Security Analysis of Digital-Based Physically Unclonable Functions: Dataset Generation, Machine Learning Modeling, and Correlation Analysis

Enas Abulibdeh[a], Shimaa Naser[b], Hani Saleh[a], Baker Mohammad[a], Mahmoud Al-Qutayri[a], Sami Muhaidat[b]

[a]*System on Chip Lab, Computer and Communication Engineering, Khalifa University, Abu Dhabi, 127788, Abu Dhabi, UAE*
[b]*KU 6G Center, Computer and Communication Engineering, Khalifa University, Abu Dhabi, 127788, Abu Dhabi, UAE*

Abstract

Physically unclonable functions (PUFs) are circuit primitives that offer a promising and cost-effective solution for various security applications, such as integrated circuits (IC) counterfeiting, secret key generation, and lightweight authentication. PUFs leverage semiconducting variations of ICs to extract intrinsic responses based on applied challenges, establishing unique challenge-response pairs (CRPs) for each device. The security analysis of PUFs is crucial to identify the device weaknesses and ensure response integrity. Accordingly, CRP-based examination plays a major role in defining the resistivity of the block against general and modeling-based attacks. Such analysis requires an updated and representative dataset for training and evaluation. However, there is a lack of benchmark datasets for assessing the effectiveness and resistance of PUF devices. Motivated by this, in this work, a comprehensive dataset from two different architectures a digital-based PUF implemented on a field programmable gate array (FPGA). The dataset involves responses from FPGAs with the maximum number of collected CRPs reaching 300K records. The dataset provides a significant number of CRPs for a multi-bit response, where the spatial and temporal adjacency are implicitly defined in the extracted CRPs. Moreover, we investigate different approaches utilizing the generated dataset such as machine learning-based modeling, correlation analysis, and entropy analysis. The CRPs are employed to train linear and nonlinear Support Vector Machine (SVM) models, and the prediction accuracy of SVM models is used as an indicator of the PUF's vulnerability to

modeling attacks. As the prediction accuracy does not exceed 65% over 10K CRPs, the extracted dataset sufficiently verifies the resiliency of the device against ML-based modeling attacks. Additionally, Pearson's coefficient is computed on a 10K-bit vector to determine the correlation between the bits of the response. The calculations expose some correlations between ± 0.25, which warns of potential threads. Finally, the paper discusses some potential future research directions and challenges that are envisioned to enhance the security performance of PUFs.

Keywords: Correlation, CRPs, entropy, FPGA, machine learning, modeling, PUF, RO, security analysis

---

1. Introduction

The Internet of Things (IoT) plays a vital role in diverse applications, by enabling seamless connectivity and efficient data transfer allowing for chanced operational efficiency and efficient decision-making. The exchange of information in the IoT ecosystem encompasses a vast array of information, including users' locations, vital signs of the human body, and the realm of autonomous vehicles, to mention just a few instances. Nevertheless, due to the broadcasting nature of the Wireless links, they are subject to various forms of attacks. According to Kaspersky, 1.51 billion IoT breaches were reported in the first half of 2021. Although conventional cryptography-based approaches have gained significant popularity for ensuring secure data communication and authentication, their integration with resource-limited IoT devices poses a major challenge. The complexity associated with these sophisticated schemes tends to drain the limited resources of IoT devices. Hence, it has become imperative to address this issue by exploring alternative lightweight security solutions. In this regard, physical unclonable function (PUF) is envisioned as a promising security paradigm that supports low-cost authentication protocols and key generation and protects integrated circuits (ICs) from counterfeiting [1]. PUF has merged as a low-cost security primitive that eliminates the need for intricate key generation processes and secure storage of sensitive information. Recently, different commercial systems have adopted PUF as an integral component of their security architecture. For instance, Silicon Labs seamlessly integrates PUF technology with advanced security software functionalities in their Wireless Gecko Series 2 platform. Similarly, Maxim comprises PUF in the MAX32520 ChipDNA Secure ARM

Cortex M4 microcontroller, which delivers multi-level protection.
Conceptually, a PUF device exploits the variation of the physical characteristics of the underlying hardware such as wire connections. More specifically, the PUF utilizes a designated input known as the challenge C to define the physical properties. Due to its unique nature, PUF produces a distinct and unpredictable output known as the response R. It is worth noting that R varies from one device to another as shown in Figure 1. Thus, by applying the same challenge C to three PUF devices X, Y, and Z, three different responses are produced, namely R_Y, R_X, and R_Z, respectively. Intrinsic electronic PUF or Silicon PUF (SPUF) utilizes the process variations of ICs. For instance, the ring oscillator PUF (ROPUF) is a delay-based SPUF that evaluates the delay between two ROs that incorporate logic gates and wires.

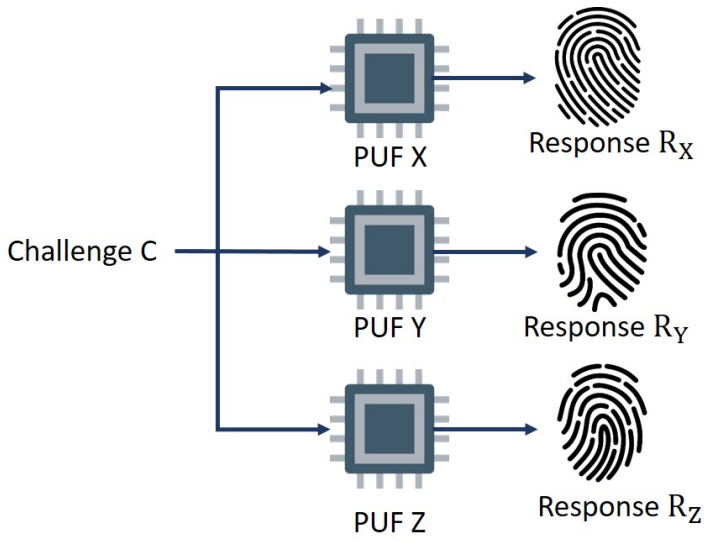


Figure 1: The uniqueness characteristic of PUF response over different devices of the same architecture, where $R_X \neq R_Y \neq R_Z$.

Nevertheless, the set of challenge-response pairs (CRPs) of a particular PUF device is susceptible to direct or indirect access by intruders who acquire the capability to clone the PUF device through the application of machine learning (ML) algorithms. This allows them to construct a model that can effectively forecast the PUF's responses with high accuracy. Therefore, it is of paramount importance for PUF designers to study the security vulnerabilities of the PUFs to develop more robust designs. In this regard, the CRP

dataset serves as a valuable tool for researchers to study the characteristics of PUFs and to develop tools to improve their security and robustness. Security analysis is another important tool that involves evaluating the resilience of PUF against different attacks. It is worth mentioning that PUF security analysis involves comprehensive tests and evaluations that identify PUFs' vulnerabilities and potential threats. A set of approaches for the analysis utilizes the CRPs dataset to mathematically or experimentally model the PUF's function such a security analysis requires an updated and representative dataset for training and evaluation. However, the scarcity of benchmark datasets for assessing the effectiveness and resistance of PUF devices poses a significant challenge. In the following subsection, we overview and discuss some of the available PUF datasets and their limitations.

2. Related Works

'The diversity of PUF architectures and their sources of randomness amplifies the importance of CRPs as they are used to validate the device and assess its security level. The Hybrid Boolean Networks (HBN)-based PUF [2] utilized BN as the source of the device's randomness, which overcomes the limitations of traditional physical properties such as gate delay. The resilience of the HBN PUF to ML-modeling attacks was verified using 1K CRPs. Similarly, Y. Jiang [3] enhanced the security of PUFs by improving the complexity of their structures. 65K records with a 40-bit challenge and 1-bit response each were used to rigorously analyze RO PUF with an additional modulus process [3]. Hu et al. [4] and Aghaie et al. [5] investigated the impact of system characteristics on the vulnerability of PUFs to ML-based modeling attacks. Additionally, Aghaie et al. [5] compared the performance of ML models based on simulated or actual CRPs. 65K CRPs were collected from the design [4], and obtained by running RO for 15.729ms. On the other hand, Aghaie et al. [5] extracted 1M CRPs from the Interpose PUF, where a 64-bit challenge was applied to produce a 1-bit response. Mursi et al. [6] proposed and implemented an XOR-based PUF on Artix®-7. The circuit elements were vertically placed, and a single-bit response was generated by applying a 64-bit challenge to collect 5M CRPs. Motivated by the above, this study presents the experimental methodology for extracting the CRPs dataset from an FPGA-based ROPUF. The extracted dataset consists of a maximum of 300K records and is provided as part of this work. The dataset is relatively large for a multi-bit response, in which the physical proximity

and the conical generation are implicitly defined. Table 1 presents a comparison between the dataset provided in this study and those published in the literature.

Table 1: The state-of-art published dataset and this work dataset.

	[2]	**[6]**	**[5]**	**[4]**	**This Work**
Structure	HBN	XOR	RO	RO	RO
CRPs Size (K)	1	5K	65	4	300
Challenge Length (bit)	256	64	40	40	32
Response Length (bit)	256	1	1	1	16
Generation Time (ms)	10^{-6}	-	-	15.7	10^{-5}

The paper also proposes various practical approaches to assess the security of the PUF device, including ML-based modeling, correlation analysis, and entropy analysis. Furthermore, two specific approaches are implemented and applied to the collected dataset.

3. Dataset Generation

The dataset generation involves designing and implementing the platform and then introducing efficient data-driven approaches for data collection.

3.1. Testing Platform

The testbed aims to extract a multi-bit RO-based PUF response implemented on an FPGA board. The PUF's logic was accurately placed to avoid any bias by the topology variation as shown in Figure 2. In specific, two ROs are placed vertically (yellow and pink) where the delay unit is constructed from four look-up tables (LUTs) and occupied by one FPGA slice (left). To facilitate challenge application and response collection, an AXI interface is attached to the PUF block and managed and accessed by the FPGA processor, Microblaze. FPGA communicates with the PC using a serial-parallel UART interface as shown in Figure 3. The implementation of the PUF, IPs connection, and bitstream generation are performed by Vivado 2019.2. Additionally, the Microblaze is programmed using Vitis 2022, which forwards the sent challenge to the PUF and returns the corresponding response to the

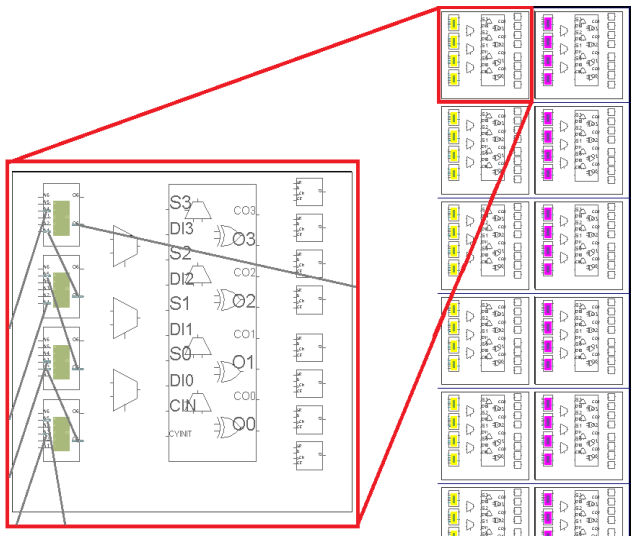


Figure 2: The FPGA placement of a delay unit in one slice (left) and the vertical placement of two ROs (right).

PC. Finally, MATLAB R2022b is used to develop a program on the PC's edge that generates the challenge, sends it to the FPGA through UART, and receives the response through UART. It is worth mentioning that we have generated the challenge randomly from a normal distribution. Figure 4 displays the great setup of the experiment components, which shows FPGA connected via UART cable to PC/USB port. MATLAB is running on a PC to manage the interfacing process.

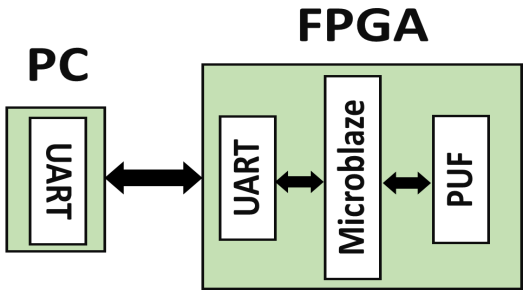


Figure 3: The testbed architecture, which includes PC and FPGA. FPGA runs and manages PUF block using the controller. At the same time, PC sends the challenge and receives the response of PUF to/from FPGA using a serial-parallel interface.

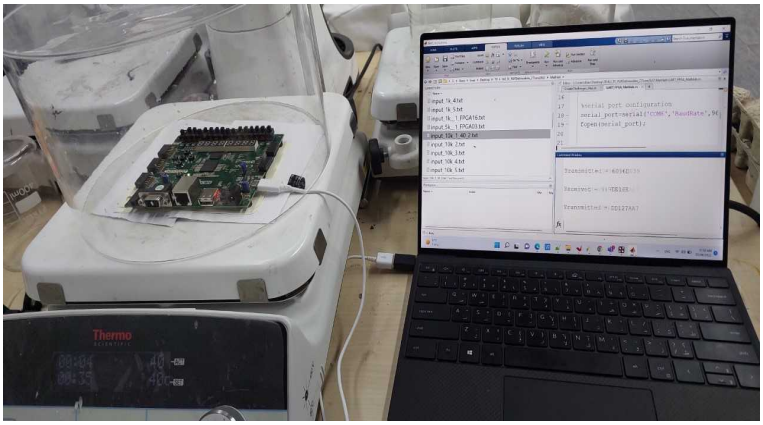


Figure 4: The actual setup of the testing platform. PC is running MATLAB code that continuously generates the challenge and receives the response. The programmed Microblaze on FPGA applies the challenge on the PUF and collects the response.

3.2. Data Generation

The datasets were extracted from two variants of RO PUF that were implemented in the FPGA. The CRPs from each architecture were collected and preserved in an independent repository. In each repository, an input challenge file was applied to 50 FPGAs that represent 50 PUF instances, and the corresponding responses were gathered from each and saved in an output response file. The data in the input and output files are aligned at the same offset, meaning that the corresponding entries in each file are related. For instance, the first line in the response file represents the output response obtained when applying the first line of the challenge file as input to the PUF device. The challenge and response are stored in hexadecimal format. Each challenge is a 32-bit string (8 hexadecimal digits), and the response size is either 32 or 16 bits depending on the underlying architecture. The adjacent bits in the response string are generated by identical circuit elements that are physically arranged in the same order in the target hardware. For example, the physical displacement between the first and fourth bits is three RO circuits. Each circuit loop in the RO PUF is vertically positioned over FPGA resources, with the adjacent loop placed at a horizontal offset. The CRPs are generated sequentially with an interleaving period of 10 ns at the circuit level. However, due to the communication between the FPGA and PC, there is an additional introduced delay. Moreover, the responses from both architectures were collected under different environmental conditions. The environmental

conditions involved temperature and voltage variations applied on the same PUF device and utilizing the same input file. Five supply voltages (including the nominal voltage 5V) and five temperatures (including the nominal temperature 25°C) were tested. The voltage and temperature were tested independently, for example, the temperature variation was applied while the supplying voltage was maintained on 5v.

4. Security Analysis

CRPs represent valuable resources for professionals to improve the security evaluation metrics of PUFs. In this context, examination methods concentrate on various aspects such as approaches that involve investigating the relationships between challenges and responses, often utilizing ML-based modeling techniques. Alternatively, some methods explore the correlations among the responses themselves. Other approaches have focused on analyzing the hardware capabilities and the implemented architecture to extract random responses, such as through entropy analysis. This study explores ML-based modeling, correlation, and entropy analysis as methodologies for effectively utilizing the dataset.

4.1. Machine Learning-Based Modeling

The behavior of the PUFs can be effectively represented through a set of collected CRPs [7]. This modeling approach does not require any auxiliary information and solely relies on computations performed on the CRPs themselves [8]. As a consequence, PUFs are susceptible to ML-based attacks [9], especially when CRPs are accessible outside the chip without any protection mechanisms in place. Constructed PUF models can take the form of numerical models derived from collected data or ML models trained on a sufficient number of CRPs [10]. The efficiency and simplicity of ML models present a significant threat to PUFs, making them vulnerable to ML-based modeling attacks. In the literature, various ML algorithms have been employed to predict PUF responses, including Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), K Nearest Neighbor (KNN), Support Vector Machine (SVM), kernel-based SVM, Evolutionary Strategies (ES), and Neural Network (NNet), with LR, SVM, and NNet showing dominant performance [8, 9, 10].

To assess the security of a PUF device, its resistance against ML-based modeling attacks is often considered. In this regard, SVM is a widely em-

ployed ML model in the literature. Additionally, the linear behavior exhibited by the delay-based PUFs is a suitable fit for SVM. Therefore, SVM with two kernels (linear and radial basis function) has been utilized in the present study. SVM is trained on 80% of the CRPs to independently predict the ninth bit of the response. The models are then trained and tested over 500, 1K, 5K, and 10K CRPs, as shown in Figure 5. It can be observed from the figure that on average, the response bit can be predicted with 65% accuracy using the non-linear kernel of SVM and 57% accuracy using the linear kernel. Hence, to predict multiple bits, an SVM model can be constructed for each bit individually. The prediction accuracy indicates the immunity of the attacked bit as a higher prediction accuracy implies that the bit is breakable by ML attacks, which partially reveals the true response. The rest of the response can be easily predicted with a brute-force attack.

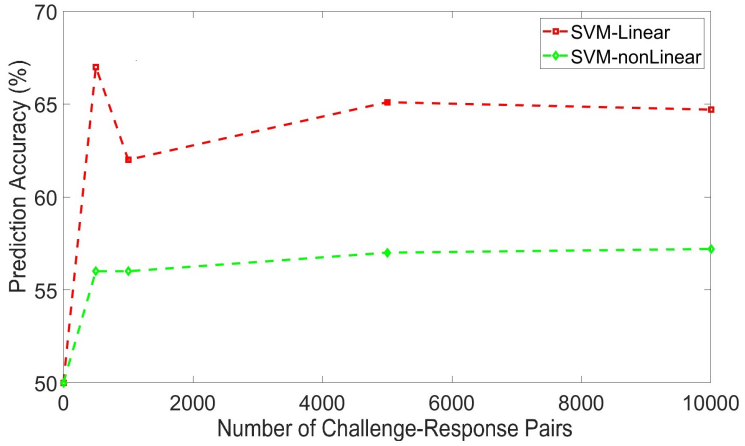


Figure 5: The prediction accuracy of the ninth bit of the PUF response utilizing SVM model with two kernels: linear and nonlinear.

4.2. Correlation Analysis

Various architectures, sources, and types of PUF devices have been proposed in the literature. As a result, PUF cells exhibit similarities due to spatial distribution, shared hardware elements, and sequential generation [11]. Consequently, conducting correlation tests between different variables proves to be a valuable tool for evaluating the degree of similarity or correlation between them. This is vital since if a subset of the correlated secret bits is exposed, an attacker can potentially predict the remaining ones. Generally,

the Pearson correlation test is utilized to assess the relationship between two variables. The Pearson coefficient (r) is described by Eq. 1.

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 \sum_{i=1}^{n}(y_i - \overline{y})^2}} \tag{1}$$

where n denotes the number of involved CRPs, x and y are the binary series of the compared bits, x_i and y_i are the bit values at offset i in both x and y vectors. It is important to highlight that the Pearson coefficient (r) ranges between -1 and 1. When $r = -1$, it indicates a strong negative relationship between the two variables, while a value of $r = +1$ indicates a strong positive relationship. Finally, if $r = 0$, it implies that the two variables are uncorrelated. Based on this, the correlation matrix is constructed for the given dataset based on the Pearson coefficient which is illustrated in Figure 6. The intersection of the row and column indicates the correlation coefficient between the corresponding bits of the PUF's response. The color of the matrix's cell reflects the correlation factor of intersected bits, while the main diagonal represents the correlation of each bit with itself. As the correlation coefficient is observed, the light red (or blue) implies that the coefficient is around ± 0.25, which means the neighbor bits are correlated due to the physical adjacency of their circuit elements.

Building upon prior analysis, the correlation may exist if the generators are physically placed close to each other, which is called spatial correlation. Similarly, the successive generations of the response utilizing the same hardware may introduce temporal correlation. Spatial correlation measures the relationship between two variables at different points in space. On the other hand, temporal correlation measures the relationship between two variables at different points in time. Spatial and temporal correlations emerge as distinct forms of correlation that encompass specific dimensions. The adjacency of the circuitry components of PUF cells may show similarities in the response bits. Moran's I, Geary's c, and Joint Count Statistic are the statistical tests that are suggested by W. Florian et al. [11] to conclude that the variables observed at one location are dependent or independent of the values of the same variable at neighboring locations. The relations between the output stream and the previous strings can also be investigated. Recurrent Neural Network along with Long-Short Term Memory (LSTM) and Transformer are suggested to analyze any temporal correlation. Such models accept M-bit response during the training phase and are used to predict xM bits. The

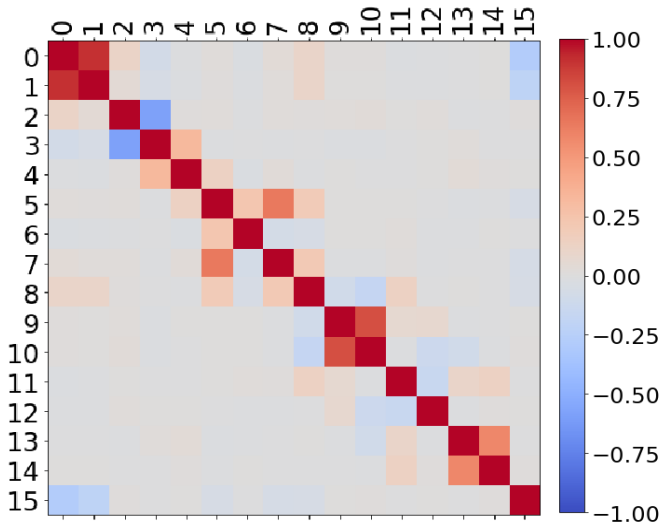


Figure 6: Person correlation coefficient of 16 response bits, where each bit is presented by a binary vector of length 10K. The results show a slight correlation between spatial neighbors.

value of x reflects the degree of correlation, where $\sim 0\%$ implies no relation and $\sim 100\%$ are highly correlated.

4.3. Entropy Analysis

Entropy serves as an indicator of the information contained within a PUF device. PUF structures with high entropy exhibit resistance against modeling-based attacks, including mathematical and ML-based modeling attacks. Evaluating entropy statistically involves employing various tests such as Shannon entropy, MinEntropy, conditional MinEntropy, Interchip hamming distance, and National Institute of Standards and Technology (NIST) tests. Context-tree weighting (CTW) and its variations [12] estimate the upper bound of the entropy that can be delivered by the device. CTW assumes that the generation of a binary string relies on a substring of length D, known as the context length. Thus, CTW represents PUF responses as a tree with a maximum depth of D, where any subsequence generates a graph of length l with $l < D$. The leaves of the tree correspond to all possible contexts present in the dataset, and their weighted probabilities can be computed based on the dataset. In this model, the edges of the tree represent the potential transitions from one symbol to another, forming substrings of

length l. The probabilities associated with these transitions can be calculated within the CTW framework. By employing CTW, it becomes possible to capture the statistical dependencies and structure within PUF responses, enabling the estimation of the maximum achievable entropy.

5. Research Directions

Performing security analysis based on CRPs is crucial for validating the usage of PUFs. However, certain obstacles hinder the effectiveness of their applications, including the lack of generalization, biasing effects, limited availability, and post-quantum analysis.

5.1. Lack of Generalization

The set of CRPs serves as a unique identifier for a specific PUF device and significantly influences the associated mathematical or empirical models. Consequently, these models cannot be easily generalized or applied to other PUF devices of the same architecture. Such challenge arises when analyzing strong PUFs that possess a large number of CRPs per device, sometimes reaching tens of millions. Developing a comprehensive and accurate model that encompasses the behavior of multiple devices into a single model becomes a complex task, and achieving convergence becomes uncertain. Addressing this challenge requires careful consideration of the device-specific characteristics and appropriate data analysis techniques such as data fusion, normalization, and augmentation. Furthermore, *Ensemble Learning* is a potential technique for handling this challenge by combining the predictions of multiple models with the aim to provide more generalized and accurate predictions.

5.2. Biasing Effect

The extraction mechanisms and architectures of PUFs are designed with the aim of minimizing bias effects. However, since PUFs rely on uncontrollable physical quantities for generating responses, there is a possibility of biases in the output. These biases can reduce the efficiency of utilizing PUFs' CRPs. To ensure a more balanced and uniform distribution of the output, post-extraction processes are necessary. In this regard, addressing the bias effects by performing post-processing on the extracted PUF responses is of significant importance. This involves excluding low-confidence bits, which are more likely to be affected by biases [13]. Another technique that can be

employed is temporal majority voting (TMV). In TMV, the PUF is sampled multiple times, and the response that appears most frequently among the samples is considered the true response [14]. This approach leverages the redundancy in the PUF output to mitigate the influence of biases. By selecting the majority response, the impact of biased samples can be reduced, leading to more accurate and reliable results. On the other hand, permutation-based approaches can also be utilized to counteract bias effects. These approaches involve applying permutations to the challenge as a pre-process and/or to the response as a post-process. By shuffling the order of the challenges or responses, the biases that might be present in specific positions are spread out and randomized. This helps to decrease the influence of biasing and enhance the overall robustness of the PUF.

5.3. CRPs Availability

To produce accurate PUF ML models, a minimum number of CRPs is required, this is vital since the size of the required dataset is proportional to the PUF complexity. Nonetheless, the representative dataset is usually scarce, whilst the collection process is expensive, involves sharing privacy-critical data, or is subjected to authorities' consent. Therefore, it is vital to develop techniques that enrich the network with high-quality CRPs datasets for improving the training process of the ML models. Additionally, the age effects of PUF devices limit the validity of the model usage over time. To address these two problems, *Transfer Learning* (TL) is characterized by significant benefits that avoid the retraining overhead in case of sudden and fast network and environmental variations. In specific, transfer learning allows trained models for certain tasks under specific network and environmental conditions to be utilized as a starting point for the new task, which alleviates the need to train ML models from scratch for new unseen data. Thus, pre-trained models from one PUF can be transferred to a new PUF with the same structure. Yet, the pre-trained model should be trained and configured on a large dataset. To tackle this issue, *Generative Adversarial Networks* (GANs), which are deep learning models, can be utilized to generate synthetic CRPs by learning the underlying patterns and characteristics of the available CRPs Hence, generative-based mechanisms can be applied, when pre-trained models are unavailable.

5.4. Post-Quantum Analysis

The computational complexity of a mathematical model of a PUF device can be reduced by quantum systems and algorithms. Hence, the quantum analysis ensures the resiliency of PUF's responses against quantum attacks. *Fuzzy extractors* are cryptographic models that guarantee the integrity of PUF responses and can be used to define a secure PUF against quantum attacks [15].

6. Conclusion

Security analysis of PUFs' devices requires an updated and representative CRPs dataset for training and evaluation. However, there is a lack of benchmark datasets for assessing the effectiveness and resistance of PUF devices. Therefore, in this work, we have presented an experimental setup to extract a set of CRPs for FPGA-based PUF. Specifically, CRPs from 50 FPGAs have been collected and suggested to be used by a set of security-based evaluation metrics: ML-based modeling, correlation, and entropy analysis. To study ML-based modeling and correlation, SVM modeling and Pearson correlation have been utilized, respectively. The obtained prediction accuracy of SVM models and the small correlations observed in adjacent bits highlight the significance of CRPs-based security analysis. Finally, we highlighted some potential future research directions and challenges that need to be carefully considered to improve the effectiveness of security analysis based on PUFs' CRPs.

Acknowledgments

This work is funded and supported by Technology Innovation Institute (TII) [grant: EX2021-005]. Additional support from Khalifa University, System on Chip Lab (SoC) [grant: RC2-2018-020].

References

[1] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, A. Wilczynski, Antibluff: towards counterfeit mitigation in ic supply chains using blockchain and puf, International Journal of Information Security 20 (2021) 445–460.

[2] N. Charlot, D. Canaday, A. Pomerance, D. J. Gauthier, Hybrid boolean networks as physically unclonable functions, IEEE Access 9 (2021) 44855–44867. doi:10.1109/ACCESS.2021.3066948.

[3] Y. Jiang, Mro_ml_analysis (2022). doi:10.21227/xbpf-m598.
URL `https://dx.doi.org/10.21227/xbpf-m598`

[4] Y. Hu, Y. Jiang, W. Wang, Compact puf design with systematic biases mitigation on xilinx fpgas, IEEE Access 10 (2022) 22288–22300.

[5] A. Aghaie, A. Moradi, Inconsistency of simulation and practice in delay-based strong pufs, IACR Transactions on Cryptographic Hardware and Embedded Systems (2021) 520–551.

[6] K. T. Mursi, B. Thapaliya, Y. Zhuang, A. O. Aseeri, M. S. Alkatheiri, A fast deep learning method for security vulnerability study of xor pufs, Electronics 9 (10) (2020) 1715.

[7] N. Wisiol, B. Thapaliya, K. T. Mursi, J.-P. Seifert, Y. Zhuang, Neural network modeling attacks on arbiter-puf-based designs, IEEE Transactions on Information Forensics and Security 17 (2022) 2719–2731.

[8] P. Santikellur, R. S. Chakraborty, Correlation integral-based intrinsic dimension: A deep-learning-assisted empirical metric to estimate the robustness of physically unclonable functions to modeling attacks, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 41 (10) (2021) 3216–3227.

[9] N. A. Hazari, A. Oun, M. Niamat, Machine learning vulnerability analysis of fpga-based ring oscillator pufs and counter measures, ACM Journal on Emerging Technologies in Computing Systems (JETC) 17 (3) (2021) 1–20.

[10] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas, Puf modeling attacks on simulated and silicon data, IEEE transactions on information forensics and security 8 (11) (2013) 1876–1891.

[11] F. Wilde, B. M. Gammel, M. Pehl, Spatial correlation analysis on physical unclonable functions, IEEE Transactions on Information Forensics and Security 13 (6) (2018) 1468–1480.

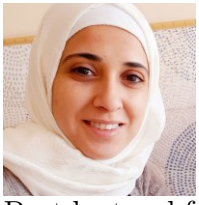
[12] M. Pehl, T. Tretschok, D. Becker, V. Immler, Spatial context tree weighting for physical unclonable functions, in: 2020 European Conference on Circuit Theory and Design (ECCTD), 2020, pp. 1–4. doi:10.1109/ECCTD49232.2020.9218325.

[13] A. Schaller, W. Xiong, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, B. Škorić, S. Katzenbeisser, J. Szefer, Decay-based dram pufs in commodity devices, IEEE Transactions on Dependable and Secure Computing 16 (3) (2019) 462–475. doi:10.1109/TDSC.2018.2822298.

[14] J. Song, H. Luo, X. Tang, K. Xu, Z. Ji, Y. Wang, R. Wang, R. Huang, A 3t edram in-memory physically unclonable function with spatial majority voting stabilization, IEEE Solid-State Circuits Letters 5 (2022) 58–61. doi:10.1109/LSSC.2022.3158630.

[15] S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, F. Ganji, D. Forte, Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions, Journal of Cryptographic Engineering (2021) 1–37.

Enas Abulibdeh received the B.Sc. and M.Sc. degrees in Computer Engineering from Jordan University of Science and Technology in 2013 and 2016, respectively. She is currently pursuing a Ph.D. degree with the Electrical and Computer Engineering Department, Khalifa University. Her research interests include physical unclonable function and its application for hardware security.



Shimaa Naser (Member, IEEE) received an M.Sc. degree in Electrical Engineering from Jordan University of Science and Technology, Jordan, 2015. Also, she received her Ph.D. degree in Electrical and Computer Engineering from Khalifa University, Abu Dhabi, UAE, 2022. She is currently a Postdoctoral fellow with the KU Center for Cyber-Physical Systems (C2PS), Khalifa University. Dr. Naser was a session chair for local conferences and a member of the technical program Committee for multiple IEEE conferences such as IEEE VTC 2022, IEEE ICC 2023, and IEEE 6GNet 2023. %Also, she participated in the peer-review process in multiple top IEEE journals such as Transactions on Communications, Transactions on Wireless Communications Communication Letters, and Photonics Journals. Dr. Naser has authored/co-authored 20+ journal and conference publications and is involved in local and international research collaborations with world-class universities in Canada and UK. Her research interests include advanced digital signal processing, convex optimization, mobile communication networks, optical wireless communications, ultra-low power networks, MIMO-based communication, and orthogonal/non-orthogonal multiple access.

Hani Saleh (Senior Member, IEEE) received the B.S. degree in Electrical Engineering from the University of Jordan, the M.S. degree in Electrical Engineering from the University of Texas at San Antonio, and the Ph.D. degree in Computer Engineering from the University of Texas at Austin. He has been an Associate Professor of electronic engineering with Khalifa University since 2012. He is an associate professor of electronic engineering at Khalifa University since 2012. He is a co-founder and an active researcher in the KSRC (Khalifa University Research Center) and the System on Chip Research Lab (SOCL). He has a total of 19 years of industrial experience in ASIC chip design. Prior to academia, he worked for many leading semiconductor design companies including Apple, Intel, AMD, Qualcomm, Synopsys, Fujitsu, and Motorola. His research interests include IoT design, deep learning, AI hardware design, DSP algorithms and hardware design, computer architecture and arithmetic, SOC design, ASIC chip design, FPGA design, and automatic computer recognition.

Baker Mohammad (Senior Member, IEEE) holds a Ph.D. in Electrical and Computer Engineering (ECE) from the University of Texas at Austin and an M.S. in ECE from Arizona State University, Tempe a B.S. degree in ECE from the University of New Mexico, Albuquerque. He is currently a professor of Electrical Engineering and Computer Science at Khalifa University and is the director of the System on Chip center. Prior to academia, he worked for six years at Qualcomm in the United States, designing high-performance and low-power DSP processors for communication and multimedia applications as a Senior Staff Engineer/Manager. Prior to that, he spent ten years at Intel Corporation, working on a wide range of microprocessor designs, including high-performance server chips (¿ 100 watts) and low-power embedded processors (¡ 1 watts). His research interests include VLSI, power-efficient computing, high-yield embedded memory, and emerging technologies such as Memristor, STTRAM, and In-Memory-Computing. He is also involved in developing microwatt-range computing platforms for wearable electronics and WSN, focusing on energy harvesting, power management, and power conversion.

Mahmoud Al-Qutayri (Senior Member, IEEE) received the B.Eng. degree from Concordia University, Montreal, Canada, in 1984, the M.Sc. degree from the University of Manchester, U.K., in 1987, and the Ph.D. degree from the University of Bath, U.K., in 1992, all in electrical and electronic engineering. He is currently a Full Professor with the Department of Electrical and Computer Engineering and the Associate Provost for Academic Operations, College of Engineering, Khalifa University, UAE. Prior to joining Khalifa University, he worked at De Montfort University, UK and the University of Bath, UK. His current research interests include wireless sensor networks, embedded systems design, in-memory computing, mixed-signal integrated circuits design and test, and hardware security.

Sami Muhaidat (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2006. from 2007 to 2008, he was an NSERC Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, ON, Canada. From 2008 to 2012, he was Assistant Professor with the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada. He is currently an Associate Professor with Khalifa University, Abu Dhabi, UAE, and a Visiting Professor with the Department of Electrical and Computer Engineering, University of Western Ontario, London, ON, Canada. He is also a Visiting Reader with the Faculty of Engineering, University of Surrey, Guildford, U.K. Dr. Muhaidat currently serves as an Area Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS. He was previously a Senior Editor of the IEEE COMMUNICATIONS LETTERS and an Associate Editor of IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was a recipient of several scholarships during his undergraduate and graduate studies and the winner of the 2006 NSERC PostDoctoral Fellowship Competition. Dr Muhaidat is a Senior Member IEEE.