Physical Unclonable Functions (PUF) for IoT Devices

ABDULAZIZ AL-MEER and SAIF AL-KUWARI, Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Qatar

Physical Unclonable Function (PUF) has recently attracted interest from both industry and academia as a potential alternative approach to secure Internet of Things (IoT) devices from the more traditional computational-based approach using conventional cryptography. PUF is a promising solution for lightweight security, where the manufacturing fluctuation process of integrated circuits is used to improve the security of IoT, as it provides low complexity design and preserves secrecy. PUF provides a low-cost low-power solution and can be implemented in both Field Programmable Gate Arrays and Application-Specific Integrated Circuits. In this survey, we provide a comprehensive review of the state of the art of PUF, its architectures, protocols, and security for IoT.

CCS Concepts: • Computing methodologies;

Additional Key Words and Phrases: Physical Unclonable Function, IoT security, hardware security, authentication, lightweight cryptography

ACM Reference Format:
Abdulaziz Al-Meer and Saif Al-Kuwari. 2023. Physical Unclonable Functions (PUF) for IoT Devices. ACM Comput. Surv. 55, 14s, Article 314 (July 2023), 31 pages.
https://doi.org/10.1145/3591464

1 INTRODUCTION

Preserving authenticity and confidentiality in Internet of Things (IoT) networks are major concerns for researchers and industries due to the increased reliance on these networks at many applications such as sensors, monitoring, and healthcare [129].

To address these concerns, Physical Unclonable Function (PUF) approaches have recently been proposed as a promising alternative to conventional cryptography, which is largely unsuitable to IoT networks mainly because of its sheer computational requirement, which often degrades battery efficiency on lightweight IoT devices.

Additionally, conventional cryptography is based on the hardness of solving some mathematical problems. However, advances in quantum computers may render such problems easy to solve [109, 112, 143]. PUF can help mitigate this risk by using the unique physical characteristics of each device to generate a unique secret key that can be used for encryption. As the output of a PUF is based

This work is partially funded by the G5797 “Developing Physical-Layer Security Schemes for Internet of Things Networks” project under the NATO’s Science for Peace Programme.
Authors’ address: A. Al-Meer and S. Al-Kuwari, Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, 34110, Qatar; emails: {abal34183, smalkuwar}@hbku.edu.qa.
Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
0360-0300/2023/07-ART314 $15.00
https://doi.org/10.1145/3591464

ACM Computing Surveys, Vol. 55, No. 14s, Article 314. Publication date: July 2023.
on physical characteristics, PUF is not susceptible to the types of attacks that a quantum computer could perform on traditional cryptographic algorithms [110].

Moreover, key distribution techniques used in conventional cryptography usually require a third party, which makes it impractical for IoT applications [136] as large-scale wireless networks require keys to be frequently updated, and that will introduce high overhead on the network.

Finally, some conventional cryptography primitives such as Message Authentication Code (MAC), rely on upper-layer mechanisms, which can be manipulated by adversaries e.g., spoofing attacks.

However, PUF offers an alliterative solution for lightweight hardware security suitable for IoT networks. PUF is based on the fact that no two identical chips having the same characterization and going through the same production line will never share the same physical properties to inevitable manufacturing variation during the fabrication of the chips [108]. PUF circuits exploit these features and utilize such variations to generate secret keys and authenticate IoT devices.

Several surveys were published on PUF considering both current PUF devices and emerging technologies. Babaei and Schiele [15] presented an overview of PUF for authenticating IoT devices and investigated the related challenges toward PUF exploitation. Similarly, Reference [146] highlighted various silicon PUF, mainly Ring Oscillator (RO) PUFs with related issues and challenges. Furthermore, Chang et al. [26] reviewed the improvement of PUF over the past decade and demonstrate vulnerabilities of PUF. Halak et al. [50] presented an overview of PUF in terms of principle and design challenges. A tutorial on PUF applications, error correction mechanisms, PUF types, and emerging technologies were presented in Reference [52]. Moreover, the authors in Reference [110] presented a review of the IoT network security challenges and investigate related attacks based on several IoT domains and discussed fuzzy extractors schemes for key extractions. In addition, Alkatheiri et al. [5] presented an experimental study of three designs in each of the two categories of PUFs: delay-based and frequency variation PUFs.

This article differs from other existing related work, in that it provides a comprehensive investigation into the essential performance evaluation and quality metrics of various PUF categories and designs. The article introduces and compares recent PUF authentication protocols specifically for lightweight devices, while also exploring the potential of different PUF architectures suitable for IoT applications, such as PUF designs implemented on Field Programmable Gate Arrays (FPGAs). Additionally, the article delves into the most common threats and attacks on PUFs and highlights open problems, identifies gaps, and discusses future directions in the field. Table 1 provides a comparison between previous survey and ours.
1.1 Motivation
One of the attractive lightweight security solutions for IoT devices is PUF. Consequently, many researchers reviewed emerging PUF technologies and their security challenges.

In addition, several PUF architectures have been proposed in recent years. However, to the best of our knowledge, there is no comprehensive review on PUF that discusses important aspects, such as the recent PUF implementations, quality evaluations, and security perspective for common and recent attacks for different PUF architectures. This has motivated us to write this survey and provide a recent review of this rather important and emerging technology.

1.2 Contributions
Our contributions in this survey can be summarized as follows:

- We investigate the essential performance evaluation and quality metrics of different PUF categories and designs.
- We introduce recent PUF authentication protocols and compare them for lightweight devices, while showing how they mitigate common attacks.
- We discuss different PUF architectures suitable for IoT applications, especially PUF designs implemented on FPGAs, which is becoming an attractive development platform.
- We investigate the most common threats and attacks on PUF and discussed multiple assumptions and scenarios.
- Finally, we discuss some open problems, identify gaps, and make recommendations and directions for future work.

1.3 Organization
The rest of the survey is organized as follows: Section 2 provides a brief discussion on the fundamentals of PUF. Section 3 describes PUF performance evaluation and quality metrics. PUF authentication protocols are then introduced in Section 4 followed by a thorough description of the popular architectures of PUF in Section 5 with analysis of specific security requirements such as strengths and weakness for each circuit design as well as performance evaluation comparison. In Section 6, we discuss common PUF implementations in both FPGAs and Application-Specific Integrated Circuits (ASIC). Section 7 discuss threats and common attack against PUF. Finally, we conclude this article in Section 8 and discuss some potential future research directions.

2 PUF FUNDAMENTALS
2.1 Definitions
The inherent unclonability of the PUF cannot be controlled, as it is based on multiple random parameters that are generated during the manufacturing process. When the binary sequence is applied to the PUF system, it will react with the corresponding response. That is, no two integrated circuits (IC) provide an identical response $R$ for the same challenge $C$ and this combination is called challenge–response pair (CRP). The PUF system contains uncontrollable random components, so when the challenge $C$ is applied to the PUF system it will react with these components in a way to produce unpredictable and random response $R$.

These random components and the inability to control the manufacturing process make the PUF system unpredictable, unique, and, more important, Physically Unclonable [25].

The PUF system is considered physically disordered with the structural information as follows:

- The related information of the PUF system could be extracted in a reliable way through measurement when different challenge $C$ is applied to the system to generate identical response $R$. 
Fig. 1. General operation of PUF.

- Due to the large possible combination of challenges \( C \), the corresponding response \( R \) cannot be predictable within a restricted time.
- It is very hard and almost impossible to model, computationally and numerically determine, and predict the CRP based on the available information and current pairs.
- The PUF system cannot be cloned and reproduced due to the variation in the manufacturing process.

The physical characteristics of the PUF circuits can vary in terms of signals transmission speed, frequency oscillation, and the initial random state of the memory elements. These characteristics can be exploited for Physical Layer Security.

PUF has been widely used to provide essential security services, such as authentication and secret key generations, especially in constrained environments, such as IoT, where power consumption and security need to be balanced. In most applications, the main function of PUF is to authenticate IoT devices as well as store secret keys.

The basic operation of PUF-based security is to provide a random choice of challenge bits to the PUF circuit and produce unpredictable and random responses. Moreover, the inevitable variations in the manufacturing process of the PUF circuit lead a unique silicon fingerprint, which provides a unique CRP for each IoT device even with the same input challenge bits [15]. Figure 1 illustrates the general operation of PUF, where \( k \)-input bits represent the challenges and \( m \)-output bits provide the unique responses.

Several security criteria should be considered to achieve high secrecy. First, the response bits need to be correlated to the specific challenge’s bits and are reproducible for the same challenge, despite any environmental factors, such as temperature and voltage. Second, the uniqueness of the CRP pairs should be verified by applying the same challenges to different PUF circuits that must generate different responses. Third, the challenge \( k \)-bits need to be large enough to limit the searchable and predictable computational of the eavesdropper.

2.2 PUF Applications

The main goal of PUF is to ensure communication security and prevent possible attacks. There are several applications of PUF that can be utilized for identification, confidentiality, and authentication. Below we list some popular PUF applications, each of which may prefer some PUF designs over others based on their requirements:

- **True Random number sequence generator**: Usually used to generate keys for encryption in communication and digital signatures and create passwords to protect the system [118].
- **Malware detection**: Malware detection is one of the most time-consuming processes in hardware security. However, PUF can efficiently detect differences between original devices and malware injected devices by examining the corresponding challenge–response pairs [124]. That is, when a chip is injected with malware, it will inevitably change the power distribution of the device, and that will deviate the response of the chip when the same challenges are applied to the PUF circuit.
- **Detection of degraded hardware performance**: The performance of the chip can be degraded due to natural aging and time. As a result, PUF challenge–response pair can detect such
devices, especially with critical applications such as aviation, military, and healthcare. The authors of Reference [19] identify the factors and related calculations to verify chip degradation.

- **Hand weapon authentication**: Utilizing embedded PUF device to authenticate users who are authorized to use some weapons. If the weapons are lost, then no one other than their original owner will be able to use them [12]. PUF in this case identify the users based on CRPs. For instance, the weapon can communicate with user wearable smart devices through **Radio Frequency Identification (RFID)** and exchange the CRPs. If the CRPs match and the user is identified, then the weapon can be used. Otherwise, it will be deactivated.

- **Self-destruction electronics**: Self-destruction is commonly required in military and defense applications, such as when a device is left on the battlefield [57]. In this case, PUF can inspect self-destruction signals and only executes self-destruction if it passes authentication.

### 2.3 PUF Categories

PUF can be classified into two main categories based on the manufacturing process: silicon PUF and non-silicon PUF. The silicon PUF relies on the mismatch fabrication process in the IC. The silicon PUF can be further categorized as delay-based PUF and memory-based PUF. However, non-silicon PUF includes a mismatch in the physical system with non-electronic components.

The authors of Reference [80] classified PUF as memory-based PUFs, which exploit the initial binary sequences of memory when it is powered on, and delay-based PUFs, which use delay variations between propagation signals of the circuit. However, more commonly, other authors classified PUFs based on their security into three types: weak, strong, and controlled PUFs [128], each with its own security properties and applications.

#### 2.3.1 Strong PUFs

Strong PUF is capable of generating a large number of CRPs due to its large circuit size, resulting in exponential growth. Nevertheless, a strong PUF remains stable despite changes in environmental conditions, making it a reliable option for authentication and key establishment purposes. Furthermore, a strong PUF is considered unpredictable, because the CRPs contain multiple combinations [108, 128].

#### 2.3.2 Weak PUFs

Weak PUF can be utilized for key generations and digital fingerprinting. However, it accepts a limited number of CRPs and is increasingly linear. Compared to strong PUF, weak PUFs provide constant responses under environmental conditions, utilize small number of CRPs pairs, and provide responses that are both unclonable and unpredictable.

#### 2.3.3 Controlled PUFs

The controlled PUF uses strong PUF as the main block and adds a control logic to control challenges from being freely applied to the PUF circuit while preventing immediate readout of the responses. Therefore, the control logic can be utilized to hinder machine learning attacks [41].

### 3 PUF PERFORMANCE EVALUATION

In this section, we discuss PUF performance evaluation and quality metrics that need to be considered while designing PUF circuits to achieve high security and prevent major attacks.

A comprehensive study of PUF performance to evaluate security can be found in Reference [82]. The first commercial performance evaluation-based PUF-embedded for RFID tags in Reference [66] and the PUF performance evaluation by delay statistics presented in Reference [64].

There are four essential parameters to evaluate on a PUF circuit, namely uniformity, uniqueness, reliability, and bit-aliasing.
• **Uniformity**: The probability that the 0s and 1s are uniformly distributed in PUF’s response $R$. Uniformity reflects the randomness of the response bits and is calculated as the percentage of **Hamming Weight (HW)** of the response bit as shown in Equation (1). The Hamming Weight of an array in binary number represents the sum of all the 1s bits in that array. For truly random response bits, the ideal value must be 50%,

$$Uniformity = \frac{1}{n} \sum_{l=1}^{n} r_{i,l} \times 100\%,$$

where $r_{i,l}$ is the $l$th bit of the response $n$-bit from a chip $i$.

• **Uniqueness**: The ability of PUF to distinguish a specific IC from other IC of the same structure when the same challenge $C$ is applied to the PUF circuit. Technically, it is defined as **Inter-device Hamming Distance (HD)** between $d$ different devices and the ideal value of uniqueness is supposed to be $50\%$. If the two chip $i$ and $j$ ($i \neq j$) have the responses $R_i$ and $R_j$ for the same challenge $C$, then the average inter-device can be calculated as

$$Uniqueness = \frac{2}{d(d+1)} \sum_{i=1}^{d-1} \sum_{j=i+1}^{d} HD(R_iR_j) \times 100\%.$$

• **Reliability**: The PUF design must be able to reproduce the same response bit $R$ to the same challenge $C$ under fluctuation of the environmental conditions, such as supply voltage and temperature. The reliability of PUF can be estimated as an average intra-device (HD) and indicate the unreliable or noisy responses bits:

$$HD_{intra} = \frac{1}{s} \sum_{i=1}^{s} HD(R_i\hat{R}_{i,t}) \times 100\%,$$

where $R_i$ for the chip $i$ is measured at the normal operation condition and $\hat{R}_i$ extracted at different supply voltage and temperature. $\hat{R}_{i,t}$ is the $t$th sample of $\hat{R}_i$. The total of $n$-bit response obtained for $s$ group. In other words, the reliability is reflecting the stability of PUF and it is measured with Equations (3) and (4),

$$Reliability = 100\% - HD_{intra}.$$

• **Bit-aliasing**: Bit-aliasing indicates the similarity of PUFs responses. When bit-aliasing occurs, different IC may produce an identical response. The bit-aliasing of the $l$th bit of an $n$-bit response is the average hamming weight of the $l$th bit across several $k$ devices. The ideal value is $50\%$, and it is defined as

$$Bit - aliasing = \frac{1}{k} \sum_{i=1}^{k} r_{i,l},$$

where $k$ is the number of PUF devices and $r_{i,l}$ is the $l$th bit of the response $n$-bit response.

### 4 PUF AUTHENTICATION PROTOCOLS AND KEY GENERATION

In this section, we describe how PUFs circuit can be used to authenticate low-cost devices, such as IoT devices and RFID, without resorting to conventional cryptography to maintain an acceptable low power consumption and reduce the overhead circuit area. Table 2 illustrates the comparison between PUF authentication protocols.
Table 2. PUF Authentication Protocols

| Ref. | Authentication method                  | Technique                     | Comments                                                                 |
|------|----------------------------------------|-------------------------------|--------------------------------------------------------------------------|
| [118] | Authenticate individual ICs            | PUF-based                     | Suitable for low-cost platform such as RFIDs                             |
| [81]  | Wi-Fi authentication of IoT devices    | PUF-based                     | Less resource and computation overhead using only 3 pairs of CRPs.        |
| [107] | Mutual Authentication Protocol         | PUF-based                     | Used for real-time applications No need to store the generated keys      |
| [6]   | Authentication privacy preservation     | PUF-based and wireless link fingerprint | Mitigate against physical and cloning attacks. Low energy consumption compared to related protocols. |
| [46]  | Lightweight pairwise protocol          | PUF-based                     | The protocol can detect nodes that have been removed or replaced         |
| [92]  | Mutual multi-factor authentication     | PUF-based and cryptographic method | Lower communication overhead. Three messages are required to achieve the authentication Fast to execute |
| [65]  | Two-factor authentication for IoV system | PUF-based and cryptographic method | There is no storage required of any secret data. They combine passwords with PUF (two-factor) |

Authentication in PUF can be performed in two phases as shown in Figure 2: the enrollment and verification phases. In the enrollment phase, the PUF circuit is directly connected to the server to receive the challenge bits created by the server. Then the PUF provides the response bits to be stored and used later in the verification phase by the server. In the verification phase, since the PUF chip is implemented into IoT devices to be authenticated by the server. The server sends the original challenges bits that have been utilized in the enrollment phase through the untrusted network to the IoT device. The IoT device then replies with the generated response bits. Finally, if the generated response bits match any entry in the original (stored) CRPs table in the server, then the IoT devices are authenticated. Additionally, the response bits for PUF circuit can be used to extract secret key to ensure confidentiality when exchanging data [15]. Also, the challenges must never be reused to prevent the man-in-the-middle attack and consequently predict the CRPs.

In fact, authentication in PUF can be done in plaintext. The authors of Reference [118] proposed a key generation protocol using PUF circuits to be implemented with conventional cryptographic primitives (e.g., RSA). The key generation operation proceeds in two steps. First, the error correction code (ECC) consists of initialization and regeneration to ensure that the PUF circuit generates the same keys under variations of environmental conditions or fluctuations in power supply and temperature. Second, key generation is executed to transform the PUF output into keys.
Moreover, the PUF-based lightweight protocol proposed in Reference [81] authenticates IoT devices during an established WiFi connection. The protocol consists of four phases: the one-time enrollment phase, connection initialization phase, router authentication phase, and client authentication phase. In the one-time enrollment phase, the PUF circuit embedded into the IoT device needs to exchange the CRPs with a particular router, which generates three random numbers as a challenge and collects their responses to be stored in the secure database of the router against the **Media Access Control Address (MAC address)** of the IoT device. In the connection initialization phase, a secure wireless connection is established between the router and the IoT device. However, in this phase, the IoT device will send the request signal, including the MAC address of the device, to the router, and then the router will search in the database for that particular MAC. If an entry is found, then the router performs the next phase. Otherwise, it terminates the connection. The router authentication phase consists of several XOR operations between the router and the IoT device. If the calculation is matched, then the router is authentic by the device and the process is continued to the final stage. Otherwise, the process is terminated. In the final phase, the router authenticates the IoT device by performing multiple XOR operations and authenticates the IoT devices.

It was shown that this protocol overcomes the security issues against several WiFi attacks, such as MAC spoofing attack, invasive attack, and evil twin attack, by using only three CRPs to secure the connections [89]. A mutual authentication protocol-based PUF was proposed in Reference [107], which utilizes keys generated by PUF to authenticate IoT devices while using on-the-fly keys to avoid key storage. Moreover, the authors of Reference [142] introduced a PUF-based key sharing approach using an inter-stage crossover structure of configurable RO PUF that is suitable for multiparty communication (where many parties are required to share the same key). The proposed key sharing protocol can be utilized for lightweight devices and produce secure and efficient key distribution.

The proposed protocol uses a hybrid PUF, which is a combination of RO (see Section 5.1.1) and Arbiter PUF (see Section 5.1.1) with the fuzzy extractors (error correction) mechanism proposed in Reference [34] to ensure reproducing the same random keys under fluctuations of the environmental, such as temperature and voltages. However, the protocol assumes that the IoT devices are already enrolled with the **Trusted Authentication Server (TAS)** for exchanging data and the CRPs stored in the TAS server. When the IoT device requests access to the server, it will send the device **identification number (ID)** to the TAS, and then TAS selects a random challenge corresponding to the device from the database and sends it to the device. Then the IoT device re-generates the responses using challenges and helper data for error correction from the server. The server will generate key pairs (private and public) and sends the public key to the device. Next, the device generates a shared message from the responses and public key using scalar multiplication. In the final stage, the server generates a shared message from the responses and private key; if both keys match, then the device is authenticated.

Furthermore, the authors of Reference [6] introduced a PUF-based authentication protocol combined with exploiting wireless channel properties, such as **Received Signal Strength Indicator (RSSI)**, to distinguish between legitimate and eavesdropper channels. Thus, data provenance is achieved in terms of confidence and data source, e.g., locations and time. The proposed protocol handles two scenarios: single hop, where the IoT device is directly connected to the server through the wireless gateway, and multi-hop, which requires intermediate devices to be connected to the wireless gateway. In the single-hop scenario, there are two phases (the authentication phase and data transfer phase), assuming that the CRPs have been stored in the server. The authentication phase has five steps: The IoT device generates responses $R$ using stored challenges $C$ to send a message that contains device ID with the random nonce encrypted with response and authentication parameter to the server, and then the gateway generates a wireless fingerprint for the link between
the IoT device and the gateway to send the message to the server. However, the server will search the CRP for verification. In the data transfer phase: The IoT device creates a message carrying data and uses the fingerprint parameters from the previous authentication phase and sends it to the wireless gateway. Therefore, the wireless gateway utilizes the parameters with the message carrying data to perform encryption and forward it to the server. Then the server decrypts the message and verifies the authentication parameters as well as provides the acknowledgment to the IoT device.

In addition, an authentication protocol based on continuously confirming the existence of a device is proposed in Reference [46]. This protocol was developed to detect the displacement of nodes through the link state changing using one CRP. In this protocol, there are two phases: the initialization phase and the Ratchet steps phase. The initialization phase consists of 23 steps to introduce the IoT nodes to each other and prepare them to the next phase. The Ratchet steps phase has 16 steps to authenticate the remote IoT node and generate/update the secret keys.

Another work proposed multi-factor authentication with a two-tier authentication mechanism [92]. The first tier depends on cryptographic primitives such as hash functions and XOR operation with configurable PUF to establish trusted relation between the IoT devices. This tier consists of six steps with several mathematical operations. The second tier exploits channel characteristics such as RSSI and Signal-to-Noise Ratio as a fingerprint for the devices, which can reduce the probability of authentication threats, so the proposed protocol authenticates the IoT devices when both tiers are validated.

Similarly, the authors of Reference [63] introduced a two-factor authentication protocol for the **Internet of Vehicles (IoV)**. This protocol relies on a combination of password and PUF to enhance the authentication mechanism, which eliminates the need to store secret keys locally, and ensures that the adversary cannot compromise the device even with physical access. However, the proposed protocol consists of three phases: the system setup phase, the registration phase, and the login and authentication phase. In the system setup phase, the keys are generated by the server and distributed the keys to the vehicles for encryption. The registration phase includes multiple internal calculations and information exchanges to register the users and sensors. Finally, in the login and authentication phase, the IoV establishes a secure connection with the server.

Furthermore, a lightweight mutual authentication protocol-based PUF is proposed in Reference [1]. The protocol comprises of two distinct phases. The first phase, known as the enrollment phase, involves the generation of a set of challenges by the backend system (containing a database) using a **pseudo-random number generator (PRNG)**. The responses are obtained from PUF in a secure environment, and the resulting CRP with the device ID is stored in the database. The second phase, referred to as the regeneration phase, involves the authentication process and the generation of a session key. Upon completion of the enrollment phase, only the device and the backend system possess knowledge of the PUF’s response to the challenges. This is because the device holds the PUF, and the backend system stores the CRPs in its database. The protocol utilizes CRPs for both device authentication and backend system authentication. The device can also issue challenges and request responses from the backend system. The device can regenerate the challenges from the enrollment phase by utilizing the same PRNG and monitoring the number of PRNG invocations. It is shown that the proposed protocol is secure against a range of threats, including physical attacks, replay attacks, machine learning attacks, man-in-the-middle attacks, and cloning attacks with small computational overhead. In addition, the concept of learning with parity noise-based authentication protocols has been proposed in Reference [9] where it was shown that the proposed protocol is secure against random guessing attack and provide lightweight authentication with provable security in a post-quantum scenario. The protocol utilized a Resistive Random Access Memory crossbar and the secret key was stored in a memory array to execute the authentication.
A hardware-focused authentication protocol that uses a device identifier generated during voltage over-scaling (VOS) was proposed to address the overhead authentication protocols [146]. This protocol employs adders in the computation unit to generate an error dependent on the process variation, which is then combined with secret keys to create a two-factor authentication mechanism. Therefore, the authors of Reference [145] analyze the machine learning-based attacks on this authentication protocol, and a new challenge self-obfuscation structure (CSoS) is proposed to enhance security and resist such attacks. The results of the experiments show that popular machine learning models like Artificial Neural Networks (ANN), Recurrent Neural Networks, and Covariance Matrix Adaptation Evolution Strategy (CMA-ES) can successfully predict the CRPs behavior of VOS-based authentication with up to 99.65% accuracy but deploying the proposed CSoS reduces the accuracy to less than 51.2%.

5 PUF ARCHITECTURES

In this section, we describe several PUF architectures suitable for IoT applications. We also discuss the strengths, weakness, quality metrics, and evaluation of common architectures as shown in Table 3. The following criteria need to be taken into account when selecting a PUF architecture:

1. Robustness against different possible attacks, such as machine learning attacks and side channel attacks [15].
2. Statistical properties and quality metrics such as
   - **Uniqueness**: the ability of the PUF circuit to generate a unique secret key when a challenges bit is provided.
   - **Reliability**: the ability of the PUF circuit to generate the same secret key under different environmental factors, e.g., temperature and voltages.
   - **Randomness**: the response bits generated from the PUF circuit contain sufficient entropy.
3. The growth of the number of CRPs in strong and weak PUF needs to be taken into account, as it can lead to increased computational complexity, which, in turn, will consume power.
4. The PUF circuits need to be implemented easily in silicon chips.

5.1 Silicon PUF

One of the common PUF architectures is silicon PUF. This architecture depends on the manufacturing variation process of the chip, which cannot be predictable and controlled. Therefore, many designs exploit this behavior to generate random keys. The silicon PUF can be broadly divided into delay-based PUF and memory-based PUF.

5.1.1 Delay-based PUF. The delay-based PUF exploits the propagation delay of the electronic circuit as a racing condition. For instance, the circuit needs to compare different paths within the design to verify which path is faster. Due to the unpredictable fabrication process of the chip, an identical design will produce different random sequence.

Arbiter PUF. During manufacturing variations of multiplexers, different delay paths are formed, where one path is usually faster than others. Depending on the input challenges bits, each multiplexer will select the next path to be switched to, which provides multiple combinations of bit path selections. Arbiter PUF [42] operates by comparing two path delays, the upper path and lower path, which are cross-connected as shown in Figure 3 and generates a response bit “0” or “1” depending on the faster path being selected by the flip-flop as an arbiter at the output.

Arbiter PUF is categorized as strong PUF. Moreover, to achieve practical statistical properties, all the delay paths must have the same length. The arbiter PUF can be implemented in both FPGA and ASIC.
Table 3. Summary of PUF Quality Metrics and Evaluation

| Categories | Ref. | PUF Architectures | Implementation Platform | Uniqueness (inter-chip) \(HD\) | Uniformity \(HW\) | Reliability (inter-chip) \(HD\) | Hardware Overhead | Power Consumption |
|------------|------|-------------------|--------------------------|-----------------|----------------|-----------------|---------------|-----------------|
| Reconfigurable LFSR-PUF | [22] | CS-APUF | CMOS | 46.8% | Pass NIST | 99.2% | 3838 \(\mu m^2\) | 68.63 \(\mu W\) |
| Reconfigurable LFSR-PUF | [35] | | Simulation | 50% | 50% | — | 4 \times 4 switch blocks | — |
| FF-APUF | [45] | | Artix-7 | 41.53% | 54% | 97.10\(^a\), 93.99\(^b\) | 128 Slices | — |
| RO | [51] | BST-APUF | Artix-7 | 49.1% | 50.3% | \(=100\)% | 150 Slices | — |
| Arbiter PUF | [73] | Arbiter PUF | TSMC 0.18 \(\mu m\) | 23% | — | 95.18\(^a\), 96.26\(^b\) | 1,212 \(\mu m^2\times1,212 \mu m\) | 137 \(\mu W\) |
| Feed-Forward Arbiter | [77] | | TSMC 0.18 \(\mu m\) | 38% | — | 90.16% | — | — |
| 3-1 DA PUF | [79] | | Virtex-5 | \(=50\)% | \(=50\)% | \(=88\)% | — | — |
| Energy-Efficient RO | [86] | Energy-Efficient RO | CMOS | 49.9% | 50% | 94.4\(^a\), 97\(^b\) | 2,168 \(\mu m^2\) | 6.63 \(mW\) |
| XOR FFAPUF | [103] | XOR FFAPUF | 3 Types FPGAs | 48\(^a\) | — | — | 224 Slices\(^c\) | — |
| FOXX APUF | [119] | FOXX APUF | Spartan-3, Virtex-6 | 42%, 44% | — | — | 703 Slices | — |
| RO PUF | [2] | Two schemes RO PUF | Spartan-7 | 46.4% | High entropy | 99.68% | 32 RO array (serial) | — |
| Configurable RO | [20] | TERO-PUF | ALTERA DE1 | 48% | — | 98.3% | 416\(^e\) | — |
| Configurable RO | [33] | | Artix-7 | 56.1% | 50.36% | 98.22\(^d\), 99.56\(^b\) | 1,128 \(\mu m^2\) | 119.4 \(\mu W\) |
| RO-based LUT | [76] | RO-based LUT | Kintex-7 | 49.15% | — | 99.16% | 8\(^g\) | — |
| RO PUF | [118] | RO PUF | Virtex-4 | 46.15% | — | 99.52% | 16 \(h\) \times 64 array\(^e\) | — |
| RO PUF | [137] | PC-PUF | Kintex-7 | 50% | Pass NIST | \(=99\)% | 365 Slices | — |
| XOR-RO | [139] | XOR-RO | Virtex-6 | 48.4% | Pass NIST | 98.33\(^d\), 98.25\(^b\) | 16\(^g\) | — |
| XOR-RO | [140] | DFRO-PUF | Simulation | 49.98% | 50.05% | 99.5%\(^d\), 98\(^b\) | — | 264 \(\mu W\) |
| LFSR-PUF | [7] | LFSR-PUF | Spartan-3E | 47.4% | — | 95.8\(^a\), 93.55\(^b\) | 2 Slices | — |
| SRUPF | [54] | SRUPF | Alinx | 49.9% | 49.8% | \(=100\)% | 20,544\(^d\) | 0.242 \(W\) |
| L-PUF | [55] | L-PUF | Alinx | 49.66% | 49.8% | — | 210\(^g\) | — |
| PL-MRO PUF | [148] | PL-MRO PUF | Artix-7 | 51.7% | High entropy | 94.5% | — | 23.44 \(\mu W\) |
| Optical PUF | [93] | Optical PUF | Optical token | 49.79% | — | 25.25% | 1cm \(\times\) 1cm \(\times\) 2.5\(mm\)^d | — |
| Optical PUF | [101] | Optical PUF | Optical token | 50% | — | 94% | 1cm \(\times\) 1cm \(\times\) 2.5\(mm\)^d | — |
| Memristor PUF | [67, 68] | Memristor PUF | Simulation | 59.1% | 48.9% | 97%, 95.5% | Two 32\(\times\)2\(^h\) | — |
| Fabricated | [69] | Memristor PUF | Fabricated | High | \(=50\)% | — | 150(1MB)\(^e\) | — |
| Memristor PUF | [99] | Memristor PUF | Fabricated | High | \(=50\)% | — | — | — |
| Simulation | [127] | Memristor PUF | Simulation | \(=50\)% | \(=50\)% | 90\(^a\) | Four\(^f\) | 104 \(\mu W\) |
| MRAM PUF | [4] | MRAM PUF | CMOS | \(=50\)% | Pass NIST\(^b\) | 99.76\(^a\), 98\(^b\) | 28 nm | — |
| MRAM PUF | [31] | MRAM PUF | Fabricated | 47% | — | 99.9% | 10 \(\times\) 20 PUF array\(^c\) | — |
| SRAM PUF | [49] | SRAM PUF | FPGA | 49.97% | — | 88\(^a\) | 4,600 SRAM memory bits | — |

(Continued)
| Categories                          | Ref. | PUF Architectures | Implementation Platform | Uniqueness (inter-chip) | Uniformity (intra-chip) | Reliability (intra-chip) | Hardware Overhead | Power Consumption |
|------------------------------------|------|-------------------|--------------------------|-------------------------|-------------------------|--------------------------|-------------------|-------------------|
| Memory-based PUF                   | [90] | MRAM PUF          | CMOS                     | 50.64%                  | 50.02%                  | 97.87%                   | m × n PUF array   | —                 |
|                                    | [72] | Butterfly PUF     | Virtex-5                 | ≈50%                    | —                       | 94%                      | 130 slices        | —                 |
|                                    | [90] | MRAM PUF          | Fabricated               | 49.8%                   | —                       | 92.3%                   | 32 × 32 PUF array | —                 |
| Carbon PUF                         | [90] | Carbon PUF        | Simulation               | 49.67%                  | —                       | 96.5%                   | serial connection  | 1.26 μW           |
|                                    | [97] | Carbon PUF        | Fabricated               | 49.7%                   | 45.3%                   | —                       | 500 μm PUF array  | —                 |
| Other PUF                          | [8]  | Anderson PUF      | Virtex-5                 | 47.9%                   | —                       | 96.4%                   | 2 Slices          | —                 |
|                                    | [11] | SR-Latch PUF      | Spartan-3                | 49.2%                   | 54.27%                  | 80%                      | 2 Slices          | —                 |
|                                    | [23] | SOT PUF           | Fabricated               | 47.2%                   | 48.6%                   | stable                   | 6 × 6 μm² (device size) | —                 |
|                                    | [56] | p-SPUF            | Alinx                    | 50.58%                  | 49.6%                   | 93.3%                   | 12 × 32 slices    | —                 |
|                                    | [78] | Modified Anderson PUF | Spartan-6               | 50.89%                  | 49.41%                  | 91.25%                   | 348 Slices        | —                 |
|                                    | [85] | Digital PUF       | Simulation               | ≈50%                    | 50%                     | ≈100%                   | 145.92 × 89.32 μm | —                 |
|                                    | [95] | Quantum PUF       | Cloud-based              | 55%                     | —                       | 96%                      | —                 | —                 |
|                                    | [106]| LHPUF             | Spartan-3E, Spartan-6    | 38.28%                  | —                       | —                       | 123 slices        | 2.500 μW          |
|                                    | [117]| Latch PUF         | CMOS 0.130μm             | 50.55%                  | —                       | 96.96%                   | 8 × 16 NOR-latch array | 0.162 μW         |
|                                    | [120]| Glitch PUF        | Spartan-3A               | 41.5%                   | —                       | 93.4%                   | —                 | —                 |
|                                    | [131]| Scan chains PUF   | Virtex-5                 | 49.86%                  | —                       | 96%                     | 98%               | 128 Slices        | —                 |
|                                    | [132]| Transformer PUF   | Artix-7                  | 49.44%                  | —                       | 98.12%                  | Efficient         | —                 |
|                                    | [138]| Hybrid PUF        | Simulation               | 50.9%                   | 52.9%                   | 99.21%                  | —                 | 285.5 μW          |
|                                    | [149]| SCA-PUF           | CMOS                     | ≈50%                    | 52.8%                   | 99.9%                   | 130 nm            | 68 nW             |

*a* Temperature variation.

*b* Voltage variation.

*c* 16 × 64 array = 1024 ROs; One RO (contain 5 inverters and 1 AND gate).

*d* Plastic token size.

*e* Memristor memory structure.

*f* Different crossbar sizes (XORed Xbar) 4 × 2, 8 × 2, 16 × 2, 32 × 2.

*g* Spartan-6.

*h* Memristive Xbar PUFs.

*i* IBM quantum hardware.

*j* The array fabricated using standard electron beam lithography process.

*k* National Institute of Standards and Technology, test results for 10K responses produced from PUF.

*l* MRAM Size (m × n cells), 4 × 128, 8 × 128, 16 × 128, 32 × 128.

*m* Serial connection of Carbon Nanotube PUF Parallel-elements.

*n* The layout sketched by CAD tool Electric.

*o* Overall silicon area (chip dimension).

*p* Power Optimized Hybrid Oscillator-arbiter design.

*q* Speed Optimized Hybrid Oscillator-arbiter design.

*r* Logic Array Block.

*s* Lookup Table.
In Reference [35], a reconfigurable arbiter PUF presented with $4 \times 4$ switch block instead of the classical $2 \times 2$, such that the $4 \times 4$ switch block can be reconfigured to increase the number of paths connection, which can be used for applications that require regular key generation. The authors in Reference [94] introduce an enhancement over the classical Arbiter PUF [42] and the Feed-Forward PUF [13] known as Double XOR Arbiter. The design consists of two identical paths of cascaded multiplexers with two SR latches and an XOR operation at the output of the circuit, which consumes less power and provides high uniqueness.

**Ring Oscillator PUF.** Ring Oscillator PUF [118] is based on the circuit oscillation between two voltage levels in specific frequency as shown in Figure 4. The circuit consists of AND gates with inverters that are connected to the multiplexer. By comparing two RO frequencies, the binary bits are generated based on incoming challenges bits by the multiplexer. At the end of the circuit, the comparator chooses the greatest counter to produce response bits. However, while the theoretical properties of RO PUF show that the oscillating frequencies must be the same, during the hardware manufacturing variations process it will inevitably cause some differences in the oscillation frequencies.

Ring Oscillator PUF is a strong PUF and can be implemented on FPGA. The main drawback of RO PUF is its sensitivity to the environment. To address this issue, the authors of Reference [33] proposed configurable RO using only two hybrid logic gates, which is not only reliable under environment variation conditions but also consumes less power and circuit area. The authors of Reference [130] further enhanced the response entropy by adding a configurable multiplexer with RO PUF circuit, which can select from inputs challenges $C$ based on the proposed selection.
algorithm. The FinFET 20-nm technology-based RO PUF is proposed in Reference [140] to overcome the hardware overhead and power consumption of classical RO PUF. However, they introduce a frequency divider with flip-flops instead of counters, comparator to reduce power consumption.

**Hybrid PUF. Lightweight Hybrid PUF (LHPUF)** [106] combines features of Arbiter PUF and RO PUFs to enhance the security as illustrated in Figure 5. LHPUF consists of \( N \) to 1 multiplexer, two counters, NAND gate, NOT gate, and one arbiter circuit that compare the faster path by the comparator to produce response bits. The result of the bit output response depends on the count of the number of “1”s or “0”s in the counter at the output. The authors of Reference [106] implemented LHPUF using FPGA (Xilinx), and it provides higher security performance as shown in Table 3 compared to traditional arbiter PUF and RO PUF with less power consumption.

Another work introduced FinFET-based-PUF with two hybrid oscillator-arbiter PUF designs, which improved the power consumption and speed compared to traditional RO and arbiter PUF [138].

**Glitch PUF.** The glitch PUF [120] exploits the glitch waveform variation of the logic gates by providing clock pulses to trigger the circuit to generate a random sequence. The design is composed of registers, a delay circuit, a glitch generator, and controls. The output value depends on the signal speed in each design stage. The experimental results show that the uniqueness is 30%.

5.1.2 Memory-based PUF. Memory-based PUF exploits the initial binary sequences of memory when it is powered on, which is provide unpredictable responses for each memory cell.

**SRAM PUF.** One of the common PUFs based on memory architecture is SRAM PUF [49, 53]. The main idea of SRAM PUF is to generate a response bit based on the boot-up of SRAM cells, which is unpredictable; that is, when the SRAM is powered ON, the initial values of the single cells in the SRAM can be “0” or “1” randomly as they are considered noisy fingerprint. Furthermore, each SRAM has unique states during this boot-up period. Figure 6 illustrates the SRAM PUF circuit that includes one cell of the SRAM memory with connected transistors.

However, SRAM PUF is a weak PUF with limited number of CRPs and is mainly applicable to microcontrollers. Hence, more layers of security are required to thwart machine learning attacks. Additionally, SRAM PUF suffers from noise effects and requires error correction [15, 53].

**Butterfly PUF.** The author of Reference [72] proposed Butterfly PUF to overcome the initialization SRAM in some FPGAs making it suitable to be implemented on all FPGAs types. This PUF is
based on the cross-coupled latches configured as a symmetrical signal wire connection. The start process of the circuit obtains one of the two different possible states, “0” or “1” at the output. This state relies on the slight variation in the cross-coupled wire connection paths, which are unique in every device.

Memristor PUF. Memristor (referred to as memory resistor) was first proposed in 1971 by Chua [29], which provides a relation between charge and flux. In 2008, HP labs [116] presented a physical model of two-terminal device, which is based on a switching process between two resistance states, such as high resistance state (HRS) (called OFF state, “0”) and low resistance state (LRS) (called ON state, “1”). This state is changed when the voltage is applied across terminals for a specific period with two main operations: SET (that represents the change of state from HRS to LRS) and RESET (refer to the transition from LRS to HRS). As a result, the memristor is suitable for PUF due to the variability of the state and switching process. Memristor is also often used as a True Random Generator [126], as it is difficult to duplicate due to its unique electrical properties. Memristors are small and consume low power, making them well suited for energy-constrained devices such as IoT devices [59]. However, integrating memristors into a PUF can be challenging due to the complexity of their electrical behavior, which causes a reduction in resistance over time as the number of switchings increases. This phenomenon can force the memristor to be stuck at a state with a certain resistance, which usually leads to failure [36].

Koeberl et al. [69] proposed memristor PUF to exploit undefined logic state regions based on memory functionality that depends on access time and applied voltage. Consequently, unpredictable sequence value is produced due to the utilization of the weak-write method. The authors of Reference [100] present a single bit memristor PUF with two control signals that specify the writing and reading operation. However, the authors of Reference [99] describe a multi bit memristor PUF as an entropy source based on the process variations of the write-time memristor cell. The Xbar memristive architecture [127] consisting of \(N \times M\) size word-lines as rows to receive the challenge bits \(N\) and bit-line as columns to produce response bits \(M\). The more Xbar rows size, the more randomness generated. An optimized and robust architecture based on memristive Xbar is presented in References [67, 68], which implements two memristive Xbar PUF utilizing two memristors devices and the logic circuit that processes the challenges and activate the PUFs.

MRAM PUF. Magnetoresistive Random-Access Memory—(MRAM) based PUF is proposed in References [31, 32] to generate unique keys and provide authentication by exploiting the variation geometric of the MRAM cell. The stream bits are stored in a Magnetic Tunnel Junction (MTJ), which consists of several layers. Due to the variation of the manufacturing process, the geometry of the cell varies in shape (rectangle or ellipse). MRAM provides superior features, such as non-volatility, cost-effectiveness in production, high speed, energy efficiency, and reliability,
making it a strong contender for usage in non-volatile memory applications [90]. However, MRAM suffers from an exponential increase in initialization time, which significantly drain memory resources [28]. Experimental evaluation of the MRAM PUF is presented in Reference [90] with the Thermally Assisted Switching MRAM (TAS-MRAM) method that is fabricated in dies. The experiment shows that TAS-MRAM consumes low power and high speed compared to SRAM. Furthermore, the authors of Reference [4] proposed a reconfigurable arbiter PUF based on hybrid Spin Transfer Torque (STT) (STT-MRAM/CMOS). The design employed the variation process of the transistors and MTJs connected in series with the control signals. The switch selection and pre-charge sense amplifier (PCSA) is used as an arbiter to determine the delays of the discharge current between paths. Therefore, the design provides sufficient entropy response and produces large and unpredictable CRPs compared to the silicon/classical arbiter PUF (Section 5.1.1). The reliability enhancement/improvement of STT-MRAM PUF response is demonstrated in Reference [58]. Furthermore, the Spin Orbit Torque (SOT) PUF proposed in Reference [23] as a reconfigurable PUF based on SOT to stimulate the motion of the Domain Wall.

5.1.3 Others Silicon PUFs. Several other silicon PUF designs have been proposed to enhance the quality metrics, including the following:

- Latch PUF [117]: introduce a unique ID for IC using cross-coupled NOR gates arrays, which improve the speed and power consumption.
- Digital PUF [85]: improves the reliability of analog PUFs.
- Coin Flipping PUF [123]: exploits the convergence time of the bistable ring circuit.
- Finite State Machine [39]: removes the need for ECC in Controlled PUF (Section 2.3.3) and improves the security.
- Subthreshold current array PUF (SCA-PUF) [149]: exploits the $I - V$ characteristics of the two arrays of transistors and the response is produced based on the comparison between two output voltages.

5.2 Non-silicon PUF

5.2.1 Optical PUF. The optical PUF was first proposed in References [93, 97] to demonstrate an inexpensive non-silicon system that consists of a token with the integrated three-dimensional micron scale glass as a physical system to generate a 2,400-bit unique key. The authors of Reference [44] developed an optical PUF that can be implemented in Printed Circuit Board (PCB) by adding an imager and Light-emitting diodes (LED). These components are covered by polymer waveguide. However, the LED light is emitted and reflected by the waveguide to the imager to generate a unique number that can be used for authentication and key generation. Therefore, any invasive attack attempting to discover the unique key will destroy the waveguide coating, which damages the secret key. Rührmair et al. [101] represent a new image transformation that enhances the PUF entropy to measure the interference pattern through the optical PUF instead of detecting the reflection compared to the previous work in References [93, 97] with the same hardware cost.

5.2.2 Quantum PUF. Quantum PUF provides control over the unique parameters of the process variation that created the classical PUF. Škorić [113] proposed quantum readout PUF (QR-PUF), which uses quantum state for both challenges and responses, usually to implement remote authentication protocols. By exploiting the no-cloning theorem [135] of the quantum state, the adversary will be detected if they intercept the CRP. Another work presented quantum secure authentication [45], which relies on phase shaping of irradiate light pulse using a spatial light modulator and analyzer plane to detect the reflected response. The quantum confinement is described in Reference [98] to provide a unique identifier for the devices by measuring the variation in resonant tunneling...
diodes. A comprehensive study of the quantum PUF is presented in Reference [10], which defines a quantum attack model and security parameters of the quantum PUF. The authors in Reference [95] propose a quantum PUF to address the security issues of workload scheduling algorithm threats for cloud-based quantum computers.

5.2.3 Carbon PUF. Carbon Nanotube Field Effect Transistor– (CNTFET) based PUF is a promising technology to provide a unique signature with low power consumption. The first design of Carbon Nanotube PUF (CNPUF) is presented in Reference [70], which is composed of pairs of CNTFET connected in series that share the same input voltage and response bits produced from comparing two-stage currents. The simulation result in Reference [70] shows that the CNPUF is reliable under temperature and voltage variation. The authors of Reference [87] introduced CNTFET PUF cell, which compares the input voltage twice using two inverters and a comparator. Similarly, the authors of Reference [75] demonstrated the fabrication of 400 CNTFET PUF devices with the same manufacturing process and evaluated their performance. The measurement shows that the devices produce high-quality metrics in terms of uniformity and uniqueness. Ternary cycle operator–based CNTFET PUF is proposed in Reference [114] with two delays line using cycle operators.

5.2.4 Others Non-silicon PUFs. Other non-silicon PUF designs have been proposed, including the following:

- **Paper-based PUF** [21]: The physical identity formed from microscopic imperfections in the surface of a paper, plastic card, and the product packaging is exploited to generate random fluctuation sequence by utilizing a portable laser scanner.
- **Phosphor PUF** [62]: The phosphor PUF proposed for brand protection in product as the physical identifier can be cloneable and reused. The idea is to produce a random sequence from scattering phosphor particles blended with cover materials such as a plastic cover attached to the product. The scattering pattern can be recognized by a mobile camera and the same scattering phosphor varies due to the camera properties such as brightness, distance and angle.
- **Radio Frequency Physical Unclonable Function (RF-PUF)** [27]: The RF-PUF utilized the inherent variation on analog/Radio Frequency characteristics, such as frequency offset, in-phase and quadrature components of the transmitter signal, which is composed of unique amplitude and phase for each transmitter. The machine learning model has been used at the receiver to extract the entropy sequence for each transmitter.
- **Image-based PUF** [133]: The authors introduce anti-counterfeiting techniques that exploit the inherent surface pattern of injection-molded plastic components for identification purposes. The unique surface pattern can be extracted by a simple camera.

6 PUF IMPLEMENTATION

FPGA is widely used to simulate the design of PUF circuits due to flexibility, customizability, and configurable logic gate as well as being faster to be deployed in IoT devices. In this section, we discuss PUF implementation in both FPGAs and ASIC. Table 3 summarizes the quality metrics and evaluation of designs in this section.

6.1 PUF on ASIC Implementation

Several PUF architectures have been implemented on CMOS technology to perform chip unclonability and identification. Due to the random variation in the manufacturing process, each fabricated chip is naturally unique. Therefore, it is difficult to clone, re-fabricate, and select the same
chip properties. Many works have been exploiting this inherent property. The authors of Reference [22] proposed an energy-efficient arbiter PUF using Current Starved (CS) inverters at the back stage of each multiplexers. The proposed arbiter utilizes two SR latches and NAND gate instead of D flip-flop in classical arbiter to improve the propagation delay at the output phase. Therefore, the design alleviates the effectiveness of fluctuating temperature at the output responses. Similarly, in Reference [86], the authors demonstrated an energy-efficient arbiter PUF that consists of 64 PUF cells using 45-nm CMOS technology. Each cell contains eight switching elements competing between different paths depending on challenge C values, eight selecting modules, and an arbiter. The design achieves high uniqueness and consumes low energy. Furthermore, the authors of Reference [4] proposed reconfigurable arbiter PUF based on hybrid Spin Transfer Torque (STT-MRAM/CMOS). The design employed the variation process of the transistors and MTJs connected in series with the control signals. The switch selection and PCSA is used as an arbiter to determine the delays of the discharge current between paths. Therefore, the design provides sufficient entropy response and produces large and unpredictable CRPs compared to the silicon/classical arbiter PUF (Section 5.1.1). The reliability enhancement/improvement of STT-MRAM PUF response is demonstrated in Reference [58]. However, the author in Reference [147] proposed the switched-capacitor PUF (SC-PUF) that consists of a switch capacitor circuit that senses and converts the mismatch between capacitor ratios into a voltage difference. The SC circuit works in charge redistribution state, providing unique keys and protection against invasive attacks. In CMOS technology, the variation between two identical transistors is determined by their distance. For instance, the author verifies the proposed SC-PUF with the mismatch of two transistors in space less than 10 μm is 0.7%. The evaluation of SC-PUF shows that the design can provide highly reliable responses with a uniqueness of 51.34%. In addition, the contact PUF proposed in Reference [61] exploits the contact failure in the interconnect layer of silicon and first metal. The contact failure is determined by the PUF bitcell, which is composed of a voltage divider including resistive load, contact, read transistor, and inverter output. However, contact failure occurs if the contact hole size is designed to be smaller than the design rule. Hence, when the contact is open, the bitcell PUF provides logic 1 and otherwise logic 0. The contact PUF has been evaluated in 180-, 130-, and 28-nm CMOS processes, and the cross-sectional views of the contact hole were obtained with a scanning electron microscope to illustrate the operation of the circuit. The design can generate sufficient randomness keys without error correction under variant temperature conditions and supply voltages. Moreover, a novel NAND-based set-reset flip-flop PUF is introduced in Reference [24] for low area overhead and power-constrained in IoT devices. The design approach relies on the cross-coupled path of the SR-FF circuit to extract the responses from a racing condition that occurs due to a forbidden input sequence (S=R=1) followed by lower inputs (S=R=0). Due to the flip-flop’s manufacturing process variation, the racing condition’s state will settle in logic “0” or “1.” The authors investigated the design with Synopsys HSPICE simulation for 90-, 45-, and 32-nm CMOS processes. However, the uniqueness of SR-FF approach is approximately 49% and reliable under different environmental conditions. In addition, the authors of Reference [141] proposed a novel dual-state analog PUF (DA PUF) that consists of the cell array (amplifier chain and readout circuit), signal drive circuit, timing control circuit, and parallel-serial converter circuit, fabricated in 55-nm CMOS process. The design provides 2 times more reliable bits compared to the traditional weak PUFs under various voltages and temperature variations with 99.9% and passes the NIST randomness test.

6.2 Arbiter PUF on FPGA

Many types of Arbiter FPGA PUFs have been proposed to improve the security of lightweight devices. The authors of Reference [79] proposed 3-1 Double Arbiter PUF with 3 arbiter PUF and
1 bit response and a new mode of operation for wires connection to an arbiter, which enhances the uniqueness of output responses. The feedback Oriented XOR flip-flop-based arbiter (FOXFF APUF) [119] for identification applications and provides a uniqueness improvement compared to Flip-Flop-based Arbiter PUF (FF-APUF) [47] by adding delay elements, such as feedback flip-flop to the design. The authors of Reference [103] introduced a combination of flip-flop and XOR gates-based arbiter, which enhances the uniqueness to 16% using families of FPGAs and consume more resources compared to the design in Reference [47]. As demonstrated in Reference [48], FF-APUF provides sufficient entropy and reliability compared to conventional arbiter PUF, which is suited for FPGA implementation and can be utilized in authentication protocols for lightweight devices. Moreover, the authors of Reference [51] introduced the new concept of bit self-test– (BST) based arbiter PUF by designing a detection circuit that produces a reliability flag. BST depends on propagation delay between paths and fluctuations in temperature and voltages. Therefore, based on the reliability flag, robust responses are generated, which is suitable for key generation and authentication.

6.3 RO PUF on FPGA

One alternative solution to conventional RO PUF is the Transient effect ring oscillator (TERO-PUF) [20], which exploits oscillation of four 64-loop TERO cells; each cell consists of cross-coupled circuit of two AND gates and two inverters. The design thwarts electromagnetic attack [18], which analyses electromagnetic emanation and obtains information from RO circuit. However, the circuit utilizes more hardware resources. Furthermore, the authors of Reference [137] introduced Phase Calibration Process (PC-PUF) technique to precisely measure the frequency of 128 RO array, which improved the stability and reduced the bit error rate of responses. In addition, the authors of Reference [40] demonstrated Galois ring oscillators (GARO-PUF), which compares different statistical parameters, such as variability and location of implemented PUF in FPGA of oscillators instead of frequencies, so the design overcomes the systematic issues that produced by RO frequencies and correlations when RO PUF implemented in some physical locations in FPGA. The RO PUF-based Lookup Table (LUT) FPGA introduced in Reference [76] extracts more entropy by applying the proposed method called Difference on Summed Difference to obtain the differences between frequencies. The design achieved sufficient entropy with low area overhead. Moreover, the authors in Reference [2] proposed two schemes (parallel and serial-based RO PUF) and replaced the counters with a Linear feedback shift register (LFSR) to eliminate the linear behavior in counters. However, the problem of linearity still appears in LFSR, so the scrambler circuit is also proposed to obliterate the correlation behavior. Therefore, the design produces unpredictable output and consumes low area and power. In Reference [139], a reconfigurable XOR gate-based RO PUF is proposed, which produced larger CRP and enhanced response stability; a reconfigurable XOR gate is implemented in the RO circuit instead of the inverter.

6.4 LFSR PUF on FPGA

Generally, LFSR has been widely used as Random Number Generator in cryptography, especially for lightweight devices with limited hardware resources. One of the security concerns associated with LFSR is its linearity and predictability. To address this, the authors of Reference [54] proposed lightweight configurable Shift Register–based PUF (SRPUF) with a non-linear function to improve the entropy and thwart machine learning attacks. Similarly, the authors of Reference [55] introduced LFSR-based strong PUF (L-PUF), which is a weak PUF at the front end of the circuit, such as Anderson PUF [8], combined with LFSR. Consequently, the authors of Reference [7] proposed asynchronous LFSR-based PUF (LFSR-PUF) that utilizes basic building blocks of the FPGA such as LUTs and flip-flops, which exploits the variation process of LFSR circuit to
produce random responses. Another work proposed a pseudo-linear feedback shift register with multiple RO (PL-MRO) PUF, which utilizes logic gates instead of shift registers in LFSR to exploit the delay behavior of the RO circuit [148]. The PL-MRO PUF, produces sufficient entropy, high speed operation, and low power consumption compared to conventional RO PUF.

6.5 Others PUF on FPGA
Several other PUF architectures have been proposed targeting FPGAs implementation and taking advantage of inherent FPGAs structures such as LUT and flip-flops. For instance, the authors of Reference [11] proposed an area-efficient SR-Latch PUF with two implementations methods that consist of four NAND gates with multiplexers to generate high entropy responses. In addition, the authors of Reference [131] introduced parallel scan design-based PUF and exploited the delay difference between pairs of shift registers as chains through the SR-Latch arbiter to reduce the area overhead and improve the uniqueness. Consequently, a combination of weak PUF and pseudo-Strong PUF (p-SPUF) was proposed in Reference [56]. The weak PUF produces a 1-bit response from the variation process of the logic gates, which feeds as an input to the LFSR. The design enhances the response randomness and can be well fitted in FPGAs due to low area cost. Furthermore, the dynamic reconfigurable PUF introduced in Reference [30] is based on three different logic circuit designs stored in external memory, so the FPGA can be configured by the programming system that has an access to external memory to select between configurable logic. This technique improves the hardware overhead, provides a large amount of CRPs, and thwarts machine learning attack. Similar work [132] proposed transformer PUF based on reconfigurable properties of RO basic circuit such as multiplexers, which select between different paths and configurable XOR gates. As a result, transformer PUF improves hardware efficiency and reliability compared to conventional configurable RO. Moreover, a modified Anderson PUF with Low-density parity checker error correction (LDPC) is proposed in Reference [65] to enhance the responses error bits. The LDPC was utilized to provide reliability under environmental variations conditions and high uniformity. However, the design has less uniqueness, which makes it unsuitable for authentication applications. Another work introduced optimization of Anderson PUF that utilized one configurable logic block in FPGA with inherent XOR gates [78], which improves the unpredictability of responses compared to conventional Anderson PUF.

7 THREAT LANDSCAPE AND SECURITY
In this section, we discuss some attacks and threats on IoT devices based on PUF. We start by describing some possible attacks and assumptions. Then we consider the following scenarios:

- Scenario 1: an adversary eavesdropping on the communications channel between IoT devices.
- Scenario 2: an eavesdropper with physical access to the devices.

In addition, the adversary can be active or passive; an active adversary can manipulate the operational temperature and power supply, while a passive adversary attempts to observe and intercept data in the communication channel. Ultimately, physical access to the PUF chip is required for active attacks.

7.1 Invasive Attack
This attack measures internal PUF properties, such as delays of the circuit and the power dissipation, to predict the response to a particular challenge. Such measurement entails physically removing external packaging and chip metal layers. However, as any probing attempt will directly affect the wiring and routing of the circuit’s delayed-paths, such actions will inevitably change the
PUF chip characteristics or even destroy it [42]. This attack is both costly and impractical, since the attacker needs specialized laboratory equipment while the IoT devices could be installed in protected or public areas.

Moreover, one of the common and powerful techniques used to breach a PUF circuit is side-channel attack. This attack relied on the leakage information that can be occupied by the power dissipation during the key generation process. For instance, the adversary can exploit the relation between power dissipation and CRPs on the PUF and measure the correlation between two variables, such as responses $R$ and correlation coefficient $r$ with the corresponding power dissipation $P$. Several works evaluated the side-channel attack in their proposed design. The authors in Reference [4] evaluated the (STT)-MRAM reconfigurable Arbiter PUF by measuring the correlation between power consumption and 800 generated responses. It was shown that there is no correlation associated between the two variables and the design resist side-channel attacks. Furthermore, the authors of Reference [71] proposed Cross-PUF attacks, which exploit the leakage power of the Latch in Arbiter PUF to train machine learning models, such as Support Vector Machines (SVM), to predict responses. Therefore, the adversary targets one PUF as a reference without recording CRPs to breach all PUFs that are fabricated from the same Graphic Design System, which contains a database of circuit layouts.

Furthermore, most commercial tamper-resistance techniques utilize battery-backed monitoring mechanisms to protect the IC from tampering. The authors of Reference [60] present a tamper-resistance battery-less approach made from standard flexPCB technology for silicon-based PUFs to protect the internal components and provide an additional layer of security, which is usually required by most cryptographic modules.

### 7.2 Non-invasive Attack

This attack attempts to intercept the communication channel between the device and the server without physical access to the internal components of the IoT device. In this case, the adversary intercepts the authentication protocol that forms the challenge-response pairs and develops machine learning models to predict them (see Section 7.2.1). The Arbiter-PUF (Section 5.1.1) is vulnerable to the machine learning attack, which works by building a model that learns the correlation of known CRPs and predicts the unknown CRPs. The authors of Reference [150] introduced a defensive interface that improves the arbiter-PUF and similar design to resist the machine learning attack. Similarly, the authors of Reference [144] proposed a Random Set-based Obfuscation (RSO) technique for PUF to complicate the correlation between CRPs and minimize the number of the collected data by the attacker to resist machine learning attack. The proposed structure is composed of an XOR gate, True Random Number Generator, non-volatile memory, and register. It provides a set-update mechanism to update the set of the CRPs number collected by the attacker when reaching the preset value. The experimental results show that the RSO can reduce the prediction accuracy for various machine learning attack for a $64 \times 64$ Arbiter PUF to 50%. Several designs have been proposed to overcome this vulnerability in the arbiter-PUF, such as XOR Arbiter PUF [88, 118] and Feed-Forward Arbiter PUF [43, 73, 122]. In addition, the authors of Reference [102] evaluated various machine learning models such as Logistic Regression (LR), SVMs, and Evolution Strategies (ES) against Arbiter PUF. Moreover, the authors of Reference [16] demonstrated a non-invasive attack against SRAM PUF based on chip correlation parameters with identical specifications that share the same manufacturing process. The experiment showed that the adversary was able to guess approximately 45% of the CRPs for SRAM PUF.

#### 7.2.1 Machine Learning Attack

Numerous research papers used these attacks against several designs, so designers can evaluate the security strength, weaknesses and how effectively the attacker can predict the CRPs.
The PUF circuit can be designed to maintain a limited number of challenges in a very short period for each authentication process. However, the challenge–response pair must never be reused to prevent any machine learning attack [128]. In fact, producing a large number of pairs is usually required to prevent such prediction. In this case, the PUF circuit will be large and that will increase computational overhead. To address this issue, the authors of Reference [14] proposed a reconfigurable design that increases the number of pairs without affecting the computational resources of the IoT.

The aforementioned attack scenarios need to be considered to develop a secure PUF circuit that can resist the machine learning attack and detect any possible invasive attack. Strong PUFs can be used with the secure authentication protocol to satisfy these security requirements. The authors of Reference [38] introduced obfuscated challenge–response protocol to prevent machine learning attacks without conventional cryptography, which consists of a PUF chip, random number generator, and control block. Furthermore, the authors of Reference [88] proposed a training model with Multi-layer Perceptrons (MLP) as a neural network to predict CRPs for XOR Arbiter PUF. The study shows that the accuracy of the prediction depends on the size of the XOR gates (i.e., when the XOR size increases the prediction accuracy percentage decreases). However, the authors believe that a prediction rate below 80% can be considered secure as the authentication process relied on multiple response bits (approximately 64 bits). Similarly, the authors of Reference [13] demonstrated a neural network attack against feed-forward XOR PUF with 50% prediction rate for multiple PUF stages. This shows that the proposed feed-forward XOR PUF is considered more secure compared to XOR PUF. Moreover, the authors of Reference [54] introduced various attack models in their design of configurable LFSR-PUF. They performed LR, ES, and Neural Networks. As a result, the prediction rate is approximately 50% of the proposed models. In Reference [132], the authors implemented two models of attacks, LR and ES, for 128-stage Transformer PUF with eight XOR gates. The evaluation achieved 60% accuracy compared to classical RO PUF with a 90% prediction rate. In addition, the authors of Reference [104] developed two mathematical attacks on previous PUF design, lightweight secure PUF [83] and composite PUF [105], which consists of multiple different PUF design stages that usually combine strong and weak PUFs. However, the authors of Reference [4] applied SVM, LR, and MLP modeling attacks on their proposed STT-MRAM reconfigurable Arbiter PUF. It was shown that the design reduces the prediction rate to 65.12% without utilizing XOR gates and 44.34% with XOR gates. Furthermore, the authors of Reference [37] studied the various modeling attacks such as LR, ES, Naive Bayes, and AdaBoost on Arbiter PUF with different cases in terms of the number of training sets, the efficiency of the machine learning algorithms and several numbers of Arbiter stages. The experiment shows that LR and ES performed better for large datasets, while Naive Bayes and AdaBoost applied for small datasets. Additionally, the training time of Naive Bayes is faster (0.0007 s) compared to other models with the highest prediction rate, as shown in Table 4.

In addition, the authors of Reference [91] introduced a novel Interpose PUF (iPUF) design consisting of upper and lower XOR-Arbiter PUF, such that the responses and challenges of the upper layer is interposed in the lower layer to create new challenges, thus generating final responses. This PUF prevents the reliability-based CMA-ES attack, where the reliability data can be obtained from repeated measurement under voltages and temperature variations. This information allows the attacker to measure the sensitivity and predict the responses. They also show that the design can prevent classical machine learning attacks including LR. However, a novel modeling attack strategy for iPUF as proposed in Reference [134] can breach the iPUF building block separately with an accuracy of 95%. Similarly, the authors of Reference [125] analyzed the vulnerabilities of the iPUF by optimizing the modeling attack using gradient-based optimization, which combines
the reliability attack, weight constraint, and LR. This framework exploits the responses and reliability information together to make the attack more effective.

Moreover, the multiplexers have been widely used in delay-based PUFs for switching between paths. However, the authors of Reference [3] evaluated multiple stages of multiplexer PUF based on the Neural Network method to predict the generated responses and showed that the multiplexer PUF is vulnerable to the machine learning attack with a high prediction rate. Similarly, the authors of Reference [111] introduced two innovative modeling attacks, referred to as logical approximation and global approximation, utilizing ANN to characterize the nonlinear structure of variant multiplexer-PUF family and XOR Arbiter PUF. The logical approximation method leverages linear functions to approximate logical operations on the combination of logical gates, including AND, NOT, and OR in the PUF design. While the global approximation method was utilized to model the correlation between the CRPs. The experimental results show that the MPUF family and XOR PUF are vulnerable to the approximation attacks with high accuracy.

Consequently, the LR and SVM modeling attacks have been analyzed against memristive Xbar PUF in Reference [68] under linear and nonlinear (e.g., XOR) architectures. The evaluation of LR-based attack shows that the XORing nonlinearity drops the prediction rate accuracy from 73% to 50.5%, which is near ideal, while exhibiting high resilience against such attacks. Table 4 summarizes the common machine learning attack models and related PUFs with the accuracy of predicting CRPs table. In addition, the authors of Reference [115] exploited the helper data techniques that are used to correct the noisy responses in PUF. They proposed Siamese Neural Network to predict

| Ref. | PUF Architectures | ML models | Prediction Rate (%) | Training Time | CRPs | Bit Length |
|------|------------------|-----------|---------------------|---------------|------|------------|
| [102] | Arbiter PUF | LR<sup>a</sup> | 95 | 0.01 s | 640 | 64 |
| [37] | Arbiter PUF | LR | 79.05 | 0.0024 s | 400 | 64 |
|       |             | ES<sup>b</sup> | 74.8 | 0.0011 s |       |       |
|       |             | Naive Bayes | 84.30 | 0.1167 s |       |       |
|       |             | AdaBoost  | 83.10 | —   |       |       |
| [102] | RO PUF [118] | QS<sup>c</sup> | 99 | — | 83,941 | 1024 |
| [88] | XOR Arbiter PUF | NN<sup>d</sup> | 50.40<sup>e</sup> | — | 24,900 | 64 |
| [13] | FF XOR PUF | NN<sup>d</sup> | 50 | — | 100,000 | 32 |
| [54] | SRPUF | LR | 49.9 | — |       |       |
|       |       | ES<sup>b</sup> | 50.20 | — |       |       |
|       |       | DL<sup>f</sup> | 50.28 | 54 min 30 s |       |       |
| [112] | Transformer PUF | LR | 60 | 60 | 2000 | 128 |
| [4]  | MRAM PUF | LR | 65.12 | 64.53 | — | 10,000 | 15 |
|       |       | SVM | 62.7 | — |       |       |
| [3]  | Multiplexer PUF<sup>h</sup> | NN | 1.26 | — | 8.55 × 10<sup>i</sup> | 32 |
| [68] | Memristor PUF | LR | 50.5<sup>i</sup> | 56.5<sup>i</sup> | — | 5000 | Xbar size 32 × 2 |
|       |       | SVM |       |       |       |       |

<sup>a</sup> Logistic Regression.
<sup>b</sup> Support Vector Machines.
<sup>c</sup> Quick Sort.
<sup>d</sup> Neural Network.
<sup>e</sup> XOR PUF.
<sup>f</sup> Evolution Strategies.
<sup>g</sup> Deep Learning methods.
<sup>h</sup> Seven stages.
<sup>i</sup> With XORing.
the dependencies of CRPs of the helper data that are publicly accessible to the attacker without direct access to the PUF.

7.2.2 Brute-force. The attacker can try to clone the CRP table of the PUF circuit by enumerating all possible combinations of challenge–response pairs by repeatedly querying the PUF circuit. Clearly, this attack is very time-consuming and will generate a huge CRP table requiring considerable storage. The authors of Reference [96] introduced a PUF-based Reliable and Lightweight Authentication Protocol that sets the standard for robustness against brute-force, replay, and modeling attacks. Similarly, the authors of Reference [74] presented a PUF-based solution to build a secure system that resists advanced attacks, including ID and password pair guessing, brute-force, and capture attacks.

7.3 Semi-invasive

This attack tries to access the PUF chip without destruction, so the adversary can apply multiple techniques, such as photonic emission analysis [121], to physically characterize the arbiter-PUF from the backside. In addition, other techniques, such as laser fault injection and optical contactless probing, have been demonstrated in Reference [84] to predict the secret key from the PUF chip. Similarly, the authors of Reference [18] proposed an electromagnetic analysis attack that identifies leakage frequencies of the Ring Oscillator PUF (Section 5.1.1). However, these types of attacks still require specialized laboratory equipment.

8 CONCLUSION AND OUTLOOK

In recent years, advances in PUF architectures provided a solution for solving and enhancing the security of IoT devices. In this article, we provided an overview of PUF architectures to provide applicable security solutions for IoT environments due to the low computational complexity of PUF circuit design and less energy and to improve the quality metrics such as randomness, uniqueness, and reliability. In addition, the PUF-based authentication protocols have been discussed and common security concerns and effective attacks against PUF were reviewed.

More work is still needed to test different properties of PUF to evaluate their security strengths and weakness. The aforementioned techniques provide lightweight authentication for IoT without utilizing the traditional cryptography methods that can increase power and resource consumption, still without having to store secret keys in memory.

More research is needed to design proper PUF architecture that prevents machine learning attacks, which traditional cryptography methods, such as hash function, are used to prevent in non-PUF solutions. However, confidentiality and integrity based on PUF on IoT devices are still not addressed by the PUF community, which makes it largely an open problem.

In practice, conventional confidentiality and integrity techniques have been utilized by the PUF authentication protocols, trading off circuit and computational complexity. Therefore, more research is needed to provide suitable and practical encryption and integrity mechanism that can be implemented in lightweight applications with low energy consumption and higher security.

REFERENCES

[1] Saeed Abdolzadeh and Axel Sikora. 2022. A lightweight mutual authentication protocol based on physical unclonable functions. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST’22). 10.1109/host54066.2022.9840132

[2] Abby Aguirre, Michael Hall, Timothy Lim, Jonathan Trinh, Wei Yan, and Fatemeh Tehranipoor. 2020. A systematic approach for internal entropy boosting in delay-based RO PUF on an FPGA. In Proceedings of the IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS’20). 623–626. 10.1109/MWSCAS48704.2020.9184468

ACM Computing Surveys, Vol. 55, No. 14s, Article 314. Publication date: July 2023.
Physical Unclonable Functions (PUF) for IoT Devices

314:25

[3] Meznah A. Alamro and Khalid T. Mursi. 2021. Machine learning attack on a multiplexer PUF variant using silicon data: A case study on rMPUFs. In Proceedings of the IEEE 6th International Conference on Computer and Communication Systems (ICCCS’21). 1017–1022. 10.1109/ICCCSS2626.2021.9449179

[4] Rashid Ali, You Wang, Haoyuan Ma, Zhengyi Hou, Deming Zhang, Erya Deng, and Weisheng Zhao. 2021. A re-configurable arbiter PUF based on STT-MRAM. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS’21). 1–5. 10.1109/ISCAS51556.2021.9401053

[5] Mohammed Saeed Alkatehiri, Yu Zhuang, Mikhail Korobkov, and Abdur Rashid Sangi. 2017. An experimental study of the state-of-the-art PUFs implemented on FPGAs. In Proceedings of the IEEE Conference on Dependable and Secure Computing. 174–180. 10.1109/DESEC.2017.8073844

[6] Muhammad Naveed Aman, Mohammed Haroon Bashir, and Biplob Sikdar. 2019. Data provenance for IoT with light weight authentication and privacy preservation. IEEE IoT J. 6, 6 (2019), 10441–10457. 10.1109/JIOT.2019.2939286

[7] Fathi Amsaad, Ahmed Sherif, Amer Dawoud, Mohammed Niamat, and Selck Kose. 2018. A novel FPGA-based LFSR PUF design for IoT and smart applications. In Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON’18). 99–104. 10.1109/NAECON.2018.8556699

[8] Jason H. Anderson. 2010. A PUF design for secure FPGA-based embedded systems. In Proceedings of the 15th Asia and South Pacific Design Automation Conference (ASP-DAC’10). 1–6. 10.1145/1611675.1611678

[9] Md Tanvir Arafin, Haoting Shen, Mark M. Tehranipoor, and Gang Qu. 2019. LPN-based device authentication using resistive memory. In Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI’19). 10.1145/3299874.3317970

[10] Myrto Arapinis, Mahshid Delavar, Mina Doosti, and Elham Kashefi. 2021. Quantum physical unclonable functions: Possibilities and impossibilities. Quantum 5 (2021), 475. DOI: 10.22331/q-2021-06-15-475

[11] Amir Ardakani and Shahriar Baradaran Shokouhi. 2016. A secure and area-efficient FPGA-based SR-latch PUF. In Proceedings of the 8th International Symposium on Telecommunications (IST’16). 94–99. 10.1109/ISTEL.2016.7881790

armatix. 2021. Armatix ip1 Limited Edition Set. Retrieved from http://www.armatix.us/ip1-Limited-Edition.804.0.html?XL=7.

[12] S. V. Sandeep Avvaru, Ziqing Zeng, and Keshab K. Parhi. 2020. Homogeneous and heterogeneous feed-forward XOR physical unclonable functions. IEEE Trans. Inf. Forens. Secur. 15 (2020), 2485–2498. 10.1109/TIFS.2020.2968113

[13] Armin Babaei and Gregor Schiele. 2017. Spatial reconfigurable physical unclonable functions for the internet of things. In Security, Privacy, and Anonymity in Computation, Communication, and Storage, Lecture Notes in Computer Science, 312–321. 10.1007/978-3-319-72395-2_29

[14] Armin Babaei and Gregor Schiele. 2019. Physical unclonable functions in the internet of things: State of the art and open challenges. Sensors 19, 14 (July 2019), 3208. 10.3390/s19143208

[15] B. M. S. Bahar Talukder, Farah Ferdaus, and Md Tausifur Rahman. 2021. Memory-based PFUs are vulnerable as well: A non-invasive attack against SRAM PFUs. IEEE Trans. Inf. Forens. Secur. 16 (2021), 4035–4049. 10.1109/TIFS.2021.3101045

[16] Ilia A. Bautista Adames, Jayita Das, and Sanjukta Banjha. 2016. Survey of emerging technology based physical unclonable functions. In Proceedings of the International Great Lakes Symposium on VLSI (GLSVLSI’16). 317–322. 10.1145/2902961.2903044

[17] Pierre Bayon, Lilian Bossuet, Alain Aubert, and Viktor Fischer. 2013. Electromagnetic analysis on ring oscillator-based true random number generators. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS’13). 1954–1957. 10.1109/ISCAS.2013.6572251

[18] Rob Berg and Van Den. 2012. Entropy analysis of physical unclonable functions.

[19] Lilian Bossuet, Xuan Thuy Ngo, Zouha Cherif, and Viktor Fischer. 2014. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. IEEE Emerg. Top. Comput. 2, 1 (2014), 30–36. 10.1109/TETC.2013.2287182

[20] James D. Buchanan, Russell P. Cowburn, Ana-Vanessa Jausovec, Dorothée Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A. Allwood, Matthew T. Bryan, and et al. 2005. ‘fingerprinting’ documents and packaging. Nature 436, 7050 (2005), 475–475. 10.1038/436475a

[21] Yuan Cao, Wenhao Zheng, Xiaoqin Zhao, and Chip-Hong Chang. 2019. An energy-efficient current-starved inverter based physical strong unclonable function with enhanced temperature stability. IEEE Access 7 (2019), 105287–105297. 10.1109/ACCESS.2019.2932022

[22] Zhen Cao, Shuai Zhang, Jian Zhang, Nuo Xu, Ruofan Li, Zhe Guo, Jijun Yun, Min Song, Qiming Zou, Li Xi, Oukjae Lee, Xiaofei Yang, Xuecheng Zou, Jeongmin Hong, and Long You. 2021. Reconfigurable physical unclonable function based on spin-orbit torque induced chiral domain wall motion. IEEE Electr. Dev. Lett. 42, 4 (2021), 597–600. 10.1109/LED.2021.3057638

[23] Rohith Prasad Challa, Sheikh Ariful Islam, and Shrivas Katkoori. 2019. An SR flip-flop based physical unclonable functions for hardware security. In Proceedings of the IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS’19). 574–577. 10.1109/MWSCAS.2019.8885066

ACM Computing Surveys, Vol. 55, No. 14s, Article 314. Publication date: July 2023.
[25] Chip-Hong Chang and Miodrag Potkonjak. 2016. Secure System Design and Trustable Computing. Springer International.

[26] Chip-Hong Chang, Yue Zheng, and Le Zhang. 2017. A retrospective and a look forward: Fifteen years of physical unclonable function advancement. IEEE Circ. Syst. Mag. 17, 3 (2017), 32–62. 10.1109/MCAS.2017.2713305

[27] Baibhab Chatterjee, Debayan Das, and Shreyas Sen. 2018. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST’18). 205–208. 10.1109/HST.2018.838916

[28] Wei-Chen Chien, Yu-Chiang Chao, Yoo-Tung Tsou, Sy-Yen Kuo, and Ching-Ray Chang. 2020. STT-DPSA: Digital PUF-based secure authentication using STT-MRAM for the internet of things. Micromachines 11, 5 (2020), 502. 10.3390/mi11050502

[29] L. Chua. 1971. Memristor—the missing circuit element. IEEE Trans. Circ. Theory 18, 5 (1971), 507–519. 10.1109/TCT.1971.1083337

[30] Yijun Cui, Chenghua Wang, Yumpeng Chen, Ziwei Wei, Mengxian Chen, and Weiqiang Liu. 2019. Dynamic reconfigurable PUFs based on FPGA. In Proceedings of the IEEE International Workshop on Signal Processing Systems (SiPS’19). 79–84. 10.1109/SiPS7522.2019.9020444

[31] Jayita Das, Kevin Scott, Drew Burgett, Srinal Rajaram, and Sanjukta Bhanja. 2014. A novel geometry based MRAM PUF. In Proceedings of the 14th IEEE International Conference on Nanotechnology. 859–863. 10.1109/NANO.2014.6968027

[32] Jayita Das, Kevin Scott, Srinal Rajaram, Drew Burgett, and Sanjukta Bhanja. 2015. MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS. IEEE Trans. Nanotechnol. 14, 3 (2015), 436–443. 10.1109/TNANO.2015.2397951

[33] Ding Deng, Shen Hou, Zhenyu Wang, and Yang Guo. 2020. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access 8 (2020), 161427–161437. 10.1109/ACCESS.2020.3021205

[34] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Advances in Cryptology - EUROCRYPT 2004, Christian Cachin and Jan L. Camenisch (Eds.). Springer, Berlin, 523–540.

[35] Elena Dubrova. 2018. A reconfigurable arbiter PUF with 4 x 4 switch blocks. In Proceedings of the IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL’18). 31–37. 10.1109/ISMVL.2018.00014

[36] A. V. Fadeev and K. V. Rudenko. 2021. To the issue of the memristor’s hrs and LRS states degradation and data retention time. Russ. Microelectr. 50, 5 (2021), 311–325. 10.1134/s1063739721050024

[37] Yue Fang, Chenghua Wang, Qingqing Ma, Chongyan Gu, Maire O’Neill, and Weiqiang Liu. 2018. Attacking arbiter PUFs using various modeling attack algorithms: A comparative study. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS’18). 394–397. 10.1109/APCCAS.2018.8605618

[38] Yansong Gao, Gefei Li, Hua Ma, Said F. Al-Sarawi, Omid Kavehe, Derek Abbott, and Damith C. Ranasinghe. 2016. Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices. In Proceedings of the IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops’16). 10.1109/percomw.2016.7457162

[39] Yansong Gao, Hua Ma, Said F. Al-Sarawi, Derek Abbott, and Damith C. Ranasinghe. 2018. PUF-FSM: A controlled strong PUF. IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst. 37, 5 (2018), 1104–1108. 10.1109/TCAD.2017.2740297

[40] Miguel García-Bosque, Guillermo Diez-Señorans, Carlos Sánchez-Azqueta, and Santiago Celma. 2020. Proposal and analysis of a novel class of PUFs based on galois ring oscillators. IEEE Access 8 (2020), 157830–157839. 10.1109/ACCESS.2020.3020200

[41] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. 2002. Controlled physical random functions. In Proceedings of the 18th Annual Computer Security Applications Conference. 149–160. 10.1109/CSAC.2002.1176287

[42] Blaise Gassend, Dwayne Clarke, Marten van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS’02). Association for Computing Machinery, New York, NY, 148–160. 10.1145/586110.586132

[43] Blaise Gassend, Daihyun Lim, Dwayne Clarke, Marten Van Dijk, and Srinivas Devadas. 2004. Identification and authentication of integrated circuits. Concurr. Comput.: Pract. Exp. 16, 11 (2004), 1077–1098. 10.1002/cpe.805

[44] Michael Geis, Karen Gettins, and Michael Vai. 2017. Optical physical unclonable function. In Proceedings of the IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS’17). 10.1109/mwscas.2017.8053156

[45] Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, BorisŠkoric, and Pepijn W. H. Pinkse. 2014. Quantum-secure authentication of a physical uncloneable key. Optica 1, 6 (December 2014), 421–424. 10.1364/OPTICA.1.000421

[46] Konstantinos Goutsos and Alex Bystrov. 2019. Lightweight PUF-based continuous authentication protocol. In Proceedings of the International Conference on Computing, Electronics Communications Engineering (iCCECE’19). 229–234. 10.1109/iccece46942.2019.8941608
[47] Chongyan Gu, Yijun Cui, Neil Hanley, and Máire O’Neill. 2016. Novel lightweight FF-APUF design for FPGA. In Proceedings of the 29th IEEE International System-on-Chip Conference (SOCC’16), 75–80.

[48] Chongyan Gu, Weiqiang Liu, Yijun Cui, Neil Hanley, Maire O’Neill, and Fabrizio Lombardi. 2019. A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation. IEEE Trans. Emerg. Top. Comput. (2019), 1–1. 10.1109/TETC.2019.2935465

[49] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls. 2007. FPGA intrinsic PUFs and their use for IP protection. In Cryptographic Hardware and Embedded Systems (CHES’07). Pascal Paillier and Ingrid Verbauwhede (Eds.). Springer, Berlin, 63–80.

[50] Basel Halak, Mark Zwolinski, and M. Syafiq Mispan. 2016. Overview of PUF-based hardware security solutions for the internet of things. In Proceedings of the IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS’16). 1–4. 10.1109/MWSCAS.2016.7870046

[51] Zhangqing He, Wanbo Chen, Lingchao Zhang, Gaojun Chi, Qi Gao, and Lein Harn. 2020. A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test. IEEE Access 8 (2020), 181751–181762. 10.1109/ACCESS.2020.3028514

[52] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. 2014. Physical unclonable functions and applications: A tutorial. Proc. IEEE 102, 8 (2014), 1126–1141. 10.1109/JPROC.2014.2320516

[53] D. E. Holcomb, W. P. Burleson, and K. Fu. 2007. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In Proceedings of the Conference on Radio Frequency Identification Security (RFID’07).

[54] Shen Hou, Ding Deng, Zhenyu Wang, Jiahe Shi, Shaoqing Li, and Yang Guo. 2020. A dynamically configurable LFSR-based PUF design against machine learning attacks. CCF Trans. High Perf. Comput. 3, 1 (2020), 31–56. 10.1007/s42514-020-00060-7

[55] Shen Hou, Yang Guo, and Shaoqing Li. 2019. A lightweight LFSR-based strong physical unclonable function design on FPGA (January 2019). IEEE Access 05 (2019), 1–1. 10.1109/ACCESS.2019.2917259

[56] Shen Hou, Yang Guo, Shaoqing Li, Ding Deng, and Yan Lei. 2019. A lightweight and secure-enhanced strong PUF design on FPGA. IEICE Electr. Expr. 16, 24 (2019), 20190695–20190695. 10.1587/exele.20190695

[57] Jeremy Hsu. 2015. New U.S. Military Chip Self Destructs on Command. Retrieved from https://spectrum.ieee.org/tech-talk/hardware/us-militarys-chip-self-destructs-on-command.

[58] Yupeng Hu, Linjun Wu, Zhoujun Chen, Yun Huang, Xiaolin Xu, Kefin Li, and Jiliang Zhang. 2021. STT-MRAM-based reliable weak PUF. IEEE Trans. Comput. (2021), 1–1. 10.1109/TC.2021.3095657

[59] Hebatallah M. Ibrahim, Heba Abunahla, Baker Mohammad, and Hoda AlKhzaimi. 2022. Memristor-based PUF for lightweight cryptographic randomness. Sci. Rep. 12, 1 (2022). 10.1038/s41598-022-11240-6

[60] Vincent Immiler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, JinYu Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, and Georg Sigl. 2018. Secure physical enclosures from covers with tamper-resistance. IACR Trans. Cryptogr. Hardw. Embed. Syst. (2018), 51–96. 10.46586/tches.v2019.i1.51-96

[61] Duhyun Jeon, Dongmin Lee, Dong Kyue Kim, and Byong-Deok Choi. 2022. Contact PUF: Highly stable physical unclonable functions based on contact failure probability in 180 nm, 130 nm, and 28 nm CMOS processes. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST’22). 85–88. 10.1109/HOST54066.2022.9839746

[62] Dan Jiang and Cheun Ngen Chong. 2008. Anti-counterfeiting using phosphor PUF. In Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification. 59–62. 10.1109/IWASID.2008.4688338

[63] Qi Jiang, Xin Zhang, Ning Zhang, Youliang Tian, Xindi Ma, and Jianfeng Ma. 2019. Two-factor authentication protocol using physical unclonable function for IoV. In Proceedings of the IEEE/CIC International Conference on Communications in China (ICCC’19). 195–200. 10.1109/IJCCChina.2019.8855828

[64] Zouha Cherif Jouini, Jean-Luc Danger, and Lilian Bossuet. 2011. Performance evaluation of physically unclonable function by delay statistics. In Proceedings of the IEEE 9th International New Circuits and Systems Conference. 482–485. 10.1109/NEWCAS.2011.5981324

[65] Manasa kalya and Sathish Kumar. 2020. Low complexity ldpc error correction code for modified anderson PUF to improve its uniformity. In Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC’20). 997–1002. 10.1109/ICOSEC49089.2020.9215273

[66] Hyunho Kang, Yohei Hori, and Akashi Satoh. 2012. Performance evaluation of the first commercial PUF-embedded RFID. In Proceedings of the 1st IEEE Global Conference on Consumer Electronics 2012. 5–8. 10.1109/GCCE.2012.6379926

[67] Muhammad Ibrar Khan, Shawkat Ali, Aref Al-Tamimi, Arshad Hassan, Ataul Aziz Ikram, and Amine Bermak. 2021. A robust architecture of physical unclonable function based on memristor crossbar array. Microelectr. J. 116 (2021), 105238. 10.1016/j.mejo.2021.105238

[68] Muhammad Ibrar Khan, Shawkat Ali, Ataul Aziz Ikram, and Amine Bermak. 2021. Optimization of memristive crossbar array for physical unclonable function applications. IEEE Access 9 (2021), 84480–84489. 10.1109/ACCESS.2021.3087810
[69] Patrick Koeberl, Unal Kocabas, and Ahmad-Reza Sadeghi. 2013. Memristor PUFs: A new generation of memory-based physically unclonable functions. In Proceedings of the Design, Automation Test in Europe Conference Exhibition (DATE’13). 428–431. 10.7873/DATE.2013.096

[70] S. T. Choden Konigsmark, Leslie K. Hwang, Deming Chen, and Martin D. F. Wong. 2014. CNPUF: A carbon nanotube-based physically unclonable function for secure low-energy hardware design. In Proceedings of the 19th Asia and South Pacific Design Automation Conference (ASP-DAC’14). 73–78. 10.1109/ASFDAC.2014.6742869

[71] Trevor Kroeger, Wei Cheng, Sylvain Guillely, Jean-Luc Danger, and Naghmeh Karimi. 2020. Cross-PUF attacks on arbiter-PUFs through their power side-channel. In Proceedings of the IEEE International Test Conference (ITC’20). 1–5. 10.1109/ITC44778.2020.9352541

[72] Sandeep S. Kumar, Jorge Guajardo, Roel Maes, Geert-Jan Schrijen, and Pim Tuyls. 2008. Extended abstract: The butterfly PUF protecting IP on every FPGA. In Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust. 67–70. 10.1109/HST.2008.4559053

[73] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas. 2004. A technique to build a secret key in integrated circuits for identification and authentication applications. In Proceedings of the Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37325). 176–179. 10.1109/VLSIC.2004.1346548

[74] JoonYoung Lee, JiHyeon Oh, DeokKyu Kwon, MyeongHyun Kim, Sunglin Yu, Nam-Su Jho, and Youngho Park. 2022. PUFTAP-IOT: PUF-based three-factor authentication protocol in IOT environment focused on sensing devices. Sensors 22, 18 (2022). 10.3390/s22187075

[75] Yongwoo Lee, Jinsu Yoon, Hyo-Jin Kim, Geon-Hwi Park, Dae Hwan Kim, Dong Myong Kim, Min-Ho Kang, and Sung-Jin Choi. 2019. Carbon nanotube network transistor for a physical unclonable functions-based security device. In Proceedings of the IEEE 19th International Conference on Nanotechnology (IEEE-NANO’19). 227–230. 10.1109/NANO46743.2019.8893990

[76] Jin Li, Lei Li, Ji Yang, Yuanhang He, Wanting Zhou, and Shiwei Yuan. 2020. An efficient and stable composed entropy extraction method for FPGA-based RO PUF. IEICE Electr. Expr. 17, 24 (2020), 20200350–20200350. 10.1587/elex.17.20200350

[77] Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas. 2005. Extracting secret keys from integrated circuits. IEEE Trans. VLSI Syst. 13, 10 (2005), 1200–1205. 10.1109/TVLSI.2005.859470

[78] Armin Lotfy, Masoud Kaveh, Diego Martin, and Mohammad Reza Mosavi. 2021. An efficient design of anderson PUF by utilization of the xilinx primitives in the SLICEM. IEEE Access 9 (2021), 23025–23034. 10.1109/ACCESS.2021.3056291

[79] Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto, and Kazuo Sakiyama. 2014. A new mode of operation for arbiter PUF to improve uniqueness on FPGA. In Proceedings of the Federated Conference on Computer Science and Information Systems. 871–878. 10.15439/2014F140

[80] Roel Maes and Ingrid Verbauwhede. 2010. Physically unclonable functions: A study on the state of the art and future research directions. In Information Security and Cryptography Towards Hardware-Intrinsic Security. Springer, Berlin, 3–37. 10.1007/978-3-642-14452-3_1

[81] Mahabub Hasan Mahalat, Shreyaa Saha, Anindan Mondal, and Bibhash Sen. 2018. A PUF based light weight protocol for secure WiFi authentication of IoT devices. In Proceedings of the 8th International Symposium on Embedded Computing and System Design (ISED’18). 183–187. 10.1109/ISED.2018.8703993

[82] Abhranil Maiti, Vikash Gunreddy, and Patrick Schaumont. 2011. A systematic method to evaluate and compare the performance of physical unclonable functions. IACR Cryptol. ePrint Arch. 2011 (01 2011), 657. 10.1007/978-1-4614-1362-2_11

[83] Mehrdad Majzooobi, Farinaz Koushanfar, and Miodrag Potkonjak. 2008. Lightweight secure PUFs. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design. 670–673. 10.1109/ICCAD.2008.4681648

[84] Dominik Merli, Johann Heyszl, Benedikt Heinz, Dieter Schuster, Frederic Stumpf, and Georg Sigl. 2013. Localized electromagnetic analysis of RO PUFs. In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST’13). 10.1109/hst.2013.6581559

[85] Jin Miao, Meng Li, Subhendu Roy, Yuzhe Ma, and Bei Yu. 2018. SD-PUF: Spliced digital physical unclonable function. IEEE Trans. Comput.-Aided. Des. Integr. Circ. Syst. 37, 5 (2018), 927–940. 10.1109/TCAD.2017.2740296

[86] Mona Moradi, Reza Faghil Mirzaee, and Sha Tao. 2020. CMOS arbiter physical unclonable function with selecting modules. In Proceedings of the 20th International Symposium on Computer Architecture and Digital Systems (CADS’20). 1–6. 10.1109/CADSS5070.2020.9211853

[87] Mona Moradi, Sha Tao, and Reza Faghil Mirzaee. 2017. Physical unclonable functions based on carbon nanotube FETs. In Proceedings of the IEEE 47th International Symposium on Multiple-Valued Logic (ISMVL’17). 124–129. 10.1109/ISMVL.2017.33

[88] Khalid T. Mursi, Yu Zhuang, Mohammed Saeed Alkatheiri, and Ahmad O. Aseeri. 2019. Extensive examination of XOR arbiter PUFs as security primitives for resource-constrained IoT devices. In Proceedings of the 17th International Conference on Privacy, Security and Trust (PST’19). 1–9. 10.1109/PST47121.2019.8949070
[89] Omar Nakhila and Cliff Zou. 2016. User-side Wi-Fi evil twin attack detection using random wireless channel monitoring. In Proceedings of the IEEE Military Communications Conference (MILCOM’16). 1243–1248. 10.1109/MILCOM.2016.7795501

[90] Arash Nejat, Frederic Ouatara, Mohammad Mohammadinodoushan, Bertrand Cambou, Ken Mackay, and Lionel Torres. 2020. Practical experiments to evaluate quality metrics of MRAM-based physical unclonable functions. IEEE Access 8 (2020), 176042–176049. DOI: 10.1109/ACCESS.2020.3024598

[91] Phuong Ha Nguyen, Durga Prasad Sahoo, Chenghu Jin, Kaleel Mahmood, Ulrich Rührmair, and Marten Van Dijk. 2019. The interpose PUF: Secure PUF design against state-of-the-art machine learning attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst. (2019), 243–290. 10.46586/tches.v2019.i4.243-290

[92] Hassan N. Noura, Reem Melki, and Ali Chehab. 2019. Secure and lightweight mutual multi-factor authentication for IoT communication systems. In Proceedings of the IEEE 90th Vehicular Technology Conference (VTC’19). 1–7. 10.1109/VTCFall.2019.8891082

[93] Ravi Fappu, Ben Recht, Jason Taylor, and Neil A. Gershenfeld. 2002. Physical one-way functions. Science 297 (2002), 2026–2030.

[94] Akash B Patel, S. Kamatchi, and Kaveri Hatti. 2021. Design of efficient low power strong PUF for security applications. In Proceedings of the 2nd International Conference on Smart Hardware and Communication (iCOSEC’21). 372–377. 10.1109/iCOSEC51865.2021.9591696

[95] Koustubh Phalak, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh. 2021. Quantum PUF for security and trust in quantum computing. IEEE J. Emerg. Select. Top. Circ. Syst. 11, 2 (2021), 333–342. 10.1109/JETCAS.2021.3077024

[96] Mahmood Azhar Qureshi and Arslan Munir. 2019. PUF-RLA: A PUF-based reliable and lightweight authentication protocol employing binary string shuffling. In Proceedings of the IEEE 37th International Conference on Computer Design (ICCD’19). 10.1109/ICCD46524.2019.00084

[97] Pappu Srinivasa Ravikanth and Stephen A. Benton. 2001. Physical one-way functions. Science 297 (2001), 2026–2030.

[98] J. Roberts, I. E. Bagci, M. A. M. Zawawi, J. Sexton, N. Hultberg, Y. J. Noori, M. P. Young, C. S. Woodhead, M. Missous, M. A. Migliorato, and et al. 2015. Using quantum confinement to uniquely identify devices. Sci. Rep. 5, 1 (2015). 10.1038/srep16456

[99] Garrett S. Rose, Nathan McDonald, Lok-Kwong Yan, and Bryant Wysocki. 2013. A write-time based memristive PUF for hardware security applications. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD’13). 830–833. 10.1109/ICCAD.2013.6691209

[100] Garrett S. Rose, Nathan McDonald, Lok-Kwong Yan, Bryant Wysocki, and Karen Xu. 2013. Foundations of memristor based PUF architectures. In Proceedings of the IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH’13). 52–57. 10.1109/NanoArch.2013.6623044

[101] Ulrich Rührmair, Christian Hilgers, and Sebastian Urban. 2013. Optical PUFs reloaded (unpublished).

[102] Ulrich Rührmair, Jan Sölter, Frank Sehnke, Xiaolin Xu, Ahmed Mahmoud, Vera Stoyanova, Gideon Dror, Jürgen Schmidthuber, Wayne Burleson, and Srinivas Devadas. 2013. PUF modeling attacks on simulated and silicon data. IEEE Trans. Inf. Forens. Secur. 8, 11 (2013), 1876–1891. 10.1109/TIFS.2013.2277978

[103] Kolasan Sahithi and N.S. Murty. 2018. Delay based physical unclonable function for hardware security and trust. In Proceedings of the International Conference on Advances in Communications, Computing and Informatics (ICACCI’18). 797–803. 10.1109/ICACCI.2018.8554739

[104] Durga Prasad Sahoo, Phuong Ha Nguyen, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty. 2015. A case of lightweight PUF constructions: Cryptanalysis and machine learning attacks. IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst. 34, 8 (2015), 1334–1343. 10.1109/TCAD.2015.2448677

[105] Durga Prasad Sahoo, Sayandeep Saha, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, and Hitesh Kapoor. 2014. Composite PUF: A new design paradigm for physically unclonable functions on FPGA. In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST’14). 50–55. 10.1109/HST.2014.6855567

[106] Sriman Sankaran, S. Shiv Shankar, and K. Nimmagadda. 2018. LHPUF: Lightweight hybrid PUF for enhanced security in internet of things. In Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES’18). 275–278. 10.1109/iSES.2018.800866

[107] Krishna Prasad Satamraj and B. Malarkodi. 2020. A PUF-based mutual authentication protocol for internet of things. In Proceedings of the 5th International Conference on Computing, Communication and Security (ICCCS’20). 1–6. 10.1109/ICCCS549678.2020.9276688

[108] Dimitrios Schimianakis. 2019. Lightweight security for the internet of things: A soft introduction to physical unclonable functions. IEEE Potent. 38, 2 (2019), 21–28. 10.1109/MPOT.2018.2849850

[109] Mahdi Shakiba-Herfah, Arsenio Chorti, and H. Vincent Poor. 2021. Physical layer security: Authentication, integrity, and confidentiality. Physical Layer Security, N. Le Khoa (Ed.). Springer International Publishing, Cham. 129–150. https://doi.org/10.1007/978-3-030-55366-1_6
[110] Alireza Shamsoshoara, Ashwija Korenda, Fatemeh Afghah, and Sherali Zeadally. 2020. A survey on physical unclonable function (PUF)-based security solutions for internet of things. Comput. Netw. 183 (2020), 107593. 10.1016/j.comnet.2020.107593

[111] Junye Shi, Yang Lu, and Jiliang Zhang. 2020. Approximation attacks on strong puf s. IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst. 39, 10 (2020), 2138–2151. 10.1109/tcad.2019.2962115

[112] P. W. Shor. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 124–134. 10.1109/SFCS.1994.365700

[113] Boris Skoríć. 2010. Quantum readout of physical unclonable functions. In Progress in Cryptology – AFRICACRYPT 2010, Daniel J. Bernstein and Tanja Lange (Eds.). Springer, Berlin, 369–386.

[114] B. Srinivasu and Anupam Chattopadhyay. 2021. Cycle PUF: A cycle operator based PUF in carbon nanotube FET technology. In Proceedings of the IEEE 21st International Conference on Nanotechnology (NANO’21), 13–16. 10.1109/NANOS1122.2021.9514291

[115] Emanuele Strieter, Christoph Frisch, and Michael Pehl. 2021. Machine learning of physical unclonable functions using helper data. IACR Trans. Cryptogr. Hardw. Embed. Syst. (2021), 1–36. 10.46586/tches.v2021.i2.1-36

[116] Dmitry B. Strukov, Gregory S. Snider, Duncan R. Stewart, and R. Stanley Williams. 2008. The missing memristor found. Nature 453, 7191 (2008), 80–83. 10.1038/nature06932

[117] Y. Su, J. Holleman, and B. Otis. 2007. A 1.6µJ/bit 96% stable chip-ID generating circuit using process variations. In Proceedings of the IEEE International Solid-State Circuits Conference. Digest of Technical Papers. 406–611. 10.1109/ISSCC.2007.375466

[118] G. Edward Suh and Srinivas Devadas. 2007. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th ACM/IEEE Design Automation Conference. 9–14.

[119] R. Sushma and N.S. Murty. 2018. Feedback oriented XOR/d flip-flop based arbiter PUF. In Proceedings of the International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECOT’18). 1444–1448. 10.1109/ICEECOT43722.2018.9001605

[120] Daisuke Suzuki and Koichi Shimizu. 2010. The glitch PUF: A new delay-PUF architecture exploiting glitch shapes. In Proceedings of the Cryptographic Hardware and Embedded Systems (CHES’10), Stefan Mangard and François-Xavier Standaert (Eds.), Springer, Berlin, 366–382.

[121] Shahin Tajik. 2019. On the Physical Security of Physically Unclonable Functions. T-Labs Series in Telecommunication Services. Springer, Berlin. 10.1007/978-3-319-75820-6

[122] Shahin Tajik, Enrico Dietz, Sven Frohmann, Jean-Pierre Seifert, Dmitry Nedospasov, Clemens Helfmeier, Christian Boit, and Helmar Dittrich. 2014. Physical characterization of arbiter PUFs. In Advanced Information Systems Engineering, Lecture Notes in Computer Science, 493–509. 10.1007/978-3-662-44709-3_27

[123] Yuki Tanaka, Song Bian, Masayuki Hiromoto, and Takashi Sato. 2018. Coin flipping PUF: A novel PUF With improved resistance against machine learning attacks. IEEE Trans. Circ. Syst. II: Expr. Briefs 65, 5 (2018), 602–606. 10.1109/TCSII.2018.2821267

[124] Mohammad Tehraniopuro and Farinaz Koushanfar. 2010. A survey of hardware trojan taxonomy and detection. IEEE Des. Test Comput. 27, 1 (2010), 10–25. 10.1109/MDT.2010.7

[125] Johannes Tobisch, Anita Aghia, and Georg T. Becker. 2021. Combining optimization objectives: New modeling attacks on strong puf s. IACR Trans. Cryptogr. Hardw. Embed. Syst. (2021), 357–389. 10.46586/tches.v2021.i2.357-389

[126] Mesbah Uddin, Md Sakib Hasan, and Garrett S. Rose. 2019. On the theoretical analysis of memristor based true random number generator. In Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI’19). Association for Computing Machinery, New York, 21–26. 10.1145/3299874.3317981

[127] Mesbah Uddin, Md Badruddoja Majumder, Karsten Beckmann, Harika Manem, Zahiruddin Alamgir, Nathaniel C. Cady, and Garrett S. Rose. 2017. Design considerations for memristive crossbar physical unclonable functions. J. Emerg. Technol. Comput. Syst. 14, 1, Article 2 (September 2017). 10.1145/3094414

[128] Ulrich R. Uhrmair, Frank Sehnke, Jan S. Olter, Gideon Dror, Srinivas Devadas, and J. Urjen Schmidhuber. 2010. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS’10). 10.1145/1866307.1866335

[129] D. Wang, B. Bai, W. Zhao, and Z. Han. 2019. A survey of optimization approaches for wireless physical layer security. IEEE Commun. Surv. Tutor. 21, 2 (2019), 1878–1911. 10.1109/COMST.2018.2883144

[130] Qian Wang and Gang Qu. 2019. A silicon PUF based entropy pump. IEEE Trans. Depend. Sec. Comput. 16, 3 (2019), 402–414. 10.1109/TDSC.2018.2881695

[131] Wenzxuan Wang, Aijiao Cui, Gang Qu, and Huawei Li. 2018. A low-overhead PUF based on parallel scan design. In Proceedings of the 23rd Asia and South Pacific Design Automation Conference (ASP-DAC’18), 715–720. 10.1109/ASPDAC.2018.8297406

[132] Ziwei Wei, Yijun Cui, Yunpeng Chen, Chenghua Wang, Chongyuan Gu, and Weiqiang Liu. 2020. Transformer PUF: A highly flexible configurable PUF based on FPGA. In Proceedings of the IEEE Workshop on Signal Processing Systems (SiPS’20), 1–6. 10.1109/SiPS05750.2020.9195259

ACM Computing Surveys, Vol. 55, No. 14s, Article 134.Publication date: July 2023.
Physical Unclonable Functions (PUF) for IoT Devices

[133] Benedikt Wigger, Thomas Meissner, Alexander Förste, Volker Jetter, and André Zimmermann. 2018. Using unique surface patterns of injection moulded plastic components as an image based physical unclonable function for secure component identification. Sci. Rep. 8, 1 (2018). 10.1038/s41598-018-22876-6

[134] Nils Wisiol, Christopher Mühl, Niklas Pirmay, Phuong Ha Nguyen, Marian Margraf, Jean-Pierre Seifert, Marten Van Dijk, and Ulrich Rüthemair. 2020. Splitting the interpose puf: A novel modeling attack strategy. IACR Trans. Cryptogr. Hardw. Embed. Syst. (2020), 97–120. 10.46586/tches.v2020.i3.97-120

[135] W. K. Wootters and W. H. Zurek. 1982. A single quantum cannot be cloned. Nature 299, 5886 (1982), 802–803. 10.1038/299802a0

[136] N. Xie, Z. Li, and H. Tan. 2021. A survey of physical-layer authentication in wireless communications. IEEE Commun. Surv. Tuto. 23, 1 (2021), 282–310. 10.1109/COMST.2020.3042188

[137] Wei Yan, Chenglu Jin, Fatemeh Tehranipoor, and John A. Chandy. 2017. Phase calibrated ring oscillator PUF design and implementation on FPGAs. In Proceedings of the 27th International Conference on Field Programmable Logic and Applications (FPL’17), 1–8. 10.23919/FPL.2017.8056859

[138] Venkata P. Yanambaka, Saraju P. Mohanty, and Elias Kougianos. 2016. Novel FinFET based physical unclonable functions for efficient security integration in the IoT. In Proceedings of the IEEE International Symposium on Nanoelectronic and Information Systems (iNIS’16). 172–177. 10.1109/iNIS.2016.047

[139] Liang Yao, Huaguo Liang, Zhengfeng Huang, Cuiyun Jiang, Maoxiang Yi, and Yingchun Lu. 2021. A lightweight configurable XOR RO-PUF design based on xilinx FPGA. In Proceedings of the IEEE 4th International Conference on Electronics Technology (ICET’21), 83–88.

[140] Amin A. Zayed, Hanady H. Issa, and Khaled A. Shehata. 2019. FinFET based low power ring oscillator physical unclonable functions. In Proceedings of the 31st International Conference on Microelectronics (ICM’19). 227–230. 10.1109/ICM48031.2019.9021283

[141] Jiliang Zhang, Lin Ding, Zhuojuan Chen, Wenshang Li, and Gang Qu. 2022. Da puf. In Proceedings of the 59th ACM/IEEE Design Automation Conference. 10.1145/3489517.3530412

[142] Jiliang Zhang and Gang Qu. 2020. Physical unclonable function-based key sharing via machine learning for IoT security. IEEE Trans. Industr. Electr. 67, 8 (2020), 7025–7033. 10.1109/TIE.2019.2938462

[143] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo. 2019. Physical layer security for the internet of things: Authentication and key generation. IEEE Wireless Commun. 26, 5 (2019), 92−98. 10.1109/MWC.2019.1800455

[144] Jiliang Zhang and Chaqun Shen. 2021. Set-based obfuscation for strong puf against machine learning attacks. IEEE Trans. Circ. Syst. I: Regul. Pap. 68, 1 (2021), 288–300. 10.1109/tcisi.2020.3028508

[145] Jiliang Zhang, Chaqun Shen, Haihan Su, Md Tanvir Arafain, and Gang Qu. 2022. Voltage over-scaling-based lightweight authentication for IoT security. IEEE Trans. Comput. 71, 2 (2022), 323–336. 10.1109/tc.2021.3049543

[146] Ji-Liang Zhang, Gang Qu, Yong-Qiang Lv, and Qiang Zhou. 2014. A survey on silicon PUFs and recent advances in ring oscillator PUFs. J. Comput. Sci. Technol. 29, 4 (2014), 664–678. 10.1007/s11390-014-1458-1

[147] Yin Zhang, Zhangqing He, Meilin Wan, Jiuyang Liu, Haoshuang Gu, and Xuecheng Zou. 2021. A SC PUF standard cell used for key generation and anti-invasive-attack protection. IEEE Trans. Inf. Forens. Secur. 16 (2021), 3958–3973. 10.1109/TIFS.2021.3089854

[148] Ting Zhou, Yuxin Ji, Mingyi Chen, and Yongfu Li. 2020. PL-MRO PUF: High speed pseudo-LFSR PUF based on multiple ring oscillators. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS’20), 1–5. 10.1109/ISCAS45731.2020.9180582

[149] Haoyu Zhuang, Xiaodan Xi, Nan Sun, and Michael Orshansky. 2020. A strong subthreshold current array PUF resilient to machine learning attacks. IEEE Trans. Circ. Syst. I: Regul. Pap. 67, 1 (2020), 135–144. 10.1109/TCSI.2019.2945247

[150] Yu Zhuang, Khalid T. Mursi, and Li Gaoxiang. 2021. A challenge obfuscating interface for arbiter PUF variants against machine learning attacks. arxiv:2103.12935 [cs.CR]. Retrieved from https://arxiv.org/abs/2102.13935.

Received 30 January 2022; revised 6 February 2023; accepted 2 April 2023