International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I5P102

Volume 72 Issue 5, 16-25, May 2024


*Original Article*

# Blockchain-Enabled Key Generation Using Physical Unclonable Function for IoT Security

Houda Lhore[1*], Assia El-Hadbi[1], Kaouthar Bousselam[1], Oussama Elissati[1], Mouhcine Chami[1]

[1]*National Institute of Posts and Telecommunications, STRS Lab., Rabat, Morocco.*

[*]*Corresponding Author: lhore.houda@gmail.com*

Received: 28 November 2023 Revised: 30 March 2024 Accepted: 01 April 2024 Published: 26 May 2024

***Abstract*** *- The security issue is receiving a lot of interest from researchers and providers due to the ubiquitous nature of the Internet of Things (IoT) in many different domains. The Internet of Things is a centralized system with significant limitations, including low memory capacity and limited processing power. As a result, this restriction prevents the use of conventional security methods to shield devices from identity theft and enable safe data transfer over the Internet of Things. Therefore, a new scheme is proposed to provide the security mechanism. To cover this issue, Blockchain technology is adopted in this approach to define a decentralized Internet of Things system which offers security features like transparency, tractability, etc., and where IoT is identified by assigning a unique identity and key generation application through the use of use of a hardware security primitive called a Physical Unclonable Function. This paper offers a Blockchain-enabling key generation via Physical, Unclonable Function.*

***Keywords*** *- Internet of Things, Physical Unclonable Function, Blockchain Technology, SRAM PUF, Integrity, Security.*

## 1. Introduction

The Internet of Things represents the new frontier of devices that enables us to explore new services and take advantage of various functions without intermediate assistance. As a result of this breakthrough, the network is now exchanging enormous volumes of data, for which security needs to be guaranteed. Since conventional security systems such as communication encryption, authorization, and authentication are incompatible and more challenging with these devices, security issues are evidently the most difficult parameter to ensure.

In reality, the Internet of Things represents a centralized network that is generally considered a third party, such as a server or Certificate Authority, which ensures its authentication. This decentralized scheme presents many vulnerabilities, such as a Single Point of Failure (SPF), bottlenecks in the network, and a lack of scalability [1]. Meanwhile, Blockchain technology, originally introduced in the financial domain, provides insights into other domains like the Internet of Things. Blockchain, based on a peer-to-peer network, represents a decentralized system with high-security performance [2].

Thanks to its structure and concept, Blockchain technology has many features, including ensuring transparency, fault tolerance, non-repudiation, traceability, and immutability of data. As detailed in [3], the incorporation of Blockchain technology, as a promising alternative to overcome the security concerns of the Internet of Things, combined with a hardware security primitive, has been proposed. As primary objective is to establish a global system that provides and ensures data security from the low layer "Physical layer" to the upper layer "Application layer." This hardware security primitive is well-known as a Physical Unclonable Function (PUF).

The Physical Unclonable Function is an effective solution for ensuring each device's identity and authentication, as well as securing data exchange between devices in the Internet of Things system. PUF can also be used for the key generation in Blockchain technology. In this work, a PUF-based Key Generation is proposed using the Blockchain protocol for IoT Security. The following is how the paper is structured:

Section 2 gives an outline of the Physical Unclonable Function, its concepts, features, and classification. Section 3 presents a proposed scheme for authentication based on the PUF. Section 4 covers the experimental evaluation, and Section 5 paper conclusion.

## 2. Physical Unclonable Function

### *2.1. PUF Concepts*

The Physical Unclonable Function serves as a security hardware primitive, generating a unique response commonly referred to as a digital fingerprint. This response remains

constant for a specific input, forming the Challenge-Response Pair (CRP) that characterizes the PUF's operation. The PUF leverages the inherent variations in the manufacturing process of integrated circuits, utilizing these arbitrary manufacturing variations.

Originally developed with a focus on ensuring a physical one-way function [4], PUF circuits later evolved into key generation functions within the realm of security. They also function as hardware accelerators, enabling the rapid execution of specific operations using specialized hardware.

In the literature, the PUF is described as a security hardware primitive that dynamically generates a unique response akin to a digital fingerprint. This functionality is integrated into the hardware, utilizing the electronic disorder of components. For a designated challenge input, the PUF consistently produces the same output, forming the CRP.

The responses generated by the PUF are renowned for their unpredictability, uniqueness, and non-reproducible nature due to the inherent variations and disorders introduced during the manufacturing process of each integrated circuit. Factors such as differing threshold voltages, doping concentrations, and oxide thickness contribute to the distinctiveness of each circuit's response, rendering it impossible to duplicate.

These responses are dynamically generated at runtime, eliminating the need to store response keys in memory. This approach diverges from conventional methods that require the storage of predetermined keys, thereby enhancing security by capitalizing on the unique attributes of each hardware component. The PUF, by creating a distinctive fingerprint through entropy derived from manufacturing process variations, provides a robust and secure solution for cryptographic applications.

### *2.2. Properties of PUF*

Two fundamental properties consistently emerge from various PUF definitions in the literature: unclonability and unpredictability. Unclonability arises from the inherent difficulty and near impossibility of replicating the same variations during the fabrication processes of each component. On the other hand, unpredictability stems from the challenge an attacker faces in predicting the behavior of a PUF and discerning its responses.

Moreover, additional research, such as [4, 5], outlines several properties that different PUF structures should exhibit. These features are described as follows:

#### *2.2.1. Unique*

Each PUF possesses distinct responses derived from its specific physical variations, setting it apart from others. Therefore, a collection of challenge-response pairs serves as a unique identity for each PUF.

#### *2.2.2. Evaluable or Low Cost*

This signifies that a PUF is simple to construct with an affordable price, often utilizing conventional hardware. The evaluable aspect also implies that PUF responses are easy to generate.

#### *2.2.3. Reproducible or Steady*

This feature ensures that a PUF provides the same response when subjected to the same challenge, even in varying environmental conditions. The reproducibility of responses distinguishes PUFs from True Random Number Generators (TRNGs).

#### *2.2.4. Secure*

PUFs are considered mathematically unclonable, making it challenging to create software or mathematical functions that generate every challenge-response pair combination.

They function as one-way functions, making it difficult to deduce the challenge used for the operation while knowing the response. Additionally, PUFs are tamper-evident, with any physical alteration resulting in errors and different responses from the original.

### *2.3. PUF Applications*

The Physical Unclonable Function is employed to address security issues, with three primary application types commonly utilized. The most frequent applications are as follows:

#### *2.3.1. Identification System*

Physical Unclonable Functions can serve as a system identification, enhancing anti-counterfeiting technologies by providing inherent or assigned identity. For example, integrating PUFs with Radio Frequency Identification Tags (RFID tags) prevents physical cloning and replay attacks, ensuring the security of unique identifiers. The integration of PUFs into anti-counterfeiting tags is crucial for leveraging their unclonable and unpredictable response characteristics, as discussed in various studies [6, 7, 8, 9].

#### *2.3.2. Authentication System*

The authentication system is a mechanism that enables the identification of a party and confirmation of its authenticity. In addition to assigning an identity to a device, the Physical Unclonable Function can be utilized to authenticate hardware systems. Its capability to generate a unique response facilitates the detection of compromised entities.

Authentication involves two entities: client authentication (prover) and server authentication (verifier), both relying on the challenge-response pair. A PUF-based authentication system and authentication protocols deploying the challenge-response pair to verify the entity's authentication have been proposed in [10, 11, 12].

*2.3.3. Key Generation Application*

In the domain of cryptography, the secure generation, storage, and retrieval of keys are crucial. The Physical Unclonable Function becomes a promising solution for key generation applications, providing a PUF response with high entropy necessary in cryptographic systems and unclonability against attackers. Moreover, since the PUF can supply the key whenever needed, there is no need to store it in memory. The Physical Unclonable Function is considered a promising solution for key generation applications due to its ability to meet these requirements [13].

### *2.4. PUF Metric Evaluation*

Several metrics are employed to facilitate the comparative analysis of different PUFs architectures. These metrics allow for the assessment of PUF performance in accordance with established standards commonly used for authentication protocols. Specifically, the CRP must ensure minimally some specific metrics such as Uniqueness, Randomness and Uniformity, Reliability, and Bit-Aliasing [5] [14, 15] [16].

*2.4.1. Uniqueness*

This comparative metric serves as the primary parameter, based on inherent randomness, facilitating the distinction between individual PUFs. It is contingent upon the PUF's ability to generate responses that are both unique and independent. Thereby, it quantifies the process and mismatch variations of the PUF circuit. Specifically, when considering a given PUF circuit implementation on different devices, this metric quantifies the average differentiation of their responses to the same designated challenge input under the same test conditions. Typically, for each possible response pair $(R_i, R_j)$, where $R_i$ (resp. $R_j$) is the $i_{th}$ (resp. $j_{th}$) response of $i_{th}$ (resp. $j_{th}$)) PUF, the differentiation of response can be quantified using the inter-class Hamming Distance function, as follows:

$$HD(R_i, R_j) = \sum_{k=1}^{n} R_{i,k} \oplus R_{j,k} \quad (1)$$

Where $n$ denotes the number of response bits, therefore, uniqueness is represented as the average value of the sum of the Hamming Distance across all potential response pairs. This parameter is defined by the hamming inter-distance as defined in (2):

$$U = HD_{inter}(R_i, R_j) = \frac{2}{m(m-1)} \sum_{i=0}^{m-1} \sum_{j=i+1}^{m} \frac{HD(R_i, R_j)}{n} \quad (2)$$

Where $m$ is the number of tested PUF devices.

Ensuring the unpredictability of each fingerprint necessitates obtaining divergent responses constantly when applying the same challenge. Consequently, the optimal value that can be obtained for (2) should be 50%. This value implies that the responses of any two PUF devices subjected to the same challenge should differ by half the number of bits ($n/2$ ).

*2.4.2. Randomness & Uniformity*

Randomness of a PUF key is the measure of the balance between the number of zeros and ones in the PUF response bits. Otherwise, it quantifies the statistical entropy of the n-bit key. Randomness and uniformity are nearly similar. However, the difference lies in randomness being an average of uniformity over repetitive measurements for each generated key [14, 15].

The security of a PUF device is contingent upon the PUF-generated key exhibiting an equal percentage of random zeros and ones, thereby maximizing the entropy. This characteristic is crucial for withstanding brute force and other key guessing attacks. Ideally, the uniformity of the ideal PUF should be 50%, reflecting an equal distribution of zeroes and ones for optimal performance. Consequently, a true random PUF output is obtained for this type of PUF. Generally, the evaluation of the uniformity parameter for a specific key, the response $R_i = (b_{i,1}, \ldots, b_{i,n})$, based on the hamming weight of this key, is as follows:

$$Uniformity_i = \frac{1}{n} \sum_{j=1}^{n} b_{i,j} \times 100\% \quad (3)$$

*2.4.3. Reliability*

The ability of a PUF to consistently produce exactly the same key under different test conditions, such as temperature or voltage variations, is referred to as PUF Reliability. It reaches a value of 100% if the PUF generates an identical response regardless of changes in environmental conditions. To assess this metric, a preliminary response $R_{ref}$ of the PUF under normal conditions is examined. Subsequently, the intra-Hamming distance between $R_{ref}$ and the PUF response $R_i$ underworking environmental conditions, tests are calculated. The formula for the intra-Hamming distance, denoted as $HD_{intra}$, is given by (4), which is computed for all possible PUF responses. It is noteworthy that this quantity also represents the Bit-Error-Rate (BER), which is another crucial metric commonly employed in PUF evaluation.

$$HD_{intra} = \frac{1}{m} \sum_{i=1}^{m} \frac{HD(R_i, R_{ref})}{n} \quad (4)$$

Finally, the Reliability value, expressed as a percentage under specific working environmental conditions, is defined as:

$$Reliability = (1 - HD_{intra}) \times 100 \quad (5)$$

*2.4.4. Bit-Aliasing*

The process variation of the PUF device can lead to the fixed preferred value of some response bits, even when achieving optimal bit Uniformity. Consequently, the uniformity metric becomes not enough to estimate the PUF randomness. In such cases, as certain response bits exhibit static variations from one response to another, they may introduce vulnerabilities by enabling attackers to estimate the generated key.

**Table 1. Classification of PUFs**

| PUF Name | Measurement Process | Randomness Source | Intrinsic Evaluation | Reputation | Ref. |
|---|---|---|---|---|---|
| SRAM PUF | Fully Electronic | Implicit | Intrinsic | Weak | [17] |
| Ring Oscillator PUF | | | | | [18] |
| Arbiter PUF | | | | Strong | [19] |
| Acoustical PUF | | Explicit | Extrinsic | | [20] |
| Magnetic PUF | Non-electronics | Implicit | | | [21] |
| Optical PUF | | Explicit | | | [22] |
| RF PUF | | | | | [23] |

To address this concern is the purpose, the Bit-Aliasing of the $l^{th}$ bit in the PUF identifier for the $k^{th}$ response expressed as a percentage of the Hamming weight of the $l^{th}$ bit of the identifier across $m$ devices, as defined by (6).

$$Bit_{Aliasing}(k,l) = \frac{1}{m}\sum_{i=1}^{m} b_{k,l,i} \times 100 \qquad (6)$$

Ideally, the value of the Bit-Aliasing is 50%. Deviation from this value indicates bias in some bits, thereby affecting the security of the PUF.

### *2.5. Type/Classification of PUFs*

In the state of the art, PUFs can be classified as *intrinsic* PUF or *extrinsic* PUF, according to the randomness of the PUF source. Regarding this source it can be Implicit or Explicit. Otherwise, PUFs can be classified according to the used technology. They can be *electronic*, which takes advantage of the random variation of electronic materials to generate the PUF response, such as radio-frequency-based PUFs and silicon PUFs (commonly used and embedded on a silicon chip), or *hybrid*-based on non-electronic technology, such as optical PUFs. Furthermore, PUFs can be classified according to their security reputation and strengths (Weak or strong).

#### *2.5.1. Electronic and Non-Electronic Nature*

The PUF devices can be designed using different technologies and materials, such as electronic, optical, magnetic, and chemical components. Thus, two types of PUFs can be defined based on technology:

*Electronic*

PUFs based on electronics have the possibility to gain random variation from their electronic construction, such as transistors, capacitance, and resistance, to evaluate the PUF response. In the literature, a subclass of electronics named Silicon PUF is considered electronic PUF. The first structure of PUF based on silicon is introduced in [24]. The silicon equipment gives the ability to be integrated as an additional block in the same chip.

*Non-Electronic*

It defines all PUFs that are constructed from non-electronic materials and technology. For this kind of PUF, the origin of the randomization depends on non-electronic material; for example, the Optical PUF is based on the fabrication variations at the molecular level [25].

#### *2.5.2. Intrinsic and Extrinsic PUFs*

*Intrinsic*

The intrinsic PUF is an entity that derives its random sources from its construction features, as introduced in [27]. It is defined as a generated circuit situated within a device, requiring no supplementary measures for security enhancement. PUFs are considered intrinsic when their construction fulfills two criteria:

- The generation of PUF responses must occur internally, using embedded equipment.
- They must exclusively leverage implicit randomness arising from variations during the fabrication process [4].

*Extrinsic/Non-intrinsic*

Extrinsic PUF, also called non-intrinsic PUF, is the opposite of intrinsic PUF. Its evaluation is done externally, as in the case of optical PUF. Optical PUF has random properties introduced by applying an external source to the PUF to produce the variation and generate the responses (observation of the speckle pattern) [5] [23] [27].

#### *2.5.3. Implicit and Explicit Randomness*

According to the source randomness of a PUF device, which is mainly based on this randomness variation, two types are defined: Implicit and explicit randomness. The first one is deduced from its entity (embedded instance), and the second one requires an additional process for the PUF instance to get the randomization.

This latter needs more time than an implicit one to generate a response. This variation can occur in different parameters, such as dopant concentration, oxide thickness, and effective channel. Obviously, the implicit variation is more suitable than the explicit variation. In fact, direct manipulation of this implicit variant is not possible. Thus, even the manufacturer cannot tamper with the device in the fabrication process in a manner to modify the PUF's random properties.

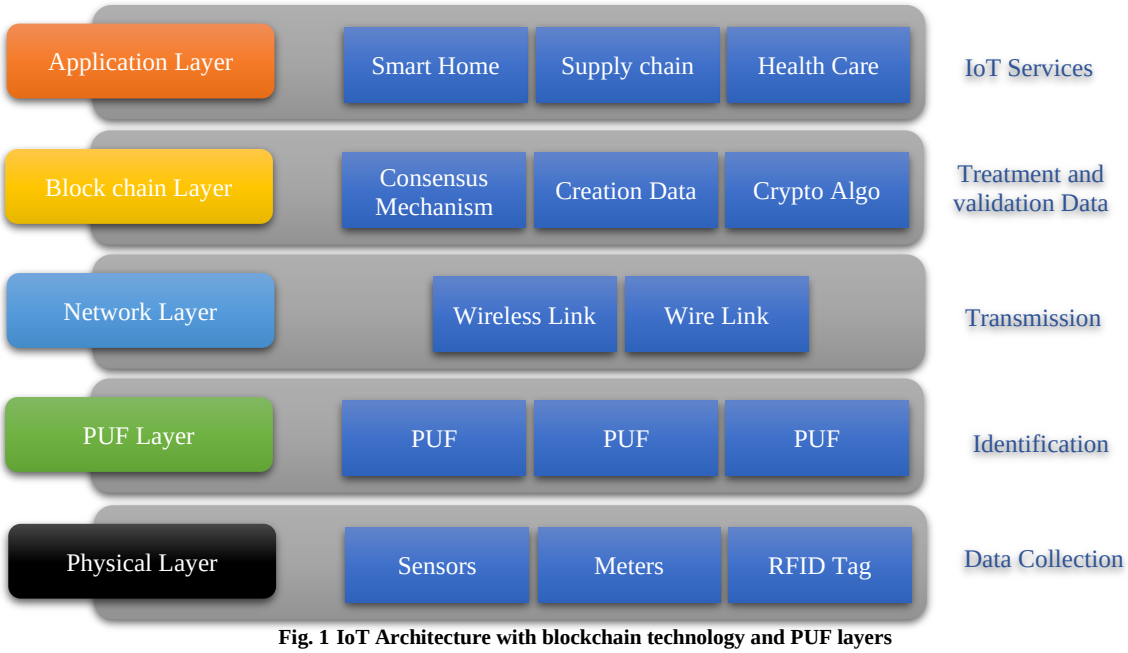


**Fig. 1 IoT Architecture with blockchain technology and PUF layers**

*2.5.4. PUF Reputation (Weak/Strong)*

The security strength and reputation of the PUF are determined by the number of challenge-response pairs generated by the PUF. Thus, this is consistent with the way that the growing size of the device is proportionate to the number of Challenge Response Pairs (CRPs). This percentage scaling is usually the primary metric that characterizes the strength of a PUF. Therefore, two categories, weak and strong PUFs, are defined [5].

*Weak PUF*

Weak PUF is characterized by a small number of CRPs, represented with a linear function of PUF size. Generally,-this category is used in secret Key generation applications. Thus, the response must remain consistent and resilient to the environmental variations and multiple readings, which have to ensure that a challenge consistently produces the same response. Otherwise, to preserve CRP confidentiality, PUF requires an additional block of security.

*Strong PUF*

Strong PUF is recognized for its large number of CRPs and its exponential variation with its size. With the huge number of responses and for a short time, the attacker will face difficulty in guessing the corresponding CRP. Furthermore, when a random selection of these CRPs is gathered during the manufacturing stage, the attacker has no capacity probability to store the response of a specified challenge. It becomes almost negligible how likely it is that the attacker has stored the challenge with his answer. This creates a system where only the person physically present at the PUF during the challenge may offer the right answer and progress through authentication despite the fact that the attacker has previously reached the PUF. Consequently, each CRP may be employed once. This step leads to countering eavesdropping attacks. Therefore, this kind of PUF is used in authentication applications. Table 1 summarizes the most commonly used Physical Unclonable Functions (PUFs) in research, with a focus on SRAM PUFs known for their reliability. The SRAM PUFs are centered on the power-up state of SRAM blocks. When an SRAM PUF powers up, each cell can start with a value of either “0” or “1.” This unique starting state becomes a distinct identifier for each device, making it different from others.

In simple terms, the challenge is like the address of an SRAM cell, and its starting value becomes the SRAM PUF response. Importantly, implementing SRAM PUFs on microcontrollers and devices is easy [28].

## 3. The Proposed PUF-Enabled Blockchain Scheme for IoT

### *3.1. The Global Proposed Architecture for IoT Security*

Blockchain technology is a chain of blocks that form a decentralized, immutable, transparent, and non-repudiable ledger of information shared between peers without any intermediate entities. Therefore, Blockchain technology has gained considerable attention from researchers to be deployed into the Internet of Things network to address security concerns.

As described in various research studies, the use of Blockchain technology has increased accuracy in tracking items, identifying fakes [29, 30], and confirming data [31], which can be accomplished in complex supply chains. In addition, smart contracts, consensus mechanisms, and related concepts offer an appealing approach to handling issues related to IoT security [32].

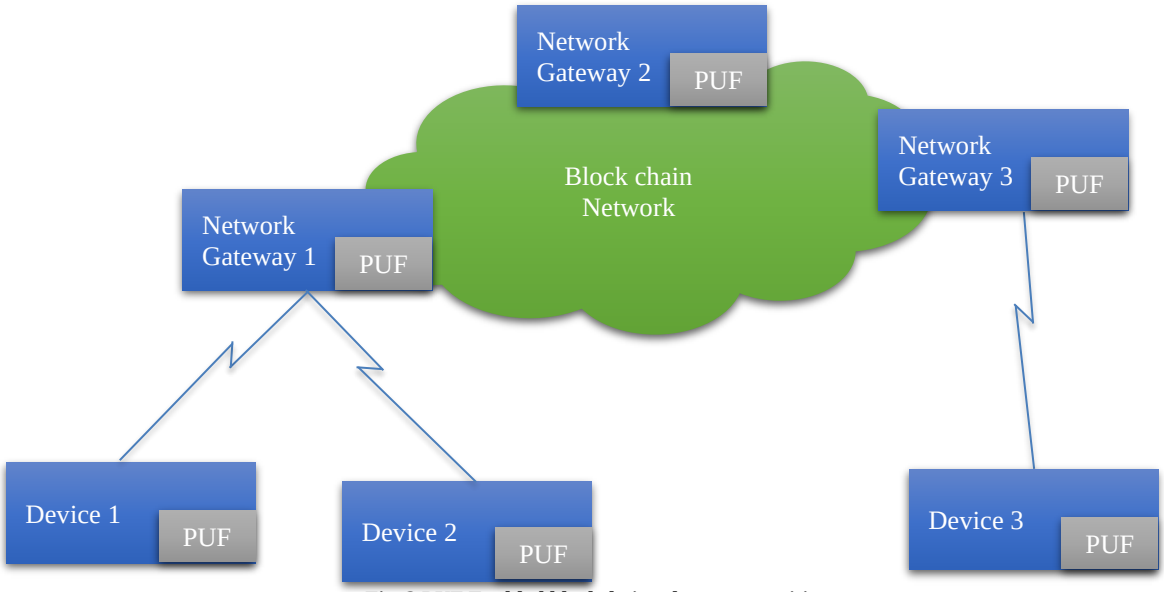


**Fig. 2 PUF Enabled blockchain scheme proposition**

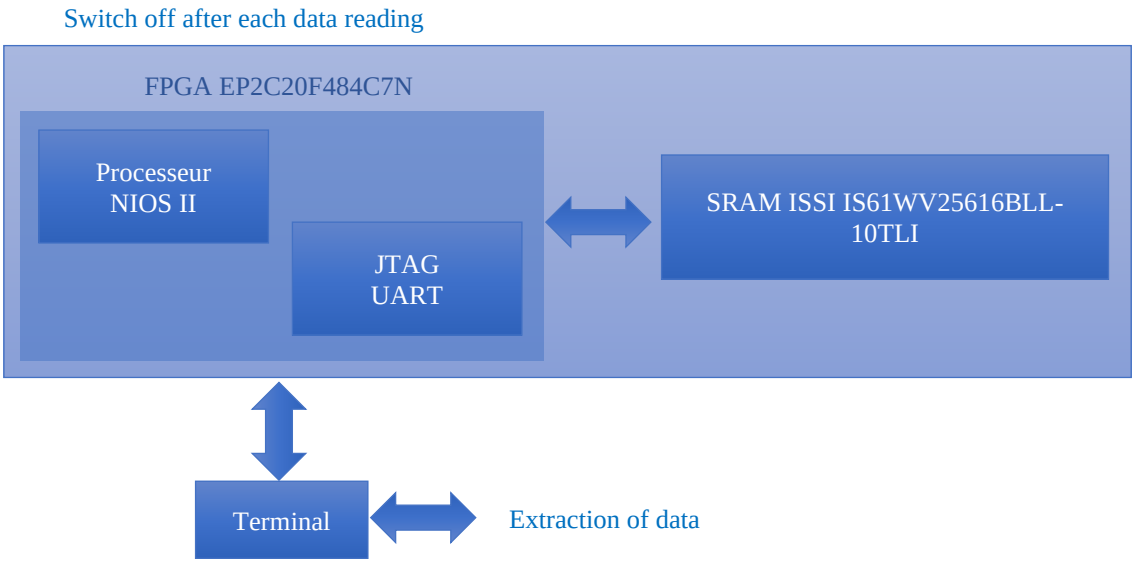


**Fig. 3 Architecture of the PUF-based SRAM measurement system using the FPGA.**

A global architecture has been proposed in [3] based on the basic architecture of the Internet of Things. This latter is mainly consisting of three layers: application layer, network layer, and physical layer. To ensure the security of data exchange within the Internet of Things, a new architecture, depicted in Figure 1, is proposed in this paper. It comprises two extra layers, in addition to the three ordinary layers, which are described as follows:

*3.1.1. Blockchain Layer*

Located between the network and application layers, this layer is deployed via an overlay network technique that creates a virtual network and broadcasts the block between nodes for validation. The Blockchain layer has the role of creating the block, applying the consensus mechanism, and broadcasting information for validation. While Blockchain uses distributed protocols (consensus mechanism), cryptography, and privacy-enabling methods (like threshold-signature schemes) to govern information visibility and trust in different parts of the network, it cannot ensure the uniqueness of physical devices even if they are following a product life cycle [33].

Additionally, there are other obstacles to overcome in the IoT ecosystem when integrating Blockchain technology, such as processing power, latency, scalability, cost, required time for encryption, and storage capacity. Therefore, a new layer is added, named the PUF layer, as a hardware solution to solve some of those problems.

*3.1.2. PUF Layer*

It is the layer positioned among the physical layer and the network layer; this layer has the primary objective of reinforcing the security of the entire system from low to high layers. Hence, the hardware primitive assures a unique identity for the devices and guarantees authentication in the network [34]. Besides, the PUF has the capacity to generate responses dynamically, as explained in the PUFs section, without needing memory to hold the value.

Thus, the proposed architecture can be used for key generation applications by exploiting the PUF responses as derived keys. This technology replaces the conventional method, which extracts a random value from the TRNGs and uses memory for data storage. In such a case, the memory requires an extra block for the security.

### *3.2. PUF-Enabled Blockchain Scheme*

An example of the PUF-enabled Blockchain scheme is depicted in Figure 2. In this architecture, a network Blockchain is implemented between a network of gateways. These gateways are considered mining node that guarantees the verification and adds a block to the Blockchain. In addition to that, since the SRAM is largely present in any electronic device, each gateway is supposed to be equipped with its own PUF in order to perform a cryptographic function, such as a key generation. Furthermore, for each device, it assigns a unique Physical Unclonable Function. These devices are subsequently connected to network gateways.

## 4. Implementation and Experimental Results

### *4.1. Experimental Evaluation of SRAM PUF*

This paper presumes the use of an electronic PUF (intrinsic) like SRAM PUF integrated into the FPGA as a Physical Unclonable Function in the proposed architecture. In order to validate the SRAM PUF, the PUF metrics described in Section 2.4 have been evaluated. The inter-distance and the intra-distance of hamming are used, respectively, to demonstrate the uniqueness and Reliability of SRAM PUF responses.

Figure 3 presents an overview of the system measurement architecture based on the FPGA to extract the answers for evaluation. Hexadecimal data is typically taken from SRAM. Thus, the initial step is to convert those responses to a bit's string responses using a Python program. Figure 4 presents a histogram of the Inter-distance of Hamming of two different PUF responses as a normal distribution. The outcome is an average of 50.33% in inter-distance. This value represents the dissimilarity between the two responses, which means that each SRAM PUF produces a unique response. The second metric to evaluate is the reliability. Therefore, using the same challenge, the intra-distance hamming is computed within two responses of the same PUF. Figure 5 represents a histogram with an average value of 9,89%. As a conclusion, the SRAM PUF is reproducible.

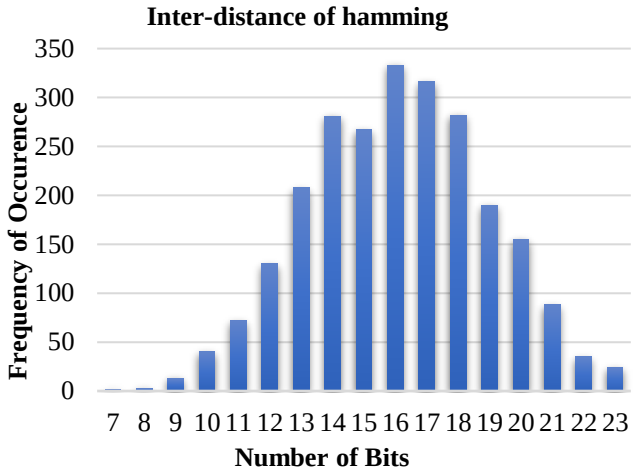


**Fig. 4 Inter-Distance of hamming of a PUF**

As defined in Section 2.5, the reliability is equal to 90.10%, which confirms that the SRAM PUF can reproduce the same response each time we need it. As a conclusion from this experimental measurement, the SRAM PUF integrated into the FPGA can be used as a proposed solution in the context of identification applications and key generation cryptography.

Thus, in the section below it will consider this PUF structure as a hardware security primitive that ensures the security of the proposed architecture in Figure 1.

### *4.2. Blockchain Protocol*

In this scheme, the Blockchain network is established between network gateways, which are designated as mining nodes. In order to access the network Blockchain, the IoT needs to establish communication and authenticate itself through the network gateway, which can confirm the IoT's identity. The enrollment phase and the authentication phase are the two sections of this communication.

*4.2.1. Enrollment Phase*

This phase aims to collect the challenge-response pairs of each device in addition to his identity before going through the authentication phase. This information is stored in a database < CRP, ID>. This operation is executed in a trusted and secure environment.

Figure 6 shows the steps of this enrollment phase, which can be described as follows:

- The network gateway chooses a random Challenge C for the device.
- The device returns to the gateway node a response R after applying the challenge C to its PUF and the Mac address <C, R, MAC>.
- The gateway network appends <C, R, MAC> to a database, storing the response and the challenge together. This process is carried out as needed to list the necessary CRPs (For example, n times).

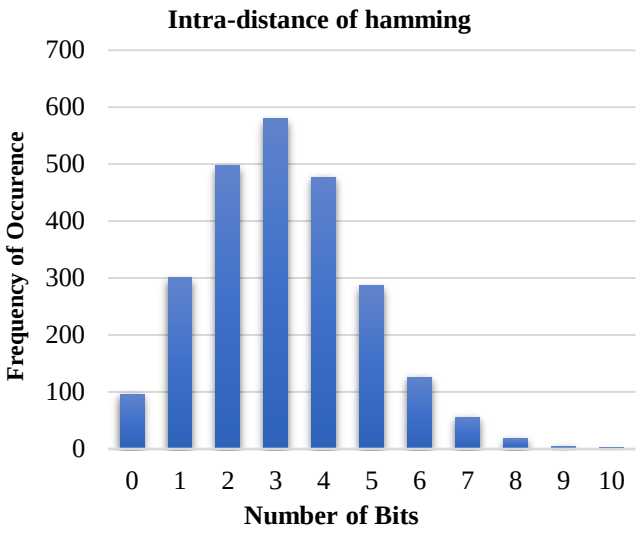


**Fig. 5 Intra-Distance of hamming of two PUF**

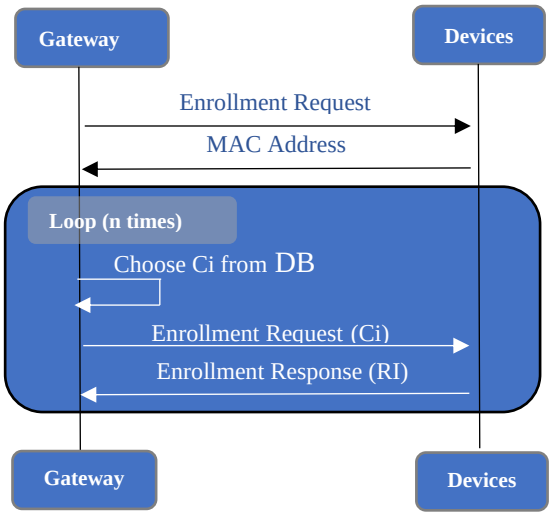


**Fig. 6 The enrollment Phase**

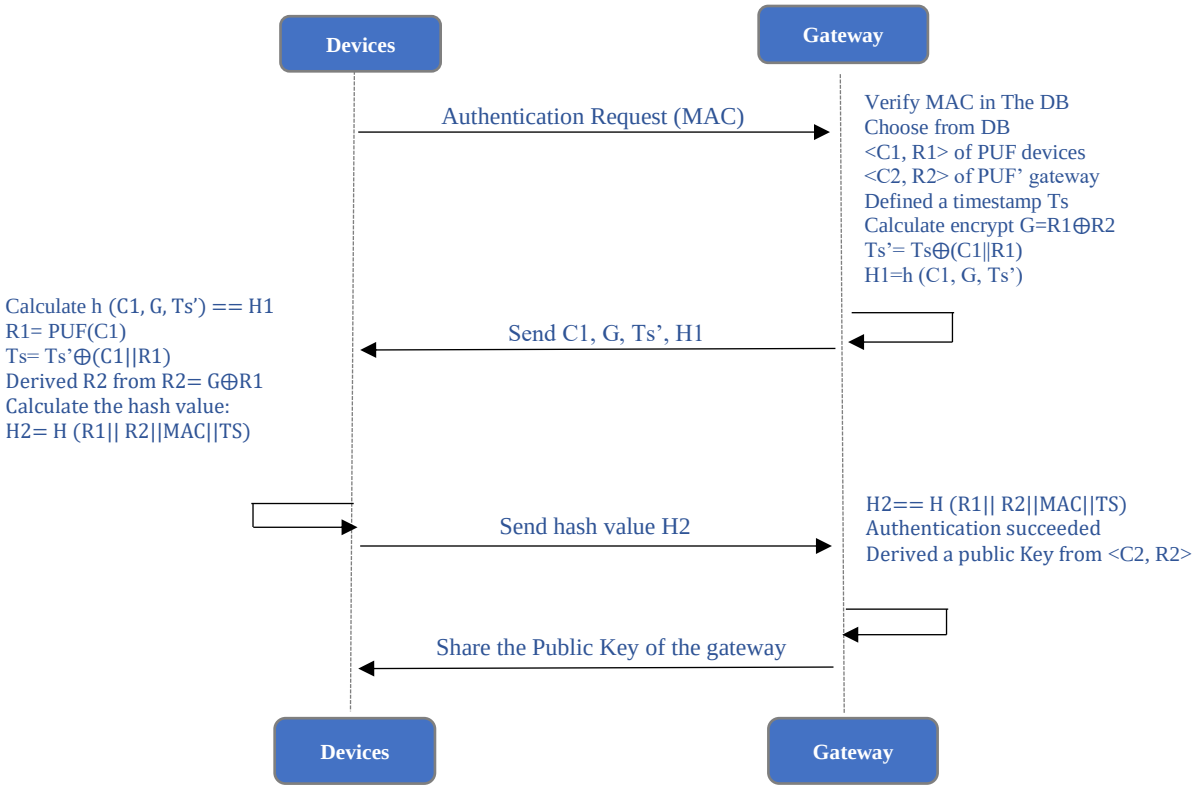


**Fig. 7 The Authentication phase**

*Authentication Phase*

In the authentication phase, as depicted in Figure 7. The IoT device sends an authentication request to the network gateway with its MAC address. The gateway checks if this address MAC is in the database. If it is fine, the gateway generates a timestamp Ts and also selects from the database a challenge C1 and its response R1 of the PUF device. It assumes that the gateway has its own PUF instance so that C2 and R2 represent its own PUF CRP. Based on these parameters, the gateway will send an encryption parameter G, C1, a new value of Ts', and a Hash value H1 that will ensure the integrity of the sent messages to the connected devices. On the other hand, the devices verify the integrity of the received message from the gateway by calculating the hash value based on C1, G, and Ts' and comparing it to H1. After verifying the H1, the device starts to compute a hash value H2 using this parameter R1, R2, Ts, and MAC address H2 = H(R1||R2|MAC||TS) after retrieving R1, R2 and Ts from data sent. Then, H2 is communicated to the gateway for comparison.

If H2== H(R1||R2|MAC||TS), the gateway will derive a public and private key from R2. Thus, the public Key will be shared with the IoT devices to send the messages. At this point, the authentication of the devices is considered successful. Notice that each use of a challenge-response pair must be discarded from the database to secure the system from a replay attack.

*Security Analysis*

This scheme will be evaluated by using an Ethereum testnet network to deploy the Blockchain network. Then, for the network gateway, a Raspberry Pi is used with a configuration as a node. Finally, the FPGA board represents the IoT devices. The Raspberry Pi and the FPGA will exploit the integrated SRAM as a Physical Unclonable Function.The proposed scheme offers a variety of security mechanisms against certain attacks.

The use of Physically Unclonable Functions as a unique identity for IoT prevents the system from falling victim to identity forgery attacks. As explained in the PUF section, it is impossible to absolutely get two identical PUFs. During each authentication process, the gateway selects a different Challenge-Response Pair, effectively thwarting cookie-hijacking attacks [35].

Furthermore, this scheme prevents replay attacks [26] by incorporating timestamp registration and regularly discarding CRPs from the database after being used during a transaction. The system also guards against eavesdropping attacks, as any data alterations aim to prevent device authentication.

## 5. Conclusion

In this paper, a new architecture of the Internet of Things is proposed. It reinforces security by adding two extra layers to the conventional IoT architecture. In fact, a Blockchain-based key generation using the Physical Unclonable Function for Internet of Things security through a proposed protocol of authentication is presented. This scheme establishes secure communication that guarantees the identification and authentication of the devices in the network and the exchange of data in a secure manner. Furthermore, this approach gives resistance against multiple attacks, such as replay attacks, hijacking attacks, etc. This work presents a proof of concept that will be implemented in a hardware device as a perspective in future work for more perception of this advantage.

## References


[1] Elham A. Shammar, Ammar T. Zahary, and Asma A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114-156150, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Fatemeh Tehranipoor et al., "DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1085-1097, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] H. Shelton Jacinto, A. Matthew Smith, and Nader I. Rafla, "Utilizing a Fully Optical and Reconfigurable PUF as a Quantum Authentication Mechanism," *OSA Continuum*, vol. 4, no. 2, pp. 739-747, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Roel Maes, and Ingrid Verbauwhede, *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*, Towards Hardware-Intrinsic Security, Information Security and Cryptography, Springer, Berlin, Heidelberg, pp. 3-37, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[5] Thomas McGrath et al., "A PUF Taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, pp. 1-26, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Dan Jiang, and Cheun Ngen Chong, "Anti-Counterfeiting Using Phosphor PUF," *2008 2nd International Conference on Anti-counterfeiting, Security and Identification*, Guiyang, China, pp. 59-62, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[7] Srinivas Devadas et al., "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," *2008 IEEE International Conference on RFID*, Las Vegas, NV, USA, pp. 58-64, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[8] Pim Tuyls, and Lejla Batina, "RFID-Tags for Anti-Counterfeiting," *Conference Paper, Topics in Cryptology – CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006*, San Jose, CA, USA, vol. 3860, pp. 115-131, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[9] Riikka Arppe, and Thomas Just Sørensen, "Physical Unclonable Functions Generated through Chemical Methods for Anti-Counterfeiting," *Nature Reviews Chemistry*, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] An Braeken, "PUF Based Authentication Protocol for IoT," *Symmetry*, vol. 10, no. 8, pp. 1-15, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Keith B. Frikken, Marina Blanton, and Mikhail J. Atallah, "Robust Authentication Using Physically Unclonable Functions," *Information Security, 12th International Conference, ISC 2009 Pisa*, Italy, vol. 5735, pp. 262-277, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[12] Amanda C. Davi Resende, Karina Mochetti, and Diego F. Aranha, "PUF-Based Mutual Multifactor Entity and Transaction Authentication for Secure Banking," *Lightweight Cryptography for Security and Privacy, 4th International Workshop, LightSec 2015*, Bochum, Germany, vol. 9542, pp. 77-96, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[13] Jeong-Hyeon Kim et al., "Reliable and Lightweight PUF-Based Key Generation Using Various Index Voting Architecture," *2020 Design, Automation & Test in Europe Conference & Exhibition*, Grenoble, France, pp. 352-357, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yohei Hori et al., "Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays," *Journal of Information Processing*, vol. 22, pp. 344-356, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[15] Abhranil Maiti, Inyoung Kim, and Patrick Schaumont, "A Robust Physical Unclonable Function with Enhanced Challenge-Response Set," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 333-345, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[16] Riccardo Della Sala, and Giuseppe Scotti, "Exploiting the DD-Cell as an Ultra-Compact Entropy Source for an FPGA-Based Re-Configurable PUF-TRNG Architecture," *IEEE Access*, vol. 11, pp. 86178-86195, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yizhak Shifman et al., "A Method to Improve Reliability in a 65-nm SRAM PUF Array," *IEEE Solid-State Circuits Letters*, vol. 1, no. 6, pp. 138-141, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Lilian Bossuet et al., "A PUF Based on a Transient Effect Ring Oscillator and Insensitive to Locking," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 1, pp. 30-36, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[19] Siarhei S. Zalivaka, Alexander A. Ivaniuk, and Chip-Hong Chang, "Reliable and Modeling Attack Resistant Authentication of Arbiter PUF in FPGA Implementation with Trinary Quadruple Response," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1109-1123, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] Girish Vaidya et al., "Sensor Identification via Acoustic Physically Unclonable Function," *ACM Journals Digital Threats: Research and Practice*, vol. 4, no. 2, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Wei Duan, and Min Song, "A Lightweight Magnetic Strong Physical Unclonable Function," *2021 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA)*, Zhuhai, China, pp. 155-156, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Xuyang Lu, Lingyu Hong, and Kaushik Sengupta, "CMOS Optical PUFs Using Noise-Immune Process-Sensitive Photonic Crystals Incorporating Passive Variations for Robustness," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 9, pp. 2709-2721, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] Baibhab Chatterjee et al., "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388-398, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[24] PictureBlaise Gassend et al., "Silicon Physical Random Functions," *CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, DC USA, pp. 148-160, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ravikanth Pappu et al., "Physical One-Way functions," *Science*, vol. 297, no. 5589, pp. 2026-2030, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[26] Pratishtha Saxena, and Vijay Tiwari, "Network Security Attacks and Defence," *Journal of Computing and Information Technology*, vol. 9, no. 5, pp. 50-54, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jorge Guajardo et al., "FPGA Intrinsic PUFs and Their Use for IP Protection," *Cryptographic Hardware and Embedded Systems - CHES 2007*, vol. 4727, pp. 63-80, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[28] Sergio Vinagrero et al., "SRAM-Based PUF Readouts," *Scientific Data*, pp. 1-9, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Nir Kshetri, "1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives," *International Journal of Information Management*, vol. 39, pp. 80-89, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[30] Karl Wüst, and Arthur Gervais, "Do you Need a Blockchain?," *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, pp. 45-54, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[31] Quanqing Xu et al., "Blockchain-Based Decentralized Content Trust for Docker Images," *Multimedia Tools and Applications*, vol. 77, pp. 18223-18248, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[32] Md Ashraf Uddin et al., "A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, pp. 1-47, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Miguel Ángel Prada-Delgado et al., "PUF-Derived IoT Identities in a Zero-Knowledge Protocol for Blockchain," *Internet of Things*, vol. 9, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[34] S. Alireza Shamsoshoara et al., "A Survey on Physical Unclonable Function (PUF)-Based Security Solutions for Internet of Things," *Computer Networks*, vol. 183, pp. 1-77, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[35] Suphannee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis, "The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp. 724-742, 2016. [CrossRef] [Google Scholar] [Publisher Link]