Enhanced Arbiter PUF Construction Model to Strengthening PUF-based Authentication

Rizka Reza Pahlevi
Graduate School of Informatics
Nagoya University
Nagoya, Japan
e-mail: pahlevirr@net.itc.nagoya-u.ac.jp

Hirokazu Hasegawa
Center for Strategic Cyber
Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: hasegawa@nii.ac.jp

Yukiko Yamaguchi
Information Technology Center
Nagoya University
Nagoya, Japan
e-mail: yamaguchi@itc.nagoya-u.ac.jp

Hajime Shimada
Information Technology Center
Nagoya University
Nagoya, Japan
e-mail: shimada@itc.nagoya-u.ac.jp

***Abstract*—In recent years, ensuring robust security in digital systems has become increasingly challenging, particularly in the realm of authentication. Physical Unclonable Functions (PUFs) have emerged as a promising solution due to their intrinsic ability to leverage manufacturing variations to produce unique and unpredictable responses. This paper presents a novel arbiter PUF construction designed to enhance authentication. The proposed PUF incorporates a cyclic model with four crossed lines in the signature generator to improve overall security. Extensive evaluations on six different Field Programmable Gate Array (FPGA) boards demonstrate that the proposed arbiter PUF achieves ideal levels of uniqueness (40.52% to 58.17%), bit aliasing (48.52% to 60.03%), reliability (80.98% to 96.49%), and balanced uniformity (47.95% to 61.40%). Additionally, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are maintained within acceptable limits (1.59% to 2.49% for FAR and 1.13% to 2.35% for FRR). Compared to existing arbiter PUF designs, our proposed model shows significant improvements in key security metrics, underscoring its potential for robust and secure authentication applications.**

Keywords-physical unclonable functions; authentication; arbiter PUF.

I. INTRODUCTION

In recent years, the domain of security has encountered increasingly challenging issues, particularly in the realm of authentication [1]–[4]. As technological advancements continue to accelerate, the methods employed by malicious entities have also evolved, necessitating the development of more robust security solutions. One promising area of research that has garnered substantial attention is the utilization of PUFs. PUFs capitalize on the inherent randomness introduced during the manufacturing processes of physical devices [2], [5]–[11]. This randomness results in unique and unpredictable responses when a device is queried, rendering it difficult to replicate or predict. Therefore, these distinctive characteristics theoretically position PUFs as a viable solution for generating secure authentication token.

Silicon-based PUFs represent a prominent subset of PUF technologies, offering solutions that can be seamlessly integrated with other systems. Among silicon-based PUFs, delay-based PUFs are particularly notable for their reduced bias compared to memory-based PUFs and their ability to exploit a wider range of manufacturing variables [1], [2], [10]–[16]. A prime example of delay-based PUFs is the arbiter PUF, developed in 2004 [17], [18], which exemplifies a delay-based PUF construction model. The arbiter PUF is classified as a weak PUF and is frequently targeted by various attacks. One common vulnerability is its susceptibility to statistical model attacks, which exploit the correlation between the Challenge-Response Pairs (CRPs) of the arbiter PUF, underscoring its inadequate security properties. Several studies have explored methods to improve the security of arbiter PUFs. One approaches employed an efficient XOR arbiter PUF to bolster uniqueness and security [3]. This efficient XOR arbiter PUF resulting in significant improvements in uniqueness. However, when evaluating PUFs, it is crucial to consider both their intended applications and their security characteristics. Consequently, a significant body of research focuses on designing or enhancing PUFs to meet these stringent security requirements [16], [19].

This study proposed arbiter PUF construction. While it may initially appear similar to other delay-based PUFs, our research demonstrates its capability to enhance and maintain nearly ideal secure PUF attributes. Compared to other arbiter PUF models, such as the XOR arbiter PUF, flip-flop arbiter PUF, and traditional arbiter PUF, our proposed arbiter PUF exhibits superior or nearly ideal security features. For a thorough security assessment, we propose a comprehensive PUF security evaluation. This evaluation measures the level

of protection provided by the PUF, encompassing metrics such as FAR, FRR, uniqueness, reliability, uniformity, and bit aliasing. Additionally, we implemented our PUF construction on six different FPGA boards to validate its effectiveness and reliability across varied hardware environments.

The remaining part of this article is organized as follows. Section II discusses previous research aimed to improved arbiter PUF. Section III describes the construction of the proposed arbiter PUF and evaluation metrics. Section IV discusses the collection of the dataset, the experimental results and provides further discussion about the proposed arbiter PUF. Finally, Section V concludes the work and outlines the future research plan.

II. Related work

Arbiter PUF is a primer example of delay-based PUF, which was developed in 2004 [17], [18], that notable for their reduced bias compared to memory-based PUFs. The arbiter PUF is typically constructed using two lines, each consisting of a number (N) of 2-1 multiplexers (MUX gates). Several studies have been conducted to enhance the performance of arbiter PUFs. Machida et al. [20] proposed a arbiter PUF construction aimed at improving unpredictability. This unpredictability was measured through prediction rate, uniqueness, randomness, and steadiness. They introduced both conventional arbiter PUFs and double arbiter PUFs. The double arbiter PUFs were constructed by XORing the outputs of multiple conventional arbiter PUFs. Their research, tested on three FPGAs, found that the conventional arbiter PUFs exhibited better steadiness compared to the double arbiter PUFs. However, both types generally achieved near-ideal randomness and uniqueness. Mahalat et al. [21] proposed a Path-Changing Switch (PCS) based arbiter PUF to address the low uniqueness issue in conventional arbiter PUFs. The PCS comprised four inverters and three MUXes. Implemented on fifteen Xilinx FPGAs, the PCS-based arbiter PUF achieved 49.81% uniqueness, 49.77% uniformity, and 98.19% reliability (steadiness). Anandakumar et al. [3] introduced an efficient XOR arbiter PUF to tackle poor uniqueness. This design consisted of three blocks of XOR PUFs, with each block's output captured by an arbiter. The arbiter outputs were stored in a 15-bit shift register, and the final response was obtained by XORing the golden responses from each shift register. Their efficient XOR arbiter PUF achieved 48.69% uniqueness, 50.73% uniformity, and 99.41% reliability. Yang et al. [22] proposed a arbiter PUF using improved switch components to address poor uniqueness and high resource consumption on FPGAs. To optimize resource usage, they introduced Programmable Delay Lines (PDLs) and MUXes. Their PDL + MUX arbiter PUF achieved 45.2% uniqueness and 0.357% steadiness (with the ideal steadiness value being 0%).

To ensure PUFs can be used for security purposes, such as authentication, they must be thoroughly evaluated. We categorize the evaluation into two types: classical PUF evaluations and PUF authentication-specific evaluations. The classical PUF evaluations include uniqueness, uniformity, and steadiness. The PUF authentication-specific evaluations include bit-aliasing, FAR, and FRR. Uniqueness, one of the most commonly used metrics, measures the correlation between chips using the same CRP and evaluates the differences between one chip and others. Achieving an ideal uniqueness value is crucial to avoid misidentification of the CRP from a particular chip. However, measuring uniqueness alone is not sufficient. Bit-aliasing complements uniqueness by ensuring no shared variable or systemic bias affects both chips similarly. This metric guarantees that input from a PUF to different chips will produce distinct output patterns, reducing security risks like brute force and replay attacks. Nevertheless, addressing bias alone is not enough; the composition of the PUF output must also be evaluated.

Uniformity measures the balance between bits '1' and '0' in the PUF output, ideally aiming for equal distribution to enhance security by reducing the likelihood of brute force attacks. Ensuring that PUF outputs are unique, free of bias, and uniform is necessary, but these metrics must be supported by reliability. Steadiness evaluates how consistent the output is when the same input is applied, often measured by the Hamming distance. Ideally, steadiness should be zero, meaning no bit errors occur; however, due to inherent noise during the PUF process, achieving zero steadiness is challenging, necessitating error correction mechanisms. To measure authentication performance, FAR and FRR are used. FAR measures how often incorrect PUF outputs are accepted in authentication systems, while FRR measures how often correct PUF outputs are rejected. In biometric systems, FAR and FRR below 2.5% are considered acceptable, and this benchmark is used for PUFs as well. Balancing FAR and FRR is challenging because reducing one often increases the other.

III. Improved Arbiter PUF Construction for Robust Authentication

A. PUF Construction Model

The proposed arbiter PUF consists of two main components: the signature generator and the arbiter. The signature generator is responsible for producing the signal and comprises four lines, each containing a series of MUX gates. At first glance, the proposed arbiter PUF resembles the double arbiter PUF proposed by Machida et al. [20], but it incorporates significant differences. The proposed arbiter PUF consists of four sets of lines instead of two sets. The increased number of lines is intended to maintain circuit delay, thereby reducing bias caused by some paths having minimal circuit delay. Additionally, the cyclic model aims to ensure fair circuit delay by evenly distributing the signal across all paths. This crossing pattern facilitates a more efficient and manageable physical design process while ensuring that signal travel times from inputs to outputs are balanced across all four paths. By maintaining circuit delay through fair path creation and signal distribution, the PUF quality is potentially enhanced. The circuit topology of the proposed arbiter PUF is illustrated in Figure 1. For the arbiter component, we utilized elements from conventional

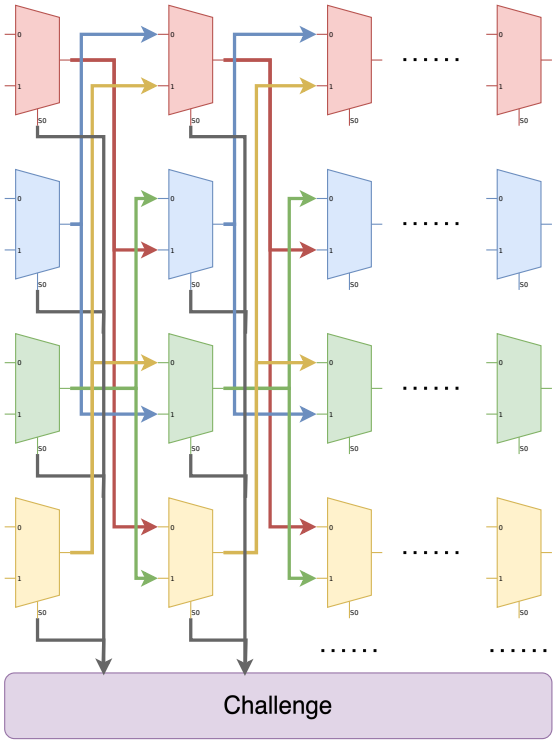

Figure 1. Signature generator of proposed arbiter PUF

arbiter PUF. The final MUX gates in the series of signature generators produce a spike signal, which is then distributed to multiple D Flip-Flops.

B. Security Evaluation Metric

1) Uniqueness: Ideally, the Hamming distance between responses to the same challenge from different chips should average around 50% of the total response size. To quantify this, a cross-measurement of the Hamming distance between responses from different chips is necessary. The uniqueness is calculated using (1).

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

In (1), *n* represents the number of responses obtained from the same challenge across different chips. R_i and R_j denote the PUF responses from the *i*-th and *j*-th chips, respectively, while $HD(R_i, R_j)$ is the Hamming distance between these responses. The term *m* is the bit length of the PUF response.

2) Bit aliasing: Ideally, the bit-aliasing value should be close to 50%, indicating a balanced distribution and enhancing security. Equation (2) is used to calculate bit-aliasing.

$$BA(n) = \frac{1}{N} \sum_{i=0}^{R-1} r_{i,n} \quad (2)$$

In (2), *N* represents the number of challenges used to generate responses from the PUF chip, and $r_{i,n}$ denotes the *n-th* bit of the response generated from the *i-th* challenge. The index *i* ranges from 0 to *R-1*, where *R* is the total number of collected responses.

3) Uniformity: Ideally, the distribution should be equal, with each bit appearing 50% of the time. Equation (3) is used to measure uniformity.

$$Uniformity = \frac{1}{n} \sum_{l=1}^{n} R_{i,l} \quad (3)$$

In (3), *n* represents the number of repeated responses taken for the same challenge, and $R_{i,l}$ denotes the *i-th* bit of the response generated in the *l-th* repetition. The index *l* ranges from 1 to *n*, covering all repetitions of the collected responses.

4) Steadiness: Ideally, a PUF chip should always provide a consistent and reliable response to the same challenges. The bit deviation in response can be quantified using intra-class Hamming Distance (HD_{intra}). The intra-class Hamming distance is calculated using (4).

$$HD_{\text{intra}} = \sum_{i=1}^{k} |x_i - x_i'| \quad \text{where} \quad D = \begin{cases} 0 & \text{if } x = x' \\ 1 & \text{if } x \neq x' \end{cases} \quad (4)$$

In (4), *k* is the length of the PUF response, x_i represents the *i*-th bit of the response, and $x\prime_i$ represents the corresponding *i*-th bit from another response to the same challenge.

5) FAR and FRR: Ideally, both FAR and FRR should be zero, indicating that the PUF responses are perfectly unambiguous. If the distribution of the intra-class and inter-class Hamming distances follows a Gaussian distribution, FAR and FRR can be statistically determined. The FRR is calculated using (5).

$$FRR = \frac{1}{\sigma_{\text{intra}}\sqrt{2\pi}} \int_{HD_{\max}}^{\infty} \exp\left(-\frac{1}{2}\left(\frac{x - \mu_{\text{intra}}}{\sigma_{\text{intra}}}\right)^2\right) dx \quad (5)$$

In (5), HD_{max} represents the maximum Hamming distance allowed to accept a response, μ_{intra} denotes the mean of the intra-class Hamming distances, and σ_{intra} is the standard deviation of the intra-class Hamming distances. Similarly, the FAR is calculated using (6).

$$FAR = \frac{1}{\sigma_{\text{inter}}\sqrt{2\pi}} \int_{-\infty}^{HD_{\max}} \exp\left(-\frac{1}{2}\left(\frac{x - \mu_{\text{inter}}}{\sigma_{\text{inter}}}\right)^2\right) dx \quad (6)$$

In (6), μ_{inter} represents the mean of the inter-class Hamming distances, and σ_{inter} represents the standard deviation of the inter-class Hamming distances.

IV. Result and Discussion

A. Collection of Dataset

For this study, we implemented our proposed arbiter PUF construction on six different FPGA boards. The specific boards used are as follows: Cyclone V SE 5CSEMA4U23C6N (referred to as CHIP 1), Cyclone V SE 5CSEBA6U23I7 (referred

to as CHIP 2), Cyclone V GT 5CGTFD9E5F35C7N (referred to as CHIP 3), Cyclone V SE 5CSEBA6U23I7 (a second board, referred to as CHIP 4), MAX10 10M04SCE144C8 (referred to as CHIP 5), and Cyclone IV EP4CE22F16C6 (referred to as CHIP 6). To evaluate the performance and reliability of the PUFs, we sent 10,052 different challenges to each board. For every challenge, 1,000 response samples were collected, resulting in a comprehensive dataset. In total, we gathered 10,052,000 response samples per chip, amounting to a grand total of 60,312,000 dataset entries across all six chips.

B. Security Evaluation Result

1) Uniqueness: Utilizing (1), the average Hamming distance observed was close to the ideal uniqueness, indicating a high level of uniqueness and distinctiveness between the responses from different chips. Table I shows the results of the uniqueness measurements from the six FPGA boards.

The results show that the average Hamming distances between the chips were mostly above 50%. This indicates a high level of uniqueness and distinctiveness in the PUF responses across different chips. Notably, the Hamming distances ranged from 40.52% (between CHIP 3 and CHIP 6) to 58.17% (between CHIP 1 and CHIP 6), thereby supporting the effectiveness of our PUF design in providing unique responses.

2) Bit aliasing: Utilizing (2), the bit-aliasing value was found to be close to the ideal 50%, demonstrating that the responses are unbiased and originate from inherent manufacturing variations. Table II shows the results of bit aliasing for the proposed arbiter PUF.

The bit aliasing results reveal that the values are generally close to the ideal 50%. The values range from 48.52% (between CHIP 1 and CHIP 5) to 60.03% (between CHIP 3 and CHIP 6), with most values clustering around the 50% mark. These results confirm that the randomness in the PUF responses is primarily due to inherent manufacturing variations, thereby supporting the robustness of the PUF design.

3) Uniformity: Utilizing (3), the uniformity was found to be close ideal. Table III shows the results of the uniformity measurements for the proposed arbiter PUF. The uniformity results show that the average result is generally close to the ideal 50%. CHIP 2, with an average of 47.95%, is the closest to this ideal value, indicating a well-balanced distribution. On the other hand, CHIP 3 has the highest average at 61.40%, which is further from the ideal but still demonstrates a reasonable level of uniformity.

4) Steadiness: Utilizing (4), the steadiness was found to be close to ideal. Table III shows the results of the steadiness measurements for the proposed arbiter PUF. The results indicate a range of average intra-class Hamming distances across different chips, suggesting varying levels of steadiness. CHIP 3 exhibited the lowest average intra-class Hamming distance at 4.4920 (96.49%), indicating the highest level of consistency among the tested chips. In contrast, CHIP 2 had the highest average intra-class Hamming distance at 24.3330 (80.98%), suggesting more variability in its responses.

5) FAR and FRR: Utilizing (6), the FAR was found to be under 2.5%. Tables IV present the detailed results of FAR for the proposed arbiter PUF. The FAR results in range from 1.5940% (between CHIP 3 and CHIP 6) to 2.4940% (between CHIP 4 and CHIP 5), indicating a relatively low rate of false acceptances. Utilizing (5), the FRR was found to be under 2.5%. Table IV is shown the result of FRR. The values range from 1.1281% (CHIP 3) to 2.3465% (CHIP 2). Both FAR and FRR values are below 2.5%, which is considered acceptable for robust authentication systems.

C. Discussion

The evaluation of the proposed arbiter PUF across various metrics demonstrates its effectiveness and robustness. The uniqueness metric, measured by the Hamming distance between responses from different chips to the same challenge, yielded values close to the ideal 50%, indicating distinct and distinguishable responses across different chips (Table I). This high level of uniqueness reduces the likelihood of misidentification and enhances system security. Bit aliasing, assessed to ensure no systemic bias, showed values close to the ideal 50%, ranging from 48.52% to 65.61%, indicating minimal bias and confirming the randomness in the PUF responses originates from inherent manufacturing variations shown in Table II. The average uniformity values were generally close to the ideal 50% as shown in Table III, with CHIP 2 achieving the closest average at 47.95%. This balanced uniformity enhances the security against brute force attacks and contributes to the reliability of the PUF.

The results of steadiness, shown in Table III, reveal varying levels of steadiness across different chips. CHIP 3 exhibited the highest consistency of 4.492 (96.49%), while CHIP 2 showed more variability of 24.333 (80.98%). These findings highlight areas for improvement in ensuring more uniform steadiness across different chips, which is crucial for enhancing the reliability of the PUF. The FAR and FRR metrics are critical for assessing the authentication performance of the PUF. As detailed in Tables IV, the FAR values ranged from 1.5940% to 2.5145%, and the FRR values ranged from 1.1281% to 2.3465%. The low rates of false acceptances and rejections confirm that the system effectively distinguishes between valid and invalid responses, thereby enhancing the overall security and usability of the PUF. The high level of uniqueness, minimal bit aliasing, balanced uniformity, consistent steadiness, and low FAR and FRR values collectively underscore the superior performance of our PUF design. These results compare favorably with other arbiter PUF research, highlighting the advancements and contributions of our work to the field of PUF-based security solutions.

D. Comparison from previous research

To contextualize our findings, we compared our results with previous arbiter PUF research as summarized in Table V. The table shows that our proposed PUF achieves favorable results across various metrics. Specifically, our PUF demonstrates a FAR range of 1.5940% to 2.5145% and an FRR range of

TABLE I
UNIQUENESS OF THE PROPOSED ARBITER PUF

	CHIP 1	CHIP 2	CHIP 3	CHIP 4	CHIP 5	CHIP 6
CHIP 1	–	56.02%	54.19%	55.12%	53.64%	58.17%
CHIP 2	56.02%	–	51.05%	52.61%	50.01%	48.42%
CHIP 3	54.19%	51.05%	–	51.75%	53.78%	40.52%
CHIP 4	55.12%	52.61%	51.75%	–	52.99%	50.58%
CHIP 5	53.64%	50.01%	53.78%	52.99%	–	50.23%
CHIP 6	58.17%	48.42%	40.52%	50.58%	50.23%	–

TABLE II
BIT ALIASING OF THE PROPOSED ARBITER PUF

	CHIP 1	CHIP 2	CHIP 3	CHIP 4	CHIP 5	CHIP 6
CHIP 1	–	50.56%	53.74%	52.39%	48.57%	49.89%
CHIP 2	49.73%	–	54.53%	53.81%	51.41%	55.85%
CHIP 3	53.14%	56.08%	–	57.02%	49.28%	60.03%
CHIP 4	51.91%	54.09%	56.85%	–	49.98%	56.82%
CHIP 5	48.52%	53.60%	51.38%	51.47%	–	54.57%
CHIP 6	49.38%	57.79%	65.61%	57.33%	52.31%	–

TABLE III
UNIFORMITY AND STEADINESS OF THE PROPOSED ARBITER PUF

Chip	Uniformity (average)	Steadiness(HD_{intra}) (average)
CHIP 1	61.16%	88.63%
CHIP 2	47.95%	80.98%
CHIP 3	61.40%	96.49%
CHIP 4	53.04%	87.18%
CHIP 5	43.29%	86.88%
CHIP 6	51.94%	93.60%

1.1281% to 2.3465%, which are comparable to or better than those reported in other studies. In terms of uniqueness, our PUF's range of 48.52% to 65.61% is slightly higher than the ideal 50%, but still within an acceptable range. This indicates a high level of distinctiveness in our PUF responses. Reliability, measured through steadiness, showed a range of 96.49% to 80.98%, which is competitive with other designs. While the 4-1 Double APUF by Machida et al. [20] achieved nearly ideal uniformity values, our design maintains a reasonable balance, further enhancing security against brute force attacks. The results from Lin [23], Aknesil [24], and Yang [22] provide additional benchmarks, where our PUF consistently shows competitive performance.

V. CONCLUSION

The proposed arbiter PUF construction model presents significant advancements in the field of PUF-based authentication solutions. By integrating a cyclic crossing pattern within the signature generator, our design effectively increase the security, leading to more secure for authentication purpose. Comprehensive testing on six FPGA boards has validated the effectiveness of our design, demonstrating ideal performance in uniqueness (40.52% - 58.17%), reliability (96.49%), uniformity (47.95% - 61.40%), and bit aliasing (48.52% - 60.03%) compared to traditional arbiter PUF models. The measured FAR and FRR further confirm the robustness of our PUF in secure authentication applications. We found the FAR in range of 1.59% - 2.494%, and FRR in range 1.13% - 2.35%. In conclusion, our proposed arbiter PUF construction offers a promising solution for enhancing digital security through improved authentication mechanisms. The advancements presented in this paper contribute significantly to the development of more secure and reliable PUF technologies, paving the way for their widespread adoption in various security-critical applications. Despite these achievements, there are still areas for potential improvement. Future work could focus on optimizing the PUF architecture for even lower FAR and FRR values and introducing a method to increase the reliability. Additionally, implementing our PUF design in a broader range of hardware environments could provide deeper insights into its versatility and scalability.

ACKNOWLEDGMENT

This research has been supported by the Kayamori Foundation of Informational Science Advancement with grand number K35 Research XXVIII No. 632

REFERENCES

[1] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "A PUF-based mutual authentication scheme for Cloud-Edges IoT systems," *Future Gener. Comput. Syst.*, vol. 101, pp. 246–261, Dec. 2019.

[2] M. Barbareschi, A. De Benedictis, and N. Mazzocca, "A PUF-based hardware mutual authentication protocol," *J. Parallel Distrib. Comput.*, vol. 119, pp. 107–120, Sept. 2018.

[3] N. N. Anandakumar, M. S. Hashmi, and M. A. Chaudhary, "Implementation of efficient xor arbiter puf on fpga with enhanced uniqueness and security," *IEEE Access*, vol. 10, pp. 129832–129842, 2022.

[4] R. R. Pahlevi, P. Sukarno, and B. Erfianto, "Secure MQTT PUF-Based key exchange protocol for smart healthcare," *Jurnal Rekayasa Elektrika*, vol. 17, pp. 107–114, June 2021.

[5] Y. Guo, T. Dee, and A. Tyagi, "Barrel shifter physical unclonable function based encryption," *Cryptography*, vol. 2, p. 22, Aug. 2018.

[6] I. Papakonstantinou and N. Sklavos, "Physical unclonable functions (PUFs) design technologies: Advantages and trade offs," in *Computer and Network Security Essentials*, pp. 427–442, Cham: Springer International Publishing, 2018.

[7] A. Tsuneda, "Various auto-correlation functions of m-bit random numbers generated from chaotic binary sequences," *Entropy*, vol. 23, no. 10, 2021.

TABLE IV
FAR AND FRR OF THE PROPOSED ARBITER PUF

	FAR						FRR
	CHIP 1	**CHIP 2**	**CHIP 3**	**CHIP 4**	**CHIP 5**	**CHIP 6**	
CHIP 1	–	2.1825%	1.8879%	2.0153%	2.4738%	1.8380%	1.7899%
CHIP 2	2.1825%	–	2.2582%	2.3246%	2.4935%	2.4553%	2.3465%
CHIP 3	1.8879%	2.2582%	–	1.8419%	2.4910%	1.5940%	1.1281%
CHIP 4	2.0153%	2.3246%	1.8419%	–	2.4940%	1.8631%	2.2095%
CHIP 5	2.4738%	2.4935%	2.4910%	2.4940%	–	2.5077%	1.9949%
CHIP 6	1.8380%	2.4553%	1.5940%	1.8631%	2.5077%	–	1.4496%

TABLE V
COMPARISON OF PROPOSED PUF TO PREVIOUS ARBITER PUFS

Arbiter PUF Research	PUF Security Evaluation					
	FAR	FRR	Uniqueness	Steadiness(HD_{intra})	Uniformity	Bit Aliasing
Ideal	0%	0%	50%	100%	50%	50%
Conventional APUF [20]	–	–	4.72% / 4.96% / 4.44%	99.24% / 99.17% / 99.55%	53.81% / 56.53% / 54%	–
2-1 Double APUF [20]	–	–	41.36% / 49.70% / 48.06%	92.21% / 88.8% / 89.95%	55.19% / 31.4% / 50.63%	–
4-1 Double APUF [20]	–	–	50.46% / 51.34% / 48.78%	65.04% / 81.01% / 74.15%	55.67% / 54.76% / 54.59%	–
Path Changing Switch (PCS) [21]	–	–	49.81% / 51.34%	Avg 0.35% / Avg 1.49%	Avg **49.77%** / Avg 57.64%	–
APUF [23]	–	–	42.7%	96%	–	–
APUF [24]	–	–	15.15%	0.45% - 0.5%	98%	–
APUF [22]	–	–	45.2%	–	–	–
FOXFFAPUF [25]	–	–	42% / 44%	–	–	–
Efficient XOR APUF [3]	–	–	48.69%	99.41%	50.73%	–
Our Proposed PUF	**1.5940%** - **2.4940%**	**1.1281%** - **2.3465%**	**40.52%** - 58.17%	**96.49%** to 80.98%	47.95% - 61.40%	**48.52%** - 60.03%

[8] T. Ichiki and A. Tsuneda, "Study on security enhancement of 64-bit NFSR-based block cipher systems with ring structure," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 842–844, Oct. 2018.

[9] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (puf)-based security solutions for internet of things," *Computer Networks*, vol. 183, p. 107593, 2020.

[10] H. Xu, J. Ding, P. Li, F. Zhu, and R. Wang, "A lightweight RFID mutual authentication protocol based on physical unclonable function," *Sensors*, vol. 18, no. 3, p. 760, 2018.

[11] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, pp. 1327–1340, Oct. 2017.

[12] H. Kang, Y. Hori, T. Katashita, and M. Hagiwara, "The implementation of fuzzy extractor is not hard to do: An approach using puf data," in *Proceedings of the 30th Symposium on Cryptography and Information Security, Kyoto, Japan*, pp. 22–25, 2013.

[13] C. Bohm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. Springer Science & Business Media, Oct. 2012.

[14] K. Mahmood, S. Shamshad, M. Rana, A. Shafiq, S. Ahmad, M. A. Akram, and R. Amin, "PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication," *Journal of Information Security and Applications*, vol. 61, p. 102900, Sept. 2021.

[15] W. Xiong, A. Schaller, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, S. Katzenbeisser, and J. Szefer, "Run-time accessible DRAM PUFs in commodity devices," in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 432–453, 2016.

[16] J. R. Wallrabenstein, "Implementing authentication systems based on physical unclonable functions," *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 790–796, 2015.

[17] J. Lee, D. Lim, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, pp. 176–179, 2004.

[18] D. Lim, J. Lee, B. Gassend, G. Suh, M. van 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.

[19] Y. Nozaki and M. Yoshikawa, "Secret sharing schemes based secure authentication for physical unclonable function," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pp. 445–449, 2019.

[20] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new arbiter puf for enhancing unpredictability on fpga," *The Scientific World Journal*, vol. 2015, no. 1, p. 864812, 2015.

[21] M. H. Mahalat, S. Mandal, A. Mondal, B. Sen, and R. S. Chakraborty, "Implementation, characterization and application of path changing switch based arbiter puf on fpga as a lightweight security primitive for iot," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 27, nov 2021.

[22] J. Yang, X. Yu, and R. Wei, "A low resource consumption arbiter puf improved switch component design for fpga," *Journal of Physics: Conference Series*, vol. 2221, p. 012011, may 2022.

[23] L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Design and validation of arbiter-based pufs for sub-45-nm low-power security applications," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1394–1403, 2012.

[24] C. Aknesil and E. Dubrova, "An fpga implementation of 4×4 arbiter puf," in *2021 IEEE 51st International Symposium on Multiple-Valued Logic (ISMVL)*, pp. 160–165, 2021.

[25] R. Sushma and N. Murty, "Feedback oriented xored flip-flop based arbiter puf," in *2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 1444–1448, 2018.