ldots, l$, among ${}^{l}P_2$ arbiters and the final response is generated by XORing ${}^{l}P_2$ responses. The DA-PUF exhibits a promising resiliency against MLattack with the predictability of about 69% and 57% respectively for 2-1 DA-PUF and 3-1 DA-PUF [14, 22]. However, the XOR technique degrades the reliability of a given PUF. As can be seen in Figure 2, the reliability reduces as l increases.

In another study, an Obfuscated-PUF (OB-PUF) is proposed by Gao *et al*., [11] in which the verifier sent a partial challenge to the prover (i.e., OB-PUF) to increase the complexity of the CRPs mapping. The RNG within an OB-PUF is used to generate a random pattern. Afterwards, the random pattern is padded with a partial challenge which was sent earlier by the verifier to make up a full-length challenge. Further, OB-PUF generates a random response based on the full-length challenge. Elsewhere, Mispan *et al*., [13] proposed a challenge permutation technique to increase the complexity of the challenge-to-response mapping of an Arbiter-PUF. Both works, [11, 13] able to reduce the predictability of a conventional Arbiter-PUF to ≈ 65% for a total training CRPs of 30,000. In recent work, Vatajelu *et al*., [23] proposed symmetric encryption on Arbiter-PUF challenges using a secret key generated by a Weak-PUF. The proposed technique successfully reduces the predictability of Arbiter-PUF significantly. However, the symmetric encryption incurs area overhead and it is costly to be implemented for resource-constrained pervasive devices. In our work, we explore a new derivative of Arbiter-PUF which imitates the DA-PUF structure but without scarifying the reliability of the PUF response. In Section 5, we will discuss and compare the performance of the proposed MA-PUF with typical Arbiter-PUF and DA-PUF.

3. PROPOSED MA-PUF

The architecture of the MA-PUF is derived from the Arbiter-PUF, proposed in [8]. Figure 3 depicts the top-level architecture of the *k*-bit MA-PUF. The PUF consists of four Arbiter-PUFs, two 4-to-1 multiplexers and one arbiter (i.e., SR-latch). The same *k*-bit challenges are applied to four Arbiter- PUFs. The top delay of the MA-PUF, given as $top_{k,i}$ for $i = 1, \ldots, 4$ is input to the top multiplexer. The bottom delay of the MA-PUF, given as $bot_{k,i}$ for $i = 1, \ldots, 4$ is input to the bottom multiplexer. For each of the multiplexers, the selector bits are connected from the 2-bit of the challenges. In this study, the selector bits of the top multiplexer is c_{k-1} and c_k, while the selector bits of the bottom multiplexer is c_1 and c_2. Generally, for *m k*-bit challenges generated by the linear feedback shift register (LFSR), an average each bit position has a 50% probability of a value '1'. Therefore, each multiplexer can use any of the challenge bits position provided that the selected bits fulfil the condition of $s_{top}[1:0] \neq s_{bot}[1:0]$. The outputs of both multiplexers are input to the arbiter to generate a final response, depending on the difference in arrival times of the selected delay.

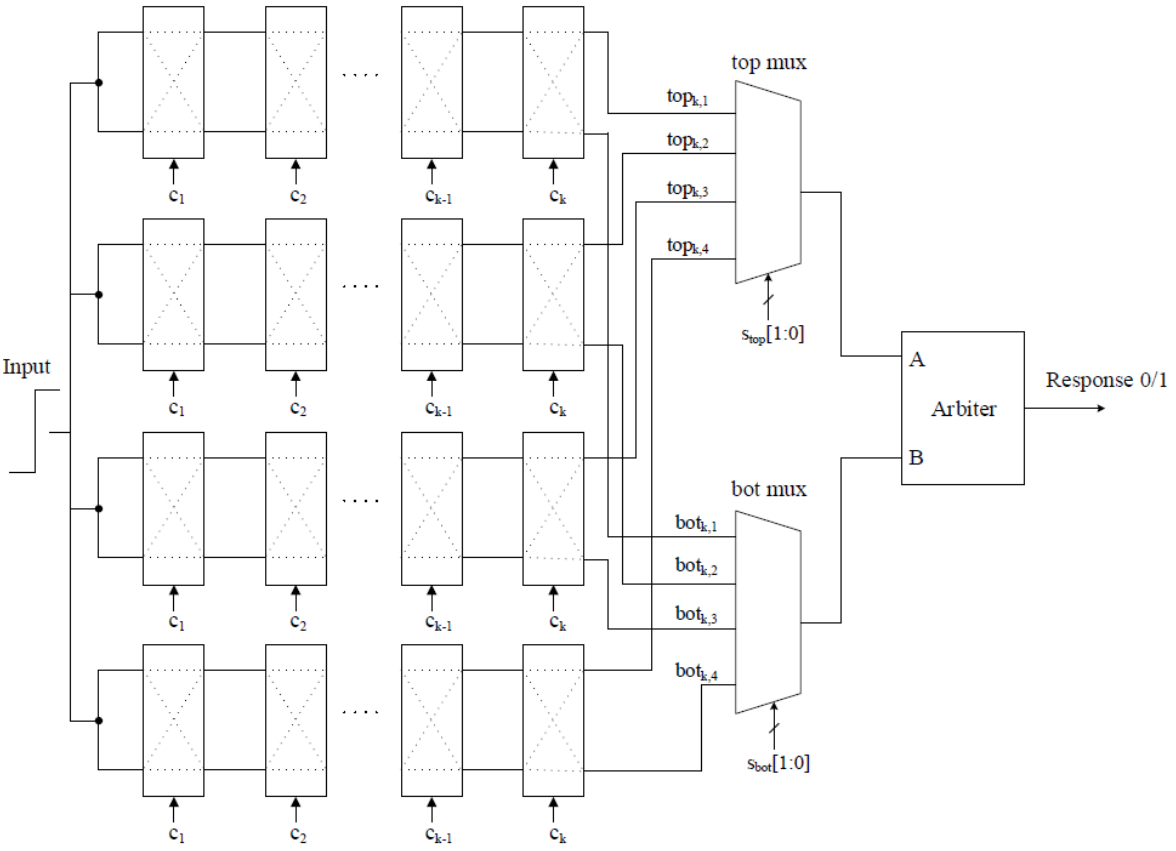

Figure 3. Top-level of *k*-bit MA-PUF

4. METHODOLOGY

The 32-bit MA-PUF (k = 32) circuit has been constructed and simulated using a low-κ 65-nm CMOS technology node with a nominal supply voltage of 1.2V and a room temperature of 25°C. The BSIM4 (V4.5) transistor model was used to simulate the MA-PUF circuit. The Monte Carlo simulation is used to model the manufacturing process variations such as threshold voltage (V_{th}), effective width, effective length, and oxide thickness. 100 PUF instances were modelled using Monte Carlo simulation by using the built-in statistical variation (3σ variations) in the technology design kit (i.e., fabrication standard). A 32-bit response is generated for each of the PUF instances. In this study, the performance of MA-PUF to resist ML-attack is evaluated following the methodology described in [24]. The Artificial Neural Network (ANN) is employed since it offers the capability of modelling highly non-linear systems and it is implemented in MATLAB environment.

5. SIMULATION RESULTS AND ANALYSIS

The standard method to quantify the quality of a PUF is described in [25]. The quality parameters are uniqueness, reliability, and uniformity. In this section, these quality metrics of the proposed PUF are discussed. Moreover, the robustness of MA-PUF against ML-attack is also discussed.

5.1. Uniqueness

The uniqueness is the ability of a PUF to be uniquely distinguished from a group of PUFs of a similar type. The uniqueness is evaluated using Inter-hamming distance (Inter-HD) and it is given as [25]:

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

where i and j represent two PUF instances under evaluation, each PUF generates n-bit response, $R_i(n)$ and $R_j(n)$, respectively when applied with the same challenge, $C = \{c_1, c_2, \ldots, c_k\}$ and m is the total number of PUF instances. A 32-bit response is generated for each MA-PUF using the methodology described in Section 4. By using the Eq. (1), the uniqueness for 100 32-bit MA-PUF instances is 49.77%. The distribution of uniqueness or Inter-HD is illustrated in Figure 4. The uniqueness of MA-PUF is very close to the ideal value of 50%. Therefore, this indicates that for the same challenge applied to two similar MA-PUFs, it has a higher probability of one MA-PUF that will generate a response of about 50% different compared to the other MA-PUF. Nonetheless, a smaller group of the MA-PUF instances has a uniqueness of less than or more than 50% as indicated by the spread of the Gaussian imitated distribution in Figure 4.

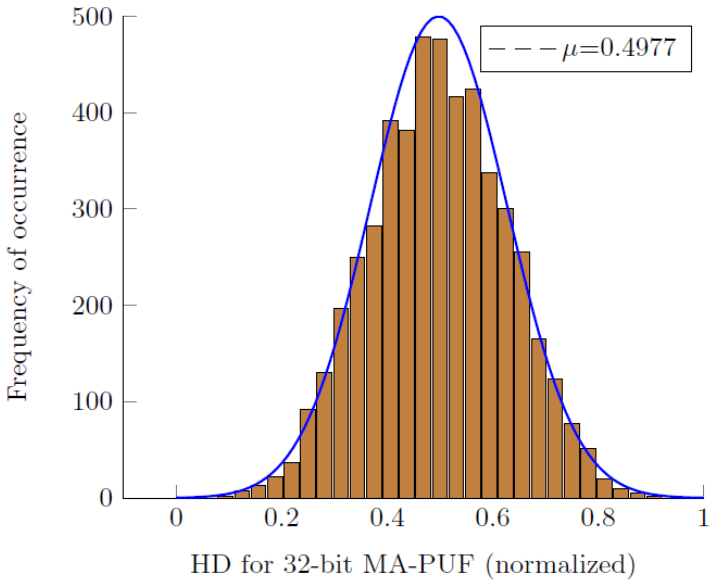

Figure 4. Uniqueness for 100 instances of 32-bit MA-PUF

5.2. Reliability

The reliability is the ability of a PUF to generate the same response over the environmental uctuations such as temperature and supply voltage when applied with the same challenges. The reliability is evaluated using Intra-HD and it is given as [25]:

$$Intra - HD = \frac{1}{m}\sum_{j=1}^{m}\frac{HD(R_i(n), R'_{i,j}(n))}{n} \times 100\% \quad (2)$$

Further, the reliability of a PUF can be computed based on Intra-HD value and it is defined as:

$$Reliability = 100\% - Intra - HD \quad (3)$$

where *i* represents PUF under evaluation which generate *n*-bit response, $R_i(n)$ at nominal temperature and supply voltage, $R'_{i,j}(n)$ is the response at different condition (i.e., temperature and/or supply voltage), and *m* is the number of samples.

To evaluate the reliability, the MA-PUF is subjected to variations in supply voltage (1.2V±10%) and/or ambient temperature from -40°C to 85°C, in which a total of 12 conditions including nominal condition as shown in Figure 5. By using Eq. (2) and (3), the average reliability of MA-PUF under the aforementioned conditions is 96%. Based on our reliability analysis, we found that the reliability of MA-PUF is approximately similar to a conventional Arbiter-PUF. The reliability of MA-PUF under each condition is depicted in Figure 5. A nominal condition, 1.2V and 25°C is used as a reference condition which explains the reliability value of 100%. For example, the response measured at 1.08V and -40°C is compared against the response measured at the reference condition, 1.2V and 25°C. Subsequently, the evaluated reliability (93.22%) is plotted in Figure 5 and this process continues for 11 other conditions. According to [26], an increase in temperature decreases *Vth*, while also decreasing the electron and hole mobilities, and vice versa. Meanwhile, an increase in supply voltage increases the overdrive voltage and current, while also decreasing the charging/discharging time of loading capacitances, and vice versa. These effects due to temperature and supply voltage variations may counteract during the circuit operation and cause unreliable responses, hence describes the observed reliability pattern in Figure 5.

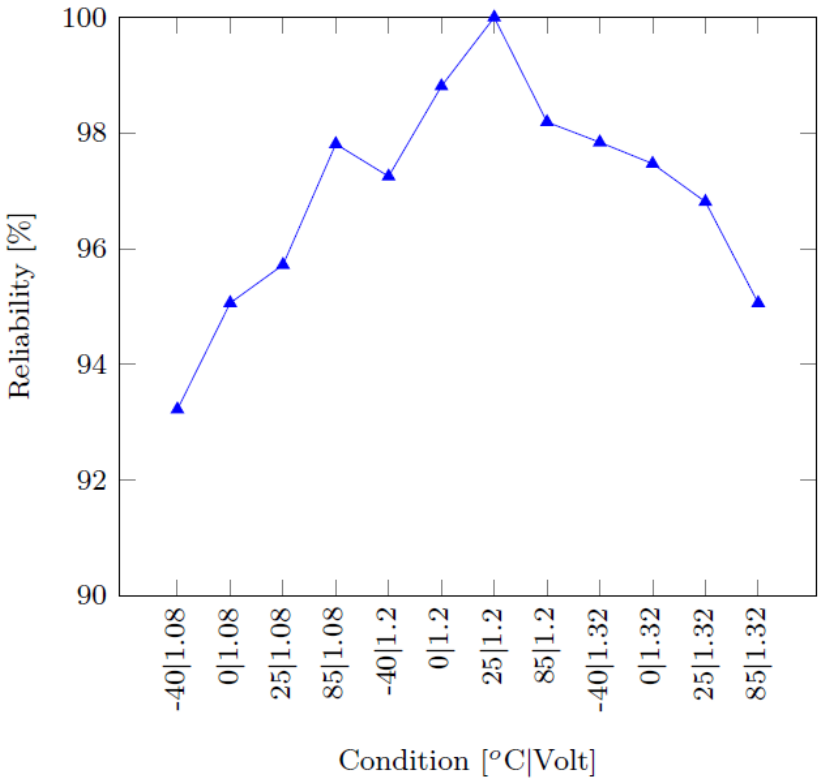

Figure 5. Reliability of 32-bit MA-PUF subjected to supply voltage and/or temperature fluctuations

5.3. Uniformity

The uniformity is defined as the proportion of 0`s and 1`s in the response bits of a PUF which characterize the randomness of the PUF response. Ideally, the number of 0`s and 1`s in response must be balanced, hence uniformity is distributed at 50%. The uniformity is evaluated using hamming weight (HW) and it is given as [25]:

$$Uniformity = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} r_{i,j} \times 100\% \quad (4)$$

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. By using the Eq. (4), the uniformity for 100 32-bit MA-PUF instances is 48.34%. The distribution of uniformity is illustrated in Figure 6. Although the mean value of the uniformity is close to the ideal value of 50%, the spread of the uniformity distribution indicates some of the MA-PUFs have unbalanced of 0`s and 1`s.

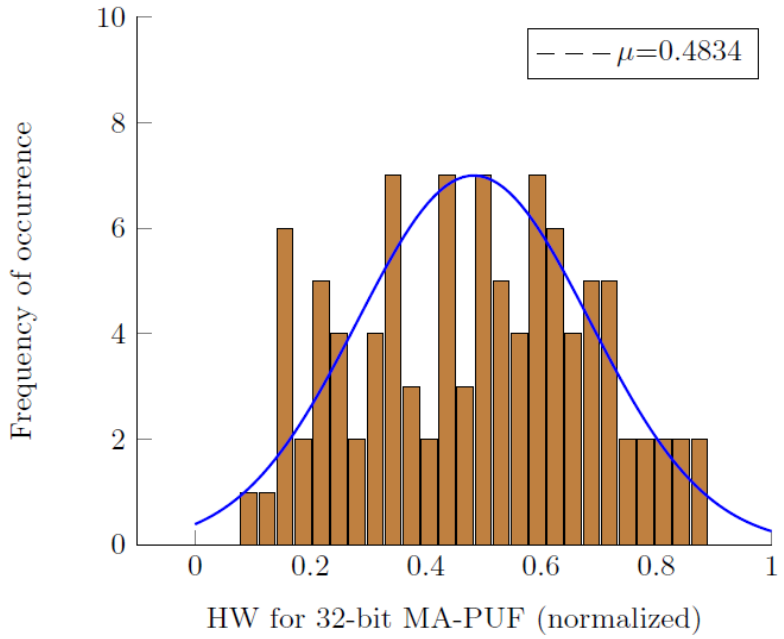

Figure 6. Uniformity for 100 instances of 32-bit MA-PUF

The above quality metrics for MA-PUF is summarized in Table I and compared against conventional Arbiter-PUF and DA-PUF. The MAPUF has a comparable uniqueness and uniformity as compared to the DA-PUF. The MA-PUF has an advantage of better reliability which is ≈ 96% as compared to the DA-PUF, ≈ 88%.

Table 1. Performance Comparison

Quality	MA-PUF	3-to-1 DA-PUF [21]	Arbiter-PUF [8]
Uniqueness (%)	49.77	50 ± 1	23
Reliability (%)	≈ 96	≈ 88	≈ 95
Uniformity (%)	48.34	≈ 50	Na

5.4. ML-attack

Another important criterion of a given PUF is resiliency against ML-attack. 32,000 CRPs have been collected for ML-attack evaluation using ANN. 30,000 CRPs have been used as a training dataset while 2,000 CRPs have been used as a testing dataset. Figure 7 shows the comparison of the susceptibility to ML-attack. Based on our evaluation, by introducing the mixing element using multiplexer in MAPUF, the predictability of a conventional Arbiter-PUF can be reduced from ≈ 99% down to ≈ 85%. The predictability of the MA-PUF can be further reduced by combining the challenge permutation technique as introduced in [13]. The MA-PUF with challenge permutation achieved ≈ 65% prediction accuracy. The challenge permutation incurs no cost as this technique can be implemented by routing obfuscation. Meanwhile, from our analysis, 3-to-1 DA-PUF shows

better resiliency against ML-attack. Nevertheless, as discussed in Section 2.2, the XOR technique used in the DA-PUF degrades its reliability (i.e., estimated reliability degradation, see Figure 2). A similar reliability degradation was also observed in [21].

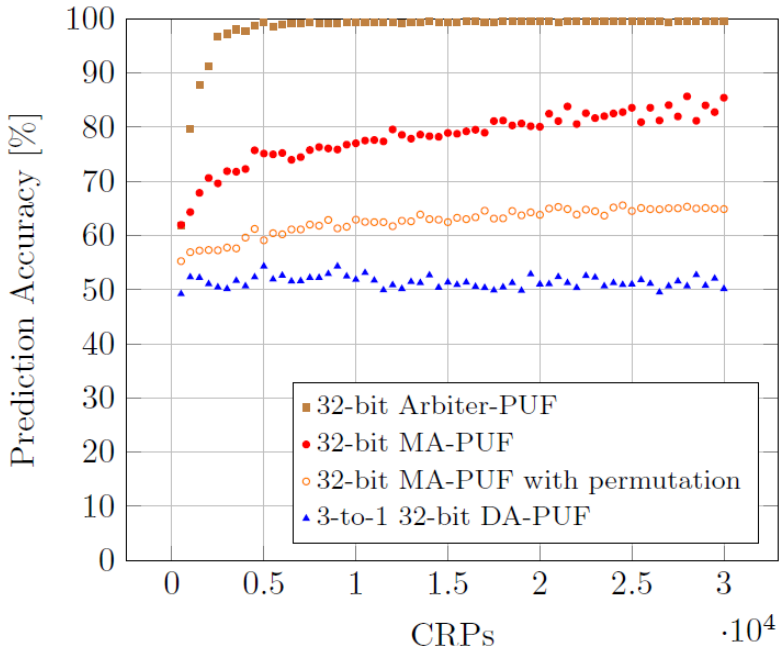

Figure 7. Comparison of the susceptibility to ML-attack

5.5. Area Consumption

For an area estimation, the behavioral model of MA-PUF, Arbiter-PUF, and 3-to-1 DA-PUF have been synthesized using Design Compiler. Table 2 lists the area in gate equivalent (GE) for the aforementioned PUFs. As expected, the area consumption for MA-PUF and 3-to-1 DA-PUF is higher than Arbiter-PUF as their architecture consists of the parallel Arbiter-PUFs. As can be seen from Table 2, MA-PUF has a slightly higher area consumption than 3-to-1 DA-PUF. Despite the highest area consumption, MA-PUF achieves better reliability as compared to 3-to-1 DA-PUF and it achieves better unpredictability against ML-attack as compared to Arbiter-PUF.

Table 2. Area Comparison

Type	Area [GE]
32-bit MA-PUF	500
32-bit Arbiter-PUF	122
3-to-1 32-bit DA-PUF	383

6. CONCLUSION

The root-of-trust is of paramount importance to build a trusted and secured computing systems. With the emergence of IoT, trusted computing systems are crucially demanding. The notion of PUF has been introduced as a promising hardware security primitive which can provide root-of-trust by extracting unique hardware characteristics. In this paper, we have proposed a new architecture for a PUF, known as MA-PUF which is derived from a conventional Arbiter-PUF and DA-PUF. MA-PUF has shown good quality metrics of uniqueness and uniformity, close to an ideal value of 50%. The reliability of MA-PUF is far better than 3-to-1 DA-PUF which achieved about 96%. The application of the XOR technique amplifies the reliability degradation of DA-PUF as the number of XOR gate increases. Hence, MA-PUF uses the multiplexing technique to avoid significant reliability degradation and to increase its resilience against ML-attack. By using the multiplexing technique, the resilient of MA-PUF against ML-attack is improved by 15% as compared to a conventional Arbiter-PUF. Although DA-PUF performs better in resisting the ML-attack of about 51% predictability, the resiliency of MA-PUF to ML-attack can be improved by combining with a challenge permutation technique. MA-PUF achieves about 65% prediction accuracy when combined with challenge

permutation technique. This technique incurs no cost which can be implemented using routing obfuscation. For an area consumption, MA-PUF consumes 500 GE. It is slightly higher than 3-to-1 DA-PUF that consumes 383 GE only.

ACKNOWLEDGMENTS

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. 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.
[2] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Transactions on Information Forensic and Security*, vol. 8, pp. 1876-1891, 2013.
[3] 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.
[4] V. Van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from d flip-flops," in *ACM Workshop on Scalable Trusted Computing*, 2010, pp. 53-62.
[5] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The Buttery PUF protecting IP on every FPGA," in *IEEE International Workshop on Hardware- Oriented Security and Trust*, 2008, pp. 67-70.
[6] P. Simons, E. Van Der Sluis, and V. Van Der Leest, "Buskeeper PUFs, a promising alternative to D Flip- Flop PUFs," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2012, pp. 7-12.
[7] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69-77, 2008.
[8] 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 *Symposium on VLSI Circuits Digest of Technical Papers*, 2004, pp. 176-179.
[9] D. Lim, "Extracting secret keys from integrated circuits," MSc. Thesis, Massachusetts Institute of Technology, 2004.
[10] U. Rührmair and J. Solter, "PUF modelling attacks: An introduction and overview," in *Design, Automation & Test in Europe Conference & Exhibition*, 2014, pp. 1-6.
[11] Y. Gao, G. Li, H. Ma, S. F. Al-Sarawi, O. Kavehei, D. Abbott, and D. C. Ranasinghe, "Obfuscated challenge response: A secure lightweight authentication mechanism for PUF-based pervasive devices," in *IEEE International Conference on Pervasive Computing and Communication Workshops*, 2016, pp. 1-6.
[12] J. Ye, Y. Hu, and X. Li, "RPUF: Physical unclonable function with randomized challenge to resist modeling attack," in *IEEE Asian Hardware Oriented Security and Trust Symposium*, 2016, pp. 1-6.
[13] M. S. Mispan, H. Su, M. Zwolinski, and B. Halak, "Cost-Efficient Designs for Modeling Attacks Resistant PUFs," in *Design, Automation & Test in Europe Conference & Exhibition*, 2018, pp. 467-472.
[14] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "Implementation of Double Arbiter PUF and Its Performance Evaluation," in *Asia and South Pacific Design Automation Conference*, 2015, pp. 6-7.
[15] L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Design and validation of Arbiter-based PUFs for sub-45nm low-power security applications," *IEEE Transactions on Information Forensic and Security*, vol. 7, no. 4, pp. 1394-1403, 2012.
[16] 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, no. 10, pp. 1200-1205, 2005.
[17] G. E. Suh and S. Devadas, "Physical Unclonable Functions for device authentication and secret key generation," in *ACM/IEEE Design Automation Conference*, 2007, pp. 9-14.
[18] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in *IEEE/ACM International Conference on Computer-Aided Design*, 2008, pp. 670-673.
[19] M. S. Mispan, "Towards Reliable and Secure Physical Unclonable Functions," Ph.D. Thesis, University of Southampton, 2018.
[20] J. Ye, Y. Hu, and X. Li, "OPUF: Obfuscation logic based physical unclonable function," in *IEEE International On-Line Testing Symposium*, 2015, pp. 156-161.
[21] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new mode of operation for arbiter PUF to improve uniqueness on FPGA," in *Federated Conference on Computer Science and Information Systems*, 2014, pp. 871-878.
[22] M. Khalafalla and C. Gebotys, "PUFs Deep Attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs," in *Design, Automation and Test in Europe Conference and Exhibition*, 2019, pp. 204-209.
[23] E. I. Vatajelu, G. D. Natale, M. S. Mispan, and B. Halak, "On the encryption of the challenge in physically unclonable functions," in *IEEE International Symposium on On-Line Testing and Robust System Design*, 2019, pp. 115-120.
[24] M. S. Mispan, B. Halak, and M. Zwolinski, "Lightweight Obfuscation Techniques for Modeling Attacks Resistant PUFs," in *IEEE International Verification and Security Workshop*, 2017, pp. 19-24.
[25] 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.

[26] P. E. Allen and D. R. Holberg, CMOS Analog Circuit Design. New York: Oxford University Press, 2002.

BIOGRAPHY 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 respec- tively. 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.

Hafez Sarkawi received B.Eng Electrical (Electronics) from Universiti Teknologi Malaysia in 2007 and M.Eng (Industrial Electronics and Control) from Universiti Malaya in 2012. Currently, he is a Lecturer at the Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka and with the Advance Sensors & Embedded Controls System (ASECs) research group. His research interests include power electronics and control systems such as DC-DC converter, robust control, and hybrid control.

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.

Radi Husin Ramlee acquired his B.Eng Electrical (Electronics) from Universiti Teknologi Malaysia in 2008 and M.Sc in Analogue & Digital IC Design from Imperial College, UK in 2009. He is currently an academician from Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka (UTeM). His research interest is in broadly areas of FPGA applications, digital hardware design, algorithm implementation in FPGA and CMOS ageing analysis.

Haslinah binti 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.