GMR
The Original

ROBUST AND SECURE IOT DEVICE AUTHENTICATION USING ON-CHIP PHYSICAL UNCLONABLE FUNCTIONS

Priti Lokhande[1*], Sangeeta Nakhate[2]

[1]Maulana Azad National Institute of Technology, Department of Electronics and Communication Engineering Bhopal, Madhya Pradesh, India, pritilokhande3692@gmail.com
[2]Maulana Azad National Institute of Technology, Department of Electronics and Communication Engineering Bhopal, Madhya Pradesh, India, nakhatesangeeta1@gmail.com
*Corresponding Author: Email: pritilokhande3692@gmail.com

ABSTRACT
The Internet of Things' (IoT) explosive growth has highlighted the need for hardware-anchored, lightweight, and scalable authentication techniques to safeguard billions of linked devices. Conventional encryption methods are unsuitable in IoT environments with restricted resources because they frequently result in high computation overhead and energy consumption. In this paper, a secure IoT authentication system based on an Encoder-MUX Based Bistable Ring Physical Unclonable Function (EMBR PUF) challenge-response scheme is presented. The suggested authentication system integrates an architecture-aware challenge-response obfuscation method inside the EMBR-PUF structure to increase resistance against modeling and replay attacks. Through encoder–MUX interactions, the applied challenge dynamically regulates the internal propagation paths, creating hidden path-dependent behavior and making the challenge–response mapping more non-linear. Nonce-assisted challenge-response obfuscation is also used to improve session-level security with a lightweight approach appropriate for Internet of Things devices. The study concentrates on mutual authentication, session key formation, and replay attack resistance in IoT networks to broaden its usefulness. Using EMBR PUF-derived challenge-response pairs, the developed method offers a mechanism to create distinct device IDs and produce a session key without using resource-intensive cryptographic primitives. Thus, the system presents a three-phase exchange protocol between a device, a gateway and the PUF to achieve mutual authentication with low latency and minimal energy overhead on the gateway. Performance evaluation of the protocol implemented on an Artix-7 FPGA demonstrates near-optimal results, achieving 48.91% uniqueness, 97.22% reliability, and 50.63% uniformity, indicating strong device differentiation. Additionally, it exhibited low communication overhead, equating to 450 bits, and furthermore outperformed existing IoT authentication protocols (including DTLS, HIP, and MAP). By operating at the system level and utilizing the EMBR PUF, the implemented design provides a lightweight, hardware assisted and scalable scheme for IoT security for next generation ecosystems.

KEYWORDS: Physical Unclonable Function (PUF), IoT Authentication, Challenge–Response Obfuscation, EMBR PUF, Hardware Security, FPGA Implementation, Lightweight Security.

1. INTRODUCTION

The Internet of Things (IoT) is a network of smart devices that are connected to the internet and work together to gather, share, and process data to make systems more efficient and automated [1]. IoT devices are being used in a lot of places, such as homes, offices, hospitals, smart grids, and transportation [2]. There are billions of IoT devices installed, and the number is continually growing [3]. Researchers have lately initiated inquiries into IoT privacy protection measures and have scrutinized the legal framework for such protections [4] [5]. A lot of people use IoT networks, which have made it hard to authenticate devices [6]. To protect sensitive data and keep the network safe, it's important that all IoT devices can talk to each other in a safe and reliable way [7]. There are a number of problems with authenticating devices on IoT networks, including high maintenance costs, high power use, and security holes [8] [9].

Using the inherent physical differences of electronic devices, Physical Unclonable Functions (PUFs) can provide unique, device-specific outputs [10] [11]. For security purposes, such as key generation and authentication, these outputs serve as device-specific fingerprints [12] [13]. Even with production techniques that are accurate to within a few micrometers, each chip is still unique due to the inherent sub-micrometer differences in integrated circuits (ICs) that PUFs use [14] [15]. By using these unique characteristics, PUF generates chip-based, lightweight fingerprints that are exceedingly challenging to replicate intentionally or with other methods [16]. Nevertheless, there are certain downsides to PUFs that could affect the authentication process's accuracy and dependability. These include the fact that PUFs expose valuables to aging and increase the cost of hardware [17][18]. They are also vulnerable to complicated assaults, such as side channel and modeling attacks, which pose a concern during CRP transmission in IoT networks [19].

IoT devices must have some sort of authentication set up in order to guarantee that only legitimate terminals can connect to the network and exchange data [20]. Due to their enormous scale and resource limitations, traditional key-based authentication methods are inadequate to stop cloning or unauthorized access in IoT devices [21]. Hardware-based

solutions like PUF provide a portable, effective method of authentication for the IoT environment [22]. PUFs employ the chip's distinct and immutable hardware fingerprints to offer a powerful substitute for key-based authentication methods [23]. To foster confidence and eventually enhance security in the IoT ecosystem, authentication must be a simple, efficient, safe, and scalable technique that PUFs can effectively offer [24].

Secure information sharing between operators and field equipment presents problems in order to address the constraints [25]. Hardware overhead, vulnerability to machine learning attacks, and environmental sensitivity are further drawbacks of current methods. (26). It is difficult to carry out complex cryptographic operations since many IoT devices have limited resources [27]. To provide mutual authentication and session key establishment, the proposed system employs EMBR PUF at the application level, ensuring robust and scalable security for IoT device interactions.

1.1 Motivation

The proposed architecture is based on an Encoder-MUX Based Bistable Ring (EMBR) PUF-based lightweight authentication protocol for Internet of Things (IoT) applications. The implemented system prioritizes the effective use of an EMBR PUF to provide session key generation, mutual authentication, and resilience to replay and side-channel attacks, even though the majority of previous research has concentrated on metrics for PUF design. The suggested framework maintains compatibility with the low-cost and resource-constrained requirements of IoT contexts while establishing dependable device-level trust by using the EMBR-PUF throughout both the enrollment and authentication phases.

- To develop a lightweight architecture aware challenge-response obfuscation-based authentication protocol for IoT systems utilizing an Encoder-MUX Based Bistable Ring (EMBR) PUF, which can act as a trustworthy hardware root of trust.
- To provide mutual authentication and establish a secure session key among the IoT device and the gateway, leveraging the EMBR PUF challenge–response pairs (CRPs).
- To achieve scalable IoT deployments by securely enrolling and verifying devices using EMBR PUFs in a centralized authentication server.

The paper is organized as follows: Section 2 provides a review of recent studies on IoT security threats and PUFs for hardware authentication. Section 3 represents the EMBR PUF prototype design, authentication process, and its operation. Section 4 discusses about the secure communication protocol. Section 5 presents the performance evaluation of the proposed protocol. Section 6 discusses about the applicability of the proposed authentication protocol to other architectures. Finally, Section 7 concludes the paper and offers some suggestions for further work.

2.RELATED WORK

PUFs provide hardware-intrinsic authentication based on process variations, which provide lightweight and secure identification. Nonetheless, PUFs experience reliability issues, vulnerability to modeling attacks, and environmental variation issues. Recent studies establish that the PUF-based authentication can be enhanced by presenting better PUF designs, reliability enhancement techniques, and protection against attacks. The studies presented below are recent advancements in the field of PUFs and are relevant to the current work.

Chen et al. [34] introduced the bistable ring PUF (BR-PUF), which leverages the metastability of an even-numbered inverter loop with access to both ends of the loop to provide different results. The BR-PUF allowed faster response generation, simpler design, and less bias caused by a routing imbalance when compared to an arbiter and ring oscillator (RO-PUFs). The average uniqueness of the BR-PUF was 14.8%, which is lower than the ideal 50% level due to cornering in the layout. Reliability was high with an intra-die HD of ~0.8% at room temperature and not higher than 5.81% with temperature changes. Under aging stress at a constant temperature of 85 °C for 29 days, reliability remained stable with intra-die HD between 0.41% and 1.96% and very low degradation.

Zhang et al. [28] introduced a configurable tristate (CT) PUF for IoT security that can act as an arbiter, ring oscillator, or bistable ring PUF flexibly. By employing XOR based obfuscation, the CT-PUF thwarted machine learning attacks with an average prediction accuracy of about 60%. In addition, the FPGA implementation had excellent PUF metrics, almost ideal uniformity 48-50%, reliable consistency (>92%), and uniqueness values near 49-50%, while incurring minimal cost and hardware design overhead.

Thirumoorthi et al. [29] introduced a hybrid chaotic-bistable ring PUF (Chaotic-BR-PUF). This design increased the robustness of BR-PUFs by obfuscating responses with nonlinear chaotic functions that progress through multiple non-repeating chaotic patterns. The Chaotic-BR-PUF was implemented on Xilinx Artix-7 FPGAs with ideal PUF metrics: uniqueness ~ 48-50%, uniformity ~ 48.5%, and reliability ~ 92% with a reasonable hardware footprint. The hybrid system's chaotic obfuscation was hostile to PAC-based k-junta modeling of a BR-PUF. It reduced the prediction accuracy of regression attack ML strategies such as SVM, KNN, and logistic regression to 50% - 60%.

Annapurna K. Y. et al. [30] presented a Secure and Provable PUF (SP-PUF) variation constrained for minimality for lightweight IoT authentication, with a focus on minimalism and low resource usage for FPGA implementations. They used the metastability of cross-coupled inverters to generate stable responses with high reproducibility. They showed 98% reliability and 38% uniqueness. The BR-PUF design would require fewer hardware resources compared to the previous arbiter and ring oscillator PUFs, making it more feasible for constrained IoT nodes.

Jin et al. [38] presented a low-overhead XOR Multi-PUF that employs configurable priority XOR gates together with an obfuscation process to enhance ML attack resistance. The configuration is also able to operate as a RO-PUF and a BR-PUF to significantly increase the number of CRPs while keeping hardware costs low. Their implementation in an FPGA on a PYNQ-Z2 board produced good PUF properties, including 48.85 % uniqueness, balanced uniformity, and over 97% reliability, while consuming slices down to 8, versus many thousands of slices in traditional RO-PUFs.

Han and Shin [36] presented an elaborate PUF architecture that depends on bistable ring (BR) feed-forward chains with a lightweight secure (LS) network to address machine learning attacks. They incorporated nonlinear transformations at the interconnect, input and output, and used XOR-based feed-forward paths to improve unpredictability as well as scalability. The cost-effective implementation of the PUF on an FPGA with 64-bit challenge as well as 32-bit response using reliable LUTs shows its viability for IoT applications. The PUF reported ~48.31% uniqueness, ~98.15% reliability, and ~49.49% randomness, while holding SVM attack prediction accuracy at ~50%, akin to an ideal unclonable case.

Li et al. [35] introduced a dynamic division multiplexing bistable PUF, which decreases the cell area while maximizing the entropy used. The system uses asymmetric transistor sizing to stabilize the pull-up (or pull-down) network, while the minimum-size complementary network is the source of main entropy. A cross-coupled twin cell array is dynamically selected such that only one selected cell will dominate the response while all other cells in the response are negligible, thus allowing the dynamic multiplexing. The design supports two independent modes of operation, both generating a key size. This PUF twin cell was fabricated in TSMC 65-nm technology, and achieved a compact 1.32 μm^2 (308 F^2) chip area. In chip level testing, both modes performed near-ideal entropy (0.9999/0.9997), uniqueness (49.9%/49.7%), and both modes produced remarkable reliability after 100 attempts (99.1%/97.7%) for NC-PUF and PC-PUF, respectively.

Huang et al. [37] presented an existing unmodeled attack-resistant strong PUF architecture that utilizes Bent functions to increase nonlinearity for increased cryptographic strength, thereby improving resilience against machine learning and cryptanalytic attacks. The design uses Maiorana-McFarland constructed Bent functions to disguise PUF responses and make them less predictable. The design also has a Feistel network where weak PUF responses become device-specific key values to enable distinct and secure challenge–responses while adhering to the Bent function construction requirements. The simulations demonstrated prior to the FPGA implementation illustrate that the approach can obtain higher cryptographic nonlinearity compared to traditional XOR arbiter PUFs. Additionally, the FPGA analysis demonstrated strong resilience to a variability of modeling assaults such as logistic regression, neural networks, and evolutionary algorithms. A summarization of the existing method is presented in Table 1.

In recent years, there have been number of studies on PUF-based authentication that have focused on the enhancement of verification schemes reliability and robustness, and mitigation of modeling attacks. Many of the PUF-based authentication schemes have made significant strides towards improving uniqueness, stability, and cloning resistance, but many still face challenges due to environmental variability, and often lack power, resource (power, and area), and the potential to scale across hardware platforms. To overcome the limitations of traditional key-based authentication in resource-constrained IoT devices, the proposed system implements a lightweight authentication scheme based on the Encoder-Mux Based Bistable Ring (EMBR) PUF. This approach ensures secure and scalable device authentication without relying on stored cryptographic keys.

Unlike conventional PUF-based authentication schemes that treat the PUF as a black-box challenge–response generator, the proposed work integrates architecture-aware obfuscation directly within the EMBR-PUF hardware structure. In the proposed design, the applied challenge not only stimulates the PUF but also dynamically controls the internal signal propagation paths through encoder–MUX interactions. Consequently, the generated response depends on hidden path-dependent propagation dynamics and cyclic bistable ring behavior, thereby introducing additional non-linearity into the challenge–response relationship. Additionally, nonce-assisted challenge and response obfuscation are included to maintain low hardware complexity appropriate for IoT devices with limited resources while enhancing defense against replay and modeling assaults.

Table 1. Summarization of Existing Methods.

Reference	Method	Contribution	Metrics	Disadvantages
Chen et al. [34]	BR-PUF	Leveraged metastability of even-numbered inverter loops for faster response, simpler design, and less bias.	Reliability was high, with intra-die HD ~0.8% at room temperature, below 5.81% under temperature changes, and stable between 0.41%–1.96% after 29 days aging at 85 °C.	Vulnerable to environmental noise affecting stability; limited scalability in large arrays.
Zhang et al. [28]	Configurable Tristate PUF (CT-PUF)	Flexible design acting as Arbiter, RO, or BR PUF; XOR obfuscation	Uniformity: 48–50%, Reliability: >92%, Uniqueness: ~49–50%	Increased design complexity due to configurability; higher
Thirumoorthi et al. [29]	Hybrid Chaotic-BR-PUF	Combined chaotic functions with BR-PUF to resist modeling attacks and enhance robustness.	Uniqueness: ~48–50%, Uniformity: ~48.5%, Reliability: ~92%	High computational overhead and resource demand; difficulty integrating into constrained hardware.

Annapurna K. Y. et al. [30]	Minimal BR-PUF	Lightweight, minimal design for IoT nodes with high reproducibility.	Reliability: ~98%, Uniqueness: ~38%	Limited adaptability for diverse environments; weaker resistance against side-channel attacks.
Jin et al. [38]	XOR Multi-PUF	Configurable XOR gates with obfuscation; scalable CRP space; low cost.	Uniqueness: 48.85%, Reliability: >97%, Balanced uniformity	Complexity in timing synchronization; potential vulnerability to fault injection attacks.
Han & Shin [36]	BR Feed-Forward + LS Network	Used XOR feed-forward with nonlinear transformations to boost unpredictability.	Uniqueness: ~48.3%, Reliability: ~98.15%, Randomness: ~49.4%	Increased latency due to nonlinear layers; sensitivity to aging effects on circuit components.
Li et al. [35]	Dynamic Division Multiplexing BR-PUF	Used asymmetric transistor sizing and dynamic twin-cell selection to maximize entropy with reduced area.	Uniqueness: ~49.7–49.9%, Reliability: 97.7–99.1%, Area: 1.32 μm²	Challenging to calibrate dynamically; possible mismatch-induced errors during operation.
Huang et al. [37]	Bent Function-based Strong PUF	Applied Bent functions + Feistel structure for strong nonlinearity and ML resistance.	Strong resilience to ML attacks (SVM, NN, EA), High cryptographic nonlinearity	Increased hardware resource usage; potential timing bottlenecks affecting throughput.

3.Proposed System

The authentication scheme proposed for IoT devices using the Encoder-Mux Based Bistable Ring (EMBR) PUF [39] follows a two-phase approach, such as enrollment and verification, as depicted in Fig. 1. In the enrollment stage, the PUF in each IoT device is connected directly to the server. The server sends a set of random inputs as a challenge to the device, and the PUF generates unique responses based on the inherent process variation of the device hardware. The challenge-response pairs (CRPs) are collected as well as stored in the server's CRP database, which, along with the device identification information, generates a unique fingerprint for each device. In the verification phase, when a device wants to access the network, the authentication server first validates the request by confirming the device ID. Then sends a new trial to the device's PUF. The response generated is sent back to the server and compared against the CRPs stored at the time of enrollment. If the response matches the data in the CRP database, then the device is considered authenticated; if not, then the request is denied. This proposed scheme has provided a lightweight as well as trustworthy authentication mechanism for IoT devices without relying on stored traditional cryptographic keys.

3.1 EMBR PUF Architecture

This paper proposes a device authentication method for IoT applications that utilizes the Encoder-Mux Based Bistable Ring PUF (EMBR PUF) [39] as presented in Fig. 2. The EMBR PUF makes use of a 4:2 priority encoder along with NOR gates and Multiplexers. One stage of EMBR PUF receives a 4-bit challenge and generates a 1-bit response. Here, the proposed 32-bit EMBR PUF gives an 8-bit response. The output from every stage is connected to the input of the next stage; the last stage's output is fed back to the input of the first stage. The priority encoder receives the 3-bit challenge input. Depending upon the output that is feedback from the previous stage and the random challenge input applied, the priority encoder will generate a consistent encoded output. This encoded output is then given to the input of two NOR gates. The fourth challenge input sent to the multiplexer's select line decides which NOR gate output can proceed to the input of the subsequent stage via the multiplexer. The device produces a random response because of the intrinsic randomness that is added during the manufacturing process.

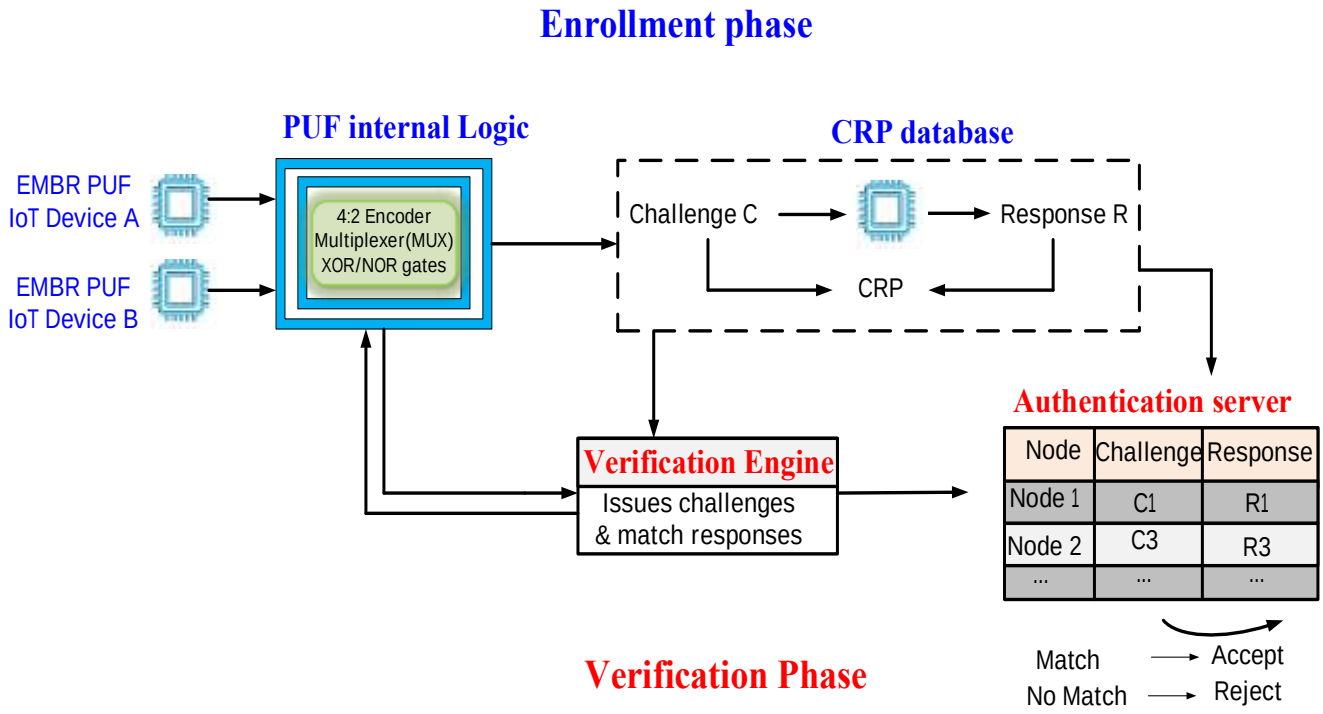

Fig. 1. Design overview of proposed EMBR PUF-based authentication scheme

To further explain, the proposed Encoder–MUX Based Bistable Ring PUF (EMBR-PUF) architecture consists of multiple interconnected bistable ring stages arranged in a cyclic feedback configuration. Each stage comprises a 4:2 priority encoder, two NOR gates, and a 2:1 multiplexer. The applied challenge input dynamically controls the multiplexer selection path, while the encoder-generated signals propagate through the NOR-gate structure to produce stage-dependent propagation behavior. The output of the final stage is fed back to the input of the first stage to establish cyclic bistable ring operation.

During response generation, the applied challenge influences both the encoder output and the internal propagation path selected through the multiplexer structure. Consequently, the generated response depends on hidden propagation dynamics, encoder-driven signal transformation, and cyclic feedback behavior. In the implemented architecture, each stage generates one response bit, and the complete EMBR-PUF response is obtained by combining the responses generated across all stages. Here, for 8-stages it generates an 8-bit response. It should be noted that the reported 8-bit response corresponds to a single evaluation instance of the implemented EMBR-PUF architecture. For practical authentication deployment, longer effective authentication responses (32-bit, 64-bit, 128-bit etc.) can be generated either through increasing the number of PUF cells or by applying several separate challenges and concatenating the resulting responses. Additionally, the proposed authentication framework further strengthens security through nonce-assisted challenge and response obfuscation, thereby significantly increasing the effective unpredictability and resistance against replay and modeling attacks.

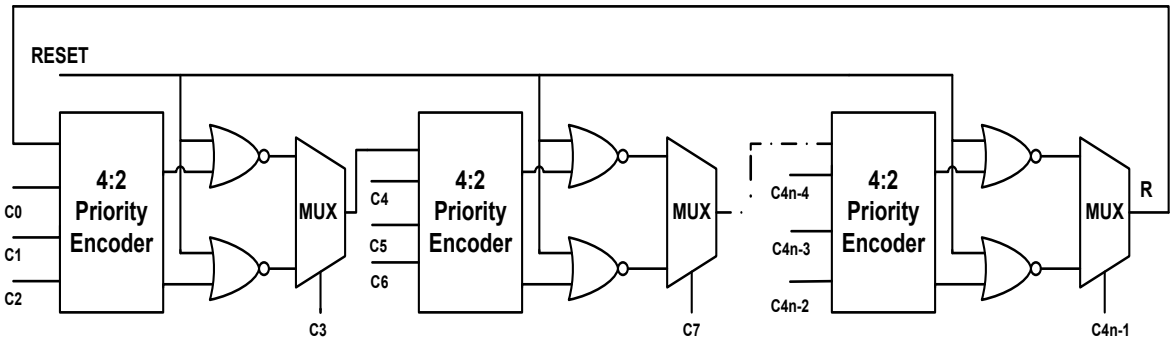

Fig. 2. Design of Encoder-Mux Based Bistable Ring PUF [39]

The primary goal of incorporating this PUF framework is to provide a secure authentication connection between an authentication server and an Internet of Things device. An effective and space-saving method for authenticating Internet of Things systems is provided by this method. Fig. 1 shows how the proposed approach creates a safe connection between the Internet of Things devices and the authentication server, protecting the privacy and integrity of data. By capitalizing on the PUF's distinct characteristics, the method effectively gets rid of any possible authentication issues. Internet of Things (IoT) devices must securely store and update challenge-response pairs (CRPs) for authentication to work. By providing a low-cost mechanism for device verification and reliable hardware identification, the proposed PUF-based

technique overcomes several limitations of conventional authentication approaches. It uses a straightforward method to guarantee safe device-to-device connectivity.

3.2 4:2 Priority Encoder

Encoders are essential for digital system security because they convert data into a coded form that only authorized users can decipher. Encoders are commonly used as the initial safeguard to encrypt data before transmission or processing in the context of communication and hardware security. Obfuscating data to prevent unwanted access, manipulation, or reverse engineering is one of the main security applications of encoders. Encoders are crucial components of cryptographic systems that are used for data pre-processing or safe encoding methods. They are extremely useful in embedded systems, smart cards, and Internet of Things devices where resource efficiency is crucial.

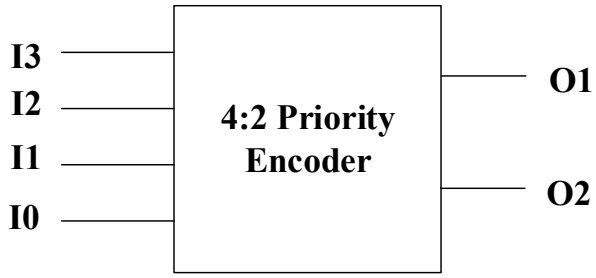

Fig. 3. Block Diagram of 4:2 Priority Encoder

A simple digital device called a 4:2 priority encoder [39] converts four input bits into a 2-bit binary code according to priority. The block diagram of a 4:2 Priority encoder is shown in Fig. 3. In contrast to a typical encoder, the encoder outputs the binary value corresponding to the highest-priority active input after assigning the inputs a priority ranging from highest (I_3) to lowest (I_0). The encoder prioritizes the input with the highest priority when several inputs are high at the same time. For example, the output will show I_2 if both I_2 and I_0 are active. Table 2 represents the truth table of a 4:2 priority encoder. The 4:2 priority encoder streamlines complicated decision-making and enhances system efficiency by condensing several input requests into a binary code.

Table 2. Truth Table of 4:2 Priority Encoder

Inputs				Outputs	
I3	I2	I1	I0	O1	O2
0	0	0	0	X	X
0	0	0	1	0	0
0	0	1	X	0	1
0	1	X	X	1	0
1	X	X	X	1	1

In Table 2, ‘X’ represents a don’t care condition, indicating that the corresponding input value does not affect the output.

3.3 Proposed Architecture-Aware Obfuscation Strategy

The proposed authentication framework employs a conventional challenge–response (CRP)-based authentication paradigm to maintain compatibility with lightweight IoT environments, while the primary novelty of this work lies in the integration of the EMBR-PUF architecture with an architecture-aware challenge and response obfuscation mechanism. Unlike existing PUF-based authentication schemes, where the PUF and the protocol are treated as independent components, the proposed approach explicitly leverages the internal structural characteristics of the EMBR-PUF during the authentication process.

In the proposed design as shown in Fig. 4, the input challenge is first transformed using a nonce-based hash function, defined by Equation (1):

$$C' = H(C \parallel N_s) \quad (1)$$

ensuring that the effective challenge applied to the PUF varies across sessions. This prevents direct reuse of challenges and mitigates replay-based attacks. The obfuscated challenge (C') is then applied to the EMBR-PUF, where a 4:2 priority encoder generates control signals (E(C')) that determine the internal configuration of the circuit.

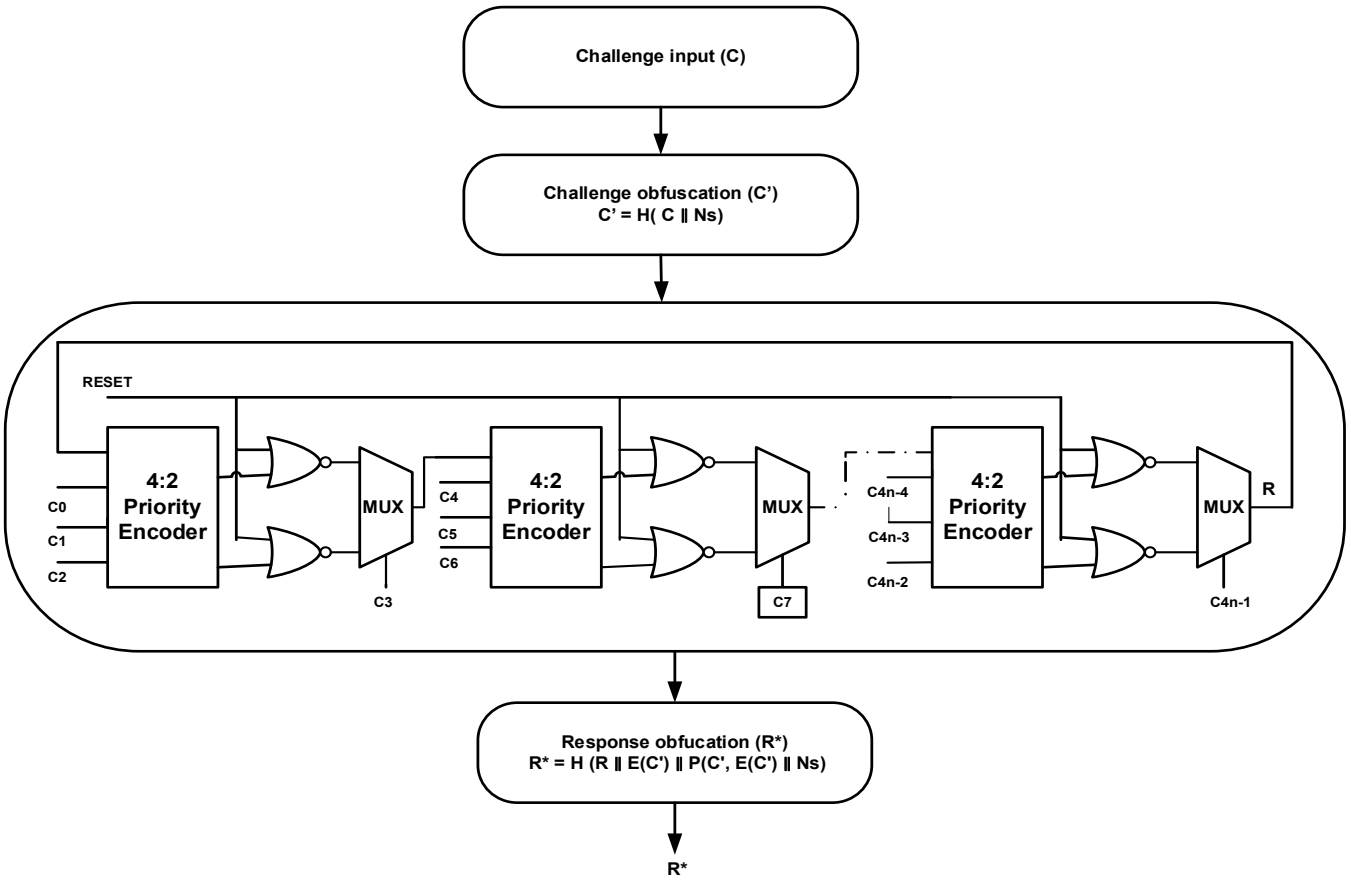

Fig. 4. Proposed Encoder-Mux Based Bistable Ring(EMBR) PUF architecture with obfuscation

The encoder output drives two parallel NOR-based logic paths, and a multiplexer selects one of these paths, resulting in a path-dependent signal propagation characterized by (P(C', E(C'))). This routing behavior directly influences the bistable ring, producing the raw PUF response (R). To further enhance security, the response is not transmitted directly; instead, it is transformed using both internal hardware parameters and session-specific randomness as represented by Equation (2) as follows:

$$R^* = H(R \parallel E(C') \parallel P(C', E(C')) \parallel Ns) \quad (2)$$

This formulation introduces a multi-layer transformation in the authentication process expressed by Equation (3) as:

$$C \rightarrow C' \rightarrow (E(C'), P(C', E(C'))) \rightarrow R \rightarrow R^* \quad (3)$$

which effectively conceals the direct relationship between the applied challenge and the observed response. This authentication protocol flow using EMBR PUF with challenge and response obfuscation is represented by Fig. 5.

The obfuscated challenge C' is generated as:

$$C' = H(C \parallel N_s)$$

where C represents the original challenge, Ns denotes the server-generated session nonce, H(.) represents the hash function, and "‖" denotes concatenation.

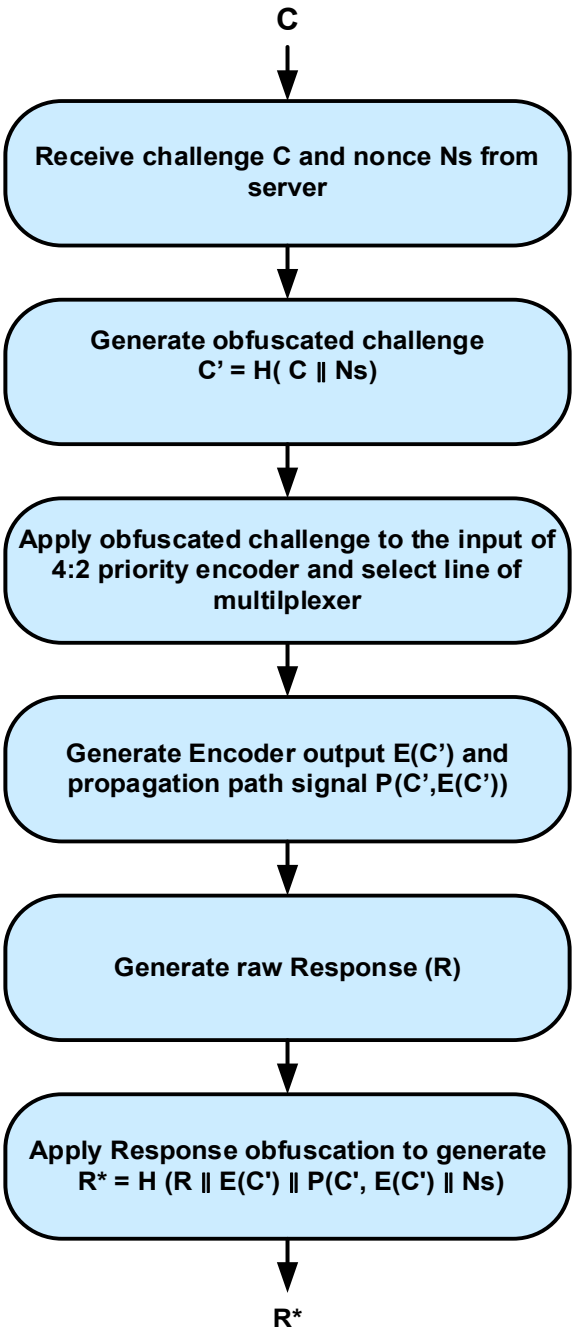

Fig. 5. EMBR PUF Authentication Protocol Flow

For example, let the original challenge and server nonce be:
C = 10101100
Ns = 11001010
After concatenation:
$(C \parallel N_s)$ = 1010110011001010
Applying the hash function generates the obfuscated challenge:
C' = H(1010110011001010)
Assuming the hash output is:
C' = 01101011
the generated obfuscated challenge (C') is then applied to the EMBR-PUF instead of the original challenge. Within the proposed EMBR-PUF architecture, the applied challenge dynamically controls the multiplexer selection paths while the encoder outputs propagate through NOR-gate logic, thereby introducing hidden propagation behavior and increased non-linearity into the challenge–response relationship.
After internal propagation through the cyclic bistable ring stages, the EMBR-PUF generates the raw response (R). Assuming the obtained raw response is:
R = 11010010

To further strengthen authentication security, the proposed framework employs response obfuscation based on encoder-dependent propagation behavior and session-specific nonce values. After the EMBR-PUF generates the raw response (R), the final authentication response (R*) is computed as:

$R^* = H(R \parallel E(C') \parallel P(C', E(C')) \parallel Ns)$

where:

R represents the raw EMBR-PUF response, E(C') denotes the encoder output corresponding to the obfuscated challenge C', P(C',E(C')) represents the path-dependent propagation information generated through encoder–MUX interactions, Ns is the server-generated session nonce, and H(.) represents the hash function.

For example, assume the following values are obtained during an authentication session:

R = 11010010

E(C') = 10101100

P(C', E(C')) = 01100111

Ns = 11001010

The concatenated authentication parameter becomes:

11010010 ‖ 10101100 ‖ 01100111 ‖ 11001010

which gives:

1101001010101100011001111100 1010

Applying the hash function to the concatenated bit stream generates the final obfuscated response:

R* = H(1101001010101100011001111100 1010)

Assuming the hash output is:

R* = 10111001

the final transmitted authentication response becomes:

R* = 10111001

Since the final response depends simultaneously on the raw PUF response, encoder-generated signals, hidden propagation-path behavior, and session nonce values, the resulting challenge–response mapping becomes highly non-linear and dynamically varying across authentication sessions. Consequently, the proposed architecture-aware obfuscation mechanism significantly strengthens resistance against replay attacks and machine-learning-based modeling attacks while maintaining lightweight implementation suitable for IoT environments.

In contrast to prior works that rely on generic obfuscation techniques such as XOR masking, LFSR-based transformations, or simple permutations, the proposed approach incorporates internal encoder states and multiplexer-based path information, which are inherently device-specific and not externally observable. This results in a hardware-driven obfuscation mechanism that tightly couples the PUF architecture with the authentication protocol.

As a result, the proposed method significantly increases resistance to machine learning-based modeling attacks, as the adversary cannot access or infer the intermediate parameters (E(C')) and (P(C', E(C'))). Moreover, the inclusion of a nonce ensures session-level freshness, preventing replay attacks without introducing significant computational overhead.

Therefore, while the overall framework remains compatible with standard CRP-based authentication, the proposed work introduces a fundamentally different architecture-aware and hardware-integrated obfuscation paradigm, which distinguishes it from existing PUF-based authentication schemes.

Table 3 shows the comparison of proposed authentication protocol with recent PUF based authentication protocol available in the literature. As shown in Table 3, the proposed EMBR-PUF-based authentication scheme achieves a balanced improvement across multiple performance and security metrics. Unlike conventional approaches that rely on direct or partially obfuscated CRPs, the proposed method avoids exposing raw challenge–response pairs by incorporating both challenge and response obfuscation mechanisms.

In terms of communication overhead and latency, the proposed scheme remains efficient due to its single-pass authentication structure combined with lightweight hash operations. The implementation complexity is also low, as the design leverages existing encoder and multiplexer structures within the EMBR-PUF without requiring additional hardware modules.

3.4 Enrollment phase

EMBR PUF-based authentication typically involves two main stages, namely the Enrollment phase and Verification phase. In the enrollment phase, as shown in Fig. 6, the EMBR PUF circuit from each IoT device is registered with the authentication server, with IoT devices having unique identifiers (for instance, D794974, D796304, D795748, etc.) connected to the server. Each IoT device consists of an EMBR PUF module that generates outputs unique to that device, which is the first step in the enrollment process. The server provides the IoT devices with a set of challenge bits (e.g., 10101011, 11010101).

Once a challenge is delivered to a device, the PUF yields a response that is also unique (e.g., 11100111, 10111101). The output depends on the inherent hardware variation of the device. The server collects the challenge-response pairs (CRPs) and stores them along with the device ID in its centralized database. In this way, a unique fingerprint of the device has been registered, which differentiates it from all other devices on the network. At the conclusion of the enrollment phase, the server now has a trusted and verified database of CRPs and IDs that can be used in the verification phase when the device attempts to connect to the network.

Table 3. A comparative analysis of the proposed scheme with recent PUF-based authentication protocols

Scheme	PUF Type	Communication Overhead	Latency	Energy	CRP Usage	Modeling Attack Resistance	Replay Protection	Implementation Complexity
Proposed Work	EMBR PUF	Low (Single Response + nonce)	Low (Single pass + hashing)	Low (No extra hardware blocks)	Limited (no raw CRP exposure)	High (encoder + path + nonce obfuscation)	Yes (nonce-based)	Low (reuses encoder & MUX)
Khalfaoui et al., [47]	Arbiter PUF	Medium (multiple exchanges)	Medium	Medium	High (direct CRP	Low (linear CRP exposure)	Yes	Medium (protocol logic)
Yang A.et al., [48]	Arbiter PUF	Medium (test + auth stages)	Medium	Medium	Medium (filtered CRPs)	Medium (partial obfuscation)	Yes	Medium (Self-test circuit)
Yalli et al., [49]	Generic PUF	Low	Medium	Low	Medium	Medium (fuzzy masking)	Yes	Medium (fuzzy logic)
Sajadi et al., [50]	Strong PUF	Medium	Medium	Medium	High	High (complex interconnection)	Yes	Medium-High (modified structure)
Jin et al., [51]	Power IoT Based PUF	Low	Low	Low	Medium	High (chaotic mapping)	Yes	Low-Medium (math
Zhuang et al.,[52]	Lightweight PUF	Low (lightweight exchange)	Low	Low	Medium (controlled CRP use)	Medium-High (protocol-level obfuscation)	Yes (nonce-based)	Low (lightweight cryptography)
Tun & Mambo [53]	Strong PUF	Medium	Medium	Medium	High	Medium (protocol-level only)	Yes	Medium

Legend:
Low = minimal resource requirement; Medium = moderate; High = significant requirement

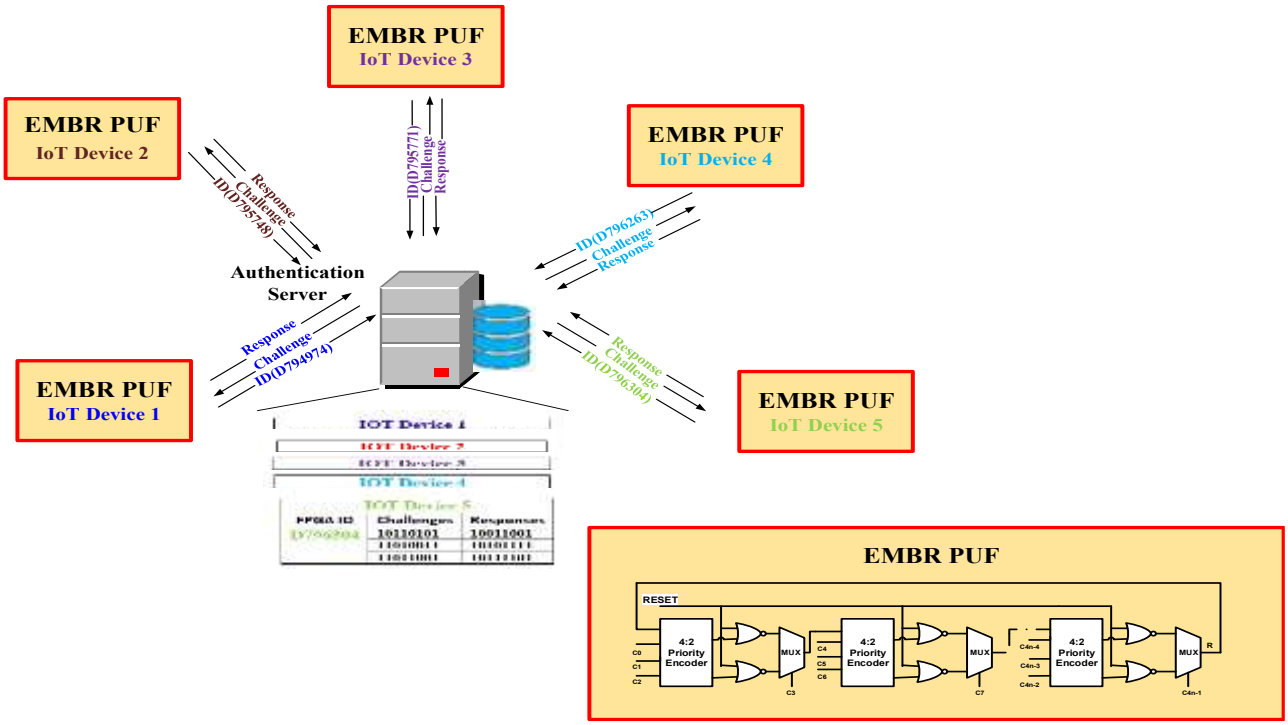

Fig. 6. Enrollment phase for the EMBR PUF

3.5 Verification Phase

During the verification step, as shown in Fig. 7, the PUF circuit dedicated to an IoT device has been used for authentication. In this phase, the server first requests each device's identification before establishing the connection. The server submits the predetermined challenge bits to the IoT device with a device ID, and that device returns the response bits to the server. If one CRP record in the database matches the response bits provided by the device, it will be validated

as authorized. Properly constructed CRPs never repeat challenge bits, to ensure integrity against a man-in-the-middle attack and to inhibit prediction of a future CRP. This process guarantees that each authentication session will be unique and is secure against replay attacks. Multiple IoT devices can be distinguished in a response by using a device ID; however, because it employs a challenge-response method, the PUF will only produce the genuine response.

The server checks the response received against its own CRP database, as shown in Fig. 7. If the received response matches the predictable value, the device is securely granted access to network resources; otherwise, it is untrusted and must be rejected. Fig. 8 shows the process involved in the verification phase of EMBR PUF. Using the unpredictability and unclonable features of the PUF, storage of cryptographic keys is entirely removed from the device.

It must also be recognized that the authentication is lightweight and particularly compatible with IoT, where restrictions on resources and the need for scalability are two major concerns. The server relates the received response to the corresponding entry in its CRP database. If the response matches the predictable value, the device is securely granted access to network resources; otherwise, it is deemed untrusted and rejected.

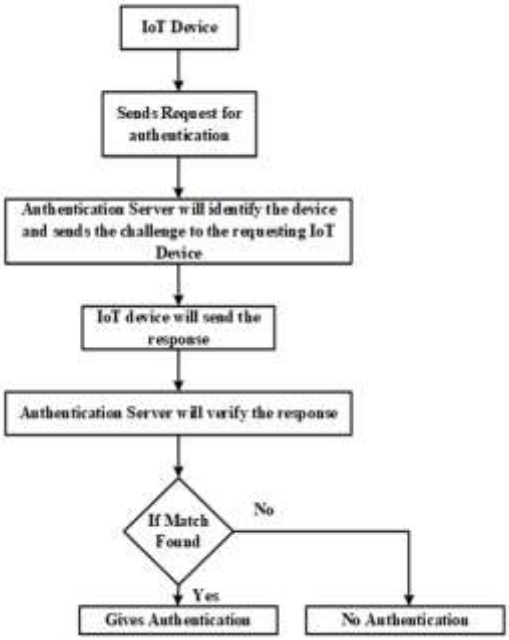

Fig. 7. Verification phase for the EMBR PUF

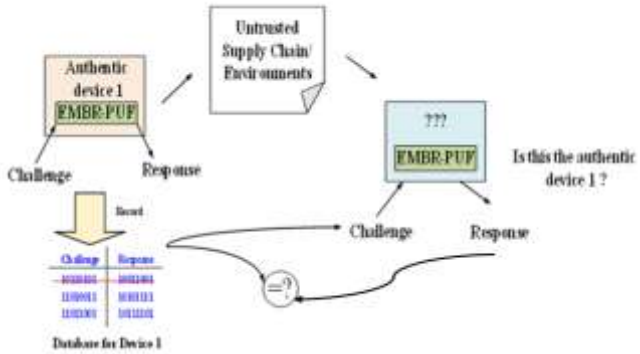

Fig. 8. Process involved in the verification phase of EMBR-PUF

3.6 Scalability and Security of Centralized CRP Management

The proposed authentication protocol assumes a centralized server that manages reference data corresponding to enrolled devices. Unlike conventional strong PUF-based systems that require storage of a large number of raw challenge–response pairs (CRPs), the proposed approach reduces storage overhead by avoiding direct exposure and storage of raw PUF responses.

During enrollment, the server stores only derived or reference values associated with the obfuscated response, rather than maintaining a complete CRP database. Since the transmitted response is computed as ($R^* = H(R \| E(C') \| P(C', E(C')) \| Ns)$), the stored data do not reveal the underlying PUF response (R) or the internal parameters (E(C')) and (P(C', E(C'))). This significantly reduces storage requirements and improves scalability, especially in large-scale IoT deployments.

From a security perspective, the use of a centralized database introduces potential risks in case of data leakage. However, in the proposed design, the stored entries correspond to cryptographically protected values. Due to the preimage resistance of the hash function, it is computationally infeasible for an adversary to recover the original PUF response or reconstruct

valid CRPs from the stored data. Furthermore, since the obfuscation incorporates internal hardware-dependent parameters that are not externally accessible, the effective challenge–response relationship remains hidden.
In terms of modeling attacks, traditional PUF systems are vulnerable when a large number of CRPs can be collected and used for machine learning-based approximation. In contrast, the proposed approach limits CRP exposure by transmitting only obfuscated responses and by incorporating session-specific nonces, which prevent reuse of observed data. Consequently, the adversary cannot obtain a consistent dataset corresponding to the true PUF behavior, thereby significantly reducing the effectiveness of modeling attacks.
Overall, the proposed CRP management strategy achieves a favourable balance between scalability, storage efficiency, and security, making it suitable for deployment in resource-constrained and large-scale authentication systems.

4.Secure Communication Protocol

The protocol presented in Fig. 9 describes the mutual authentication of a smart device (SD) and gateway (G), and the creation of a new session key using an EMBR PUF. Once device enrollment and system-level verification have been completed, the authenticated IoT device moves to the final stage of the protocol. In this stage, a secure communication session is established among the device and the server for a secure channel for the purpose of exchanging information confidentially and with protection for integrity. The device will use the verified PUF-derived credentials from device enrollment to perform functionality such as generating session keys, exchanging nonces, and authenticating messages without using conventional cryptographic primitives. SN_u denotes the serial number of the smart device, and *IDu* means the user, or device, identifier. FP_u is the user's PUF value, and ID_G is the gateway identifier. Two random nonces are generated during the process, including $N1_u$ by the smart device and $N2_G$ by the gateway. The gateway also provides a challenge, C_G which generates a unique response R_U from the PUF. $K_{u\text{-}G}$ Indicates the long-term secret shared by the device and gateway, while $SK_{u\text{-}G}$ is the new session key generated during authentication. Any data that is encrypted using a key uses the notation *E {key, data}*. The cryptographic hash function uses the notation *h(x)*, and the XOR function is represented with the symbol $\oplus$.
Initially, during execution, the smart device acquires its serial number SN_u, its PUF fingerprint FP_u, a newly generated nonce *N1u*, and its identifier ID_u. It calculates an integrity hash $h(SN_u \,\|\, FP_u \,\|\, N1_u)$ and encrypts the whole collection with the shared secret used in $K_{u\text{-}G}$ generating

$$Cipher1 = E\{K_{u-G}(SN_u, FP_u, N1_u, ID_u, h(SNu \,\|\, FP_u \,\|\, N1_u))\} \quad (4)$$

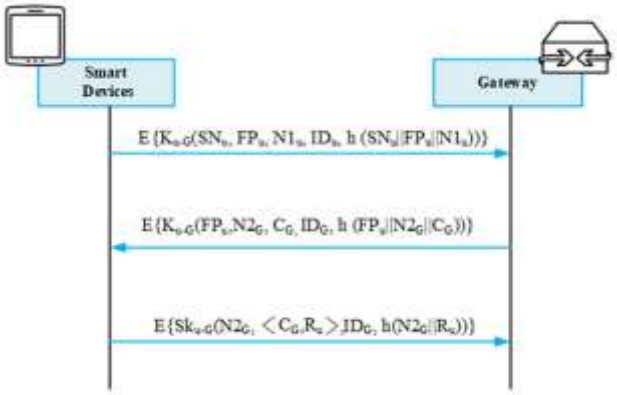

Fig. 9. PUF based secure Authentication and key exchange

The device transmits (ID_u, Cipher1) to the gateway. After decrypting the information, the gateway checks its database to determine if the fingerprint FP_u is associated with a user ID_u. In the case that the fingerprint is valid and the serial number is not previously known, it shall keep the serial number SN_u. The gateway proceeds to create its own nonce $N2_G$ and a random challenge C_G for the device's PUF. Following this, it calculates $h(FP_u \,\|\, N2_G \,\|\, C_G)$, encrypts them using $K_{u\text{-}G}$, and sends these back to the device along with ID_G.

$$Cipher2 = E\{K_{u-G}(FPu, N2_G, C_G, ID_G, h(FP_u \,\|\, N2_G \,\|\, C_G))\} \quad (5)$$

After receiving Cipher 2, the smart device decrypts it, extracts $N2_G$ and the challenge C_G, and employs its PUF on C_G to create the response R_u. Finally, the device computes the session key by XORing the hashes of its own nonce, the fingerprint, and the PUF response:

$$SK_{u-G} = h(N1_u) \oplus h(FP_u) \oplus h(R_u) \quad (6)$$

Utilizing this key, the component produces a third encrypted message where $N2_G$, the challenge-response pair (C_G, R_u), the gateway ID_G, and an appended hash $h(N2_G \,\|\, R_u)$ and it sends $(ID_G, Cipher3)$ to the gateway

$$Cipher3 = E\{SK_{u-G}(N2_G, \langle C_G, R_u \rangle, ID_G, h(N2_G \,\|\, R_u))\}$$

(7)

At last, the gateway allows the computations of the same session key $SK_{u\text{-}G}$ (because it knows $N1_u$, FP_u and R_u), decrypts Cipher3, and verifies the hash. If they are correct values, the smart device is authenticated, the session key is stored to protect the next commands or data exchanges. The vertical as shown in Fig. 9 indicates the lifelines of the smart device and the gateway, while the three horizontal arrows represent the messages that are exchanged: Cipher1 for the device request, Cipher2 for the gateway's challenge and nonce, and Cipher3 for the device's PUF response and confirm session-key. Once Cipher3 is received, authentication is completed, and both parties are in possession of $SK_{u\text{-}G}$ which will subsequently be used to secure additional traffic within the smart-home network.

5.RESULTS AND DISCUSSION

To evaluate the operational performance and practicality of the application-based EMBR PUF for IoT device authentication, the system was realized and tested on an Artix-7 FPGA using a Digilent BASYS3 board. The design as well as implementation of the EMBR PUF authentication framework were performed using the Xilinx Vivado Development Suite (Vivado), which is a solution-specific integrated toolchain for the synthesis, implementation, and optimization of FPGA-based designs. In conjunction with operational performance metrics, various performance metrics were examined to allow for strong device identification while providing secure session establishment.

5.1 Performance Metrics

To assess the effectiveness of the proposed application using EMBR PUF for the task of authentication of IoT devices, key performance metrics were analyzed in the context of secure and efficient device authentication. Uniqueness: When different IoT devices receive the same authentication challenge, they must return different responses. Reliability: The responses of the device must be stable and predictable despite environmental changes such as temperature or supply voltage. This stable response is critical to consistent device authentication. Uniformity: The responses of the device must have a nearly equal balance of '0's and '1's, reflecting the randomness and unpredictability.

In addition to these core properties of a PUF, communication cost is another important metric for practical authentication of IoT devices. Specifically, a low-cost communication protocol to minimize the amount of data exchanged between devices and servers, along with low latency and energy efficiency, is highly desirable. This must be done, especially in many types of technology or devices that are power-constrained. Together, these metrics will substantiate the plausibility of the EMBR PUF for a secure, reliable, and implementable IoT authentication ecosystem.

$$Uniqueness(U) = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{HD(R_i, R_j)}{L} \times 100\% \quad (9)$$

Where, N represents number of devices, R_i ,R_j = responses of device and, L= response length (bits), $HD(.)$ = Hamming Distance, here Ideal value=50% maximal distinction in responses across devices.

$$Reliability(R) = \left(1 - \frac{1}{M} \sum_{k=1}^{M} \frac{HD(R, R_k)}{L}\right) \times 100\% \quad (10)$$

where M is the number of repeated measurements, R is the reference response, R_k is the response at the k^{th} trial under same challenge and L represents the response length (bits), here the Ideal value=100% indicating perfect reproducibility.

Table 4. Reliability at different supply voltages

PUF Types	Reliability (%) (At 1.0V)	Reliability (%) (At 2.5V)	Reliability (%) (At 3.3V)
Proposed protocol based EMBR PUF	97.11	97.18	97.24

Reliability tests were conducted under various supply voltage situations to assess the robustness of the suggested EMBR-PUF, as indicated in Table 4. The intra-Hamming distance was calculated after the responses were gathered for the same set of challenges at various voltage levels. The findings show that the suggested PUF is resistant against power supply changes and maintains excellent reliability with just minor degradation under voltage variations.

$$Uniformity(U_f) = \frac{1}{L} \sum_{i=1}^{L} b_i \times 100\% \quad (11)$$

where b_i is the i^{th} response bit (0 or 1), L is the response bit-length, here Ideal value=50% indicating an even distribution of bits.

The overall communication cost of the suggested authentication framework can be expressed as the sum of the bits transmitted by the user, gateway, and sensor node.

$$C_{total} = C_{User} + C_{Gateway} + C_{Sensor} \quad (12)$$

where C_{user} is the bits transmitted by the user device (challenge, authentication requests), $C_{Gateway}$ is the bits transmitted by the gateway during authentication (forwarding, response aggregation) and C_{Sensor} is the bits transmitted by the sensor node (PUF responses, status updates)

5.2 Performance Evaluation

This section details the performance analysis of the EMBR PUF in terms of both its functional quality metrics and hardware-level metrics. The study analyses the design's uniqueness, uniformity, reliability of responses produced, demonstrating that the EMBR PUF is effective and appropriate for secure and efficient PUF-based authentication.

Fig. 10 presents a comparison of the communication cost measured in bits of the various authentication and key-management protocols – DTLS [40], HIP [40], ICRT [40], MAP [40], HSC-IoT [40], PAS [40], and the proposed protocol. DTLS has the highest communication cost (≈3000 bits) since it requires a handshake and certificate exchange, which causes a significant amount of overhead in transmission cost. HIP and ICRT take the communication cost down to around 1100 bits and 900 bits, respectively. MAP reduces the cost to around 700 bits. HSC-IoT and PAS are both more efficient at around 600 bits. Meanwhile, the suggested system has the least communication cost at approximately 450 bits. This shows that there was a significant reduction in the message size that was communicated when using the proposed scheme, when compared to all existing alternatives. The proposed design is very efficient in communication cost and is well-suited to resource-constrained environments in IoT.

Table 5 shows examples of challenge-response pairs (CRPs) obtained from five different FPGA-based IoT devices that implemented the EMBR-PUF prototype described. The first device used was Device 1 (FPGA ID D794974), which was challenged with 038E59C4, EFA815F8, and 6D33FA8B, generating responses of 5F, CE, and F9, respectively. Device 2 (D795748) was challenged with the same challenges, but returned different responses, appropriately assigning responses of FB, 9C, and FD to each respective challenge. Device 3 (D795771) returned responses of D6, 7F, and BE for the same challenges as Device 2. Device 4 (D796263) produced B6, 6F, and D7, and lastly Device 5 (D796304) produced responses of BD, 9B, and AE for the same challenges. The differences in responses across different devices associated with the same challenge confirm the uniqueness property embedded in the EMBR-PUF. These challenge-response pairs also form the enrollment database that is used during the verification phase for IoT device authentication.

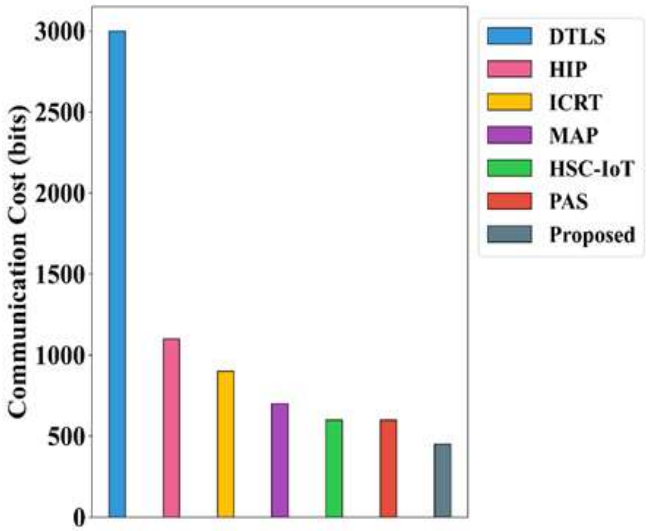

Fig. 10. Comparison of communication cost among existing schemes with the proposed protocol

Table 5. CRPs of the proposed EMBR PUF for five IoT devices on Artix-7 FPGA

IoT Device	Device ID (FPGA No.)	Challenge	Response
1	D794974	038E59C4	5F
		EFA815F8	CE
		6D33FA8B	F9
2	D795748	038E59C4	FB
		EFA815F8	9C

		6D33FA8B	FD
3	D795771	038E59C4	D6
		EFA815F8	7F
		6D33FA8B	BE
4	D796263	038E59C4	B6
		EFA815F8	6F
		6D33FA8B	D7
5	D796304	038E59C4	BD
		EFA815F8	9B
		6D33FA8B	AE

The comparison of the suggested protocol based EMBR PUF, as presented in Table 6, indicates that this PUF boasts about as well-balanced performance of uniqueness (48.65%), reliability (97.24%), and uniformity (47.21%) as those of the minimum acceptable values. Table 6 also shows that after adding obfuscation to challenge and response, uniformity (50.63%) gets improved significantly, however there is a slight improvement in the uniqueness (48.91) value whereas Reliability (97.22) remains nearly the same. The XOR-ROPUF [31] (49.40%, 99.8%, 50.76%) and standard ROPUF [33] (47.24%, 99.14%, 50.56%) measure slightly better reliability and uniformity, while the EMBR block performs consistently high on all three, with all values near acceptable, without strong tradeoffs. Inverter ROPUF [32] measures average, with (45.15%, 98%, 47.02%), and APUF [33] has very low uniqueness of 7.20% however claims good reliability (99.76%). The NC-PUF [35] versions report uniqueness values near perfect (~49.9%), reliability near perfect (~99%), but have no minimum uniformity values. BF-PUF [37] reports only 84.20% reliability. In general, the proposed protocol based EMBR PUF demonstrates the best performance, offering a well- balanced output with high reliability across all evaluated metrics.

Table 6. Performance comparison with state-of-the-art designs

PUF Types	**Uniqueness (%) (Ideal - 50%)**	**Reliability (%) (Ideal - 100%)**	**Uniformity (%) (Ideal - 50%)**
Proposed EMBR PUF Protocol with Obfuscation	48.91	97.22	50.63
Proposed protocol based EMBR PUF	48.65	97.24	47.21
XOR- ROPUF [31]	49.40%	99.8%	50.76%
Inverter ROPUF [32]	45.15%	98.0%	47.02%
ROPUF [33]	47.24%	99.14%	50.56%
APUF [33]	7.20%	99.76%	55.69%
NC-PUF [35]	49.9%	99.1%	-
NC-PUF [35]	49.7%	97.7%	-
BF-PUF [37]	-	84.20%	-

Table 7 provides a basis of comparison for communication overhead between existing IoT authentication protocols and the specified EMBR-PUF-based protocol. Communication overhead is accounted for in bits, transmitted between three entities during authentication: the User, the Gateway, and the Sensor Node. The total values represent all exchanged bits among these parties. The proposed EMBR-PUF protocol achieves a notably lower communication cost than previous schemes. Less communication overhead suggests the proposed EMBR-PUF approach utilized in this work is well-suited for resource-constrained applications in IoT, for which less data exchange on the network is advantageous for low-latency, energy-efficient and secure authentication.

Table 7. Comparison of Communication overhead (in bits) among existing IoT authentication protocols and the proposed EMBR PUF protocol

Protocol	User (bits)	Gateway (bits)	Sensor Node (bits)	Total (bits)
Li et al. [41]	704	512	256	1472
Challa et al. [42]	1536	1536	768	3840
Zhou et al. [43]	1536	1280	512	3328
Kumari et al. [44]	672	512	352	1536
Banerjee et al. [45]	800	608	640	2014
Srinivas et al. [46]	832	672	352	1856
Proposed protocol	160	160	130	450

5.3 Discussion of Experimental Results and Comparison with Existing Work

The experimental results demonstrate that the proposed EMBR-PUF achieves an average uniqueness of approximately 48% and reliability of around 97%, which are close to the ideal and acceptable ranges for practical PUF implementations. These values are consistent with those reported in existing literature for strong PUF designs.

The obtained FPGA-based EMBR-PUF metrics demonstrate that the proposed architecture maintains intrinsic PUF characteristics within the expected range for practical hardware implementations. Although the proposed architecture-aware obfuscation framework does not significantly alter the underlying hardware structure of the EMBR-PUF, the incorporation of nonce-assisted challenge transformation and response obfuscation improves the effective statistical balance and unpredictability of the generated authentication responses. Consequently, slight improvement in uniqueness and enhanced uniformity characteristics are observed, while reliability remain largely preserved due to the stability of the underlying bistable ring architecture.

It is important to note that the objective of the proposed work is not solely to improve conventional PUF metrics, but to achieve a balanced design that combines acceptable uniqueness and reliability with enhanced security and low hardware overhead. Unlike several existing approaches that require additional error correction codes or complex post-processing techniques to improve reliability, the proposed design maintains stable performance with minimal architectural complexity.

Additionally, the proposed technique greatly improves resistance to modeling and replay attacks by integrating the PUF design with an architecture-aware obfuscation mechanism at the protocol level. The suggested method differs from earlier studies that mostly concentrate on enhancing standalone PUF metrics because of its coupled hardware–protocol co-design. To further show how resilient the suggested design is under less-than-ideal operating settings, reliability analysis under various supply voltage conditions has been incorporated. These findings show that the EMBR-PUF performs consistently in a variety of environmental conditions, which makes it appropriate for real-world implementation in systems with limited resources.

Therefore, rather than concentrating only on slight improvements in particular PUF metrics, the importance of this study resides in achieving a favorable trade-off between performance, security, and implementation complexity.

A comparative analysis with previous PUF designs has been given in Table 6 to better elucidate the contribution. This analysis demonstrates that the suggested technique delivers competitive performance with increased protocol compatibility and reduced architectural complexity.

5.4 Extended Performance Evaluation

In addition to communication overhead, the performance of the proposed authentication scheme is evaluated in terms of latency, energy efficiency, and robustness under environmental variations.

Latency:

The suggested protocol mainly uses lightweight hash operations and provides a single-round authentication procedure. This lowers the total computational latency, in contrast to multi-step authentication techniques. Additionally, the EMBR-PUF's simple combinational logic (encoder, NOR gates, and multiplexer) helps to generate responses quickly.

Energy Consumption:

The proposed design is optimized for low energy consumption by avoiding complex operations such as error correction coding, iterative computations, or additional obfuscation hardware. As the existing architecture components are reused for both the functionality and security (example includes encoder and multiplexer), it minimizes the hardware overhead which makes the design suitable for resource-constrained IoT devices.

Robustness under Environmental Variations:

The reliability of the EMBR-PUF was evaluated under different supply voltage variations to examine its stability under non-ideal operating conditions. The obtained results demonstrate that the proposed architecture maintains consistent response behavior across multiple voltage levels, indicating its suitability for practical hardware deployment in resource-constrained environments.

Overall, the proposed authentication framework achieves an effective trade-off between communication overhead, computational complexity, and security robustness, thereby offering improved performance compared to existing approaches. A comparative analysis of these performance metrics is presented in Table 3.

5.5 Comparison of proposed protocol with Conventional Security Protocols

It should be noted that protocols such as DTLS and HIP are designed as general-purpose secure communication frameworks providing functionalities including session establishment, certificate management, key exchange, and encrypted end-to-end communication. Consequently, these protocols operate under different trust assumptions, computational requirements, and security objectives compared to lightweight PUF-based authentication systems.

In contrast, the proposed EMBR-PUF authentication framework primarily targets lightweight device authentication for resource-constrained IoT environments. The proposed approach focuses on reducing hardware overhead and computational complexity while improving resistance against replay and modeling attacks through architecture-aware challenge–response obfuscation. Therefore, the comparison with DTLS and HIP is intended mainly to provide a high-level perspective on communication and implementation overhead rather than a direct equivalence in security functionality or protocol scope.

To provide a more appropriate evaluation, the expanded comparison of security features of recent lightweight PUF-based authentication protocols operating under similar IoT-oriented assumptions and hardware-constrained deployment environments has been presented in Table 8.

Table 8. Security Features Based Analysis

Security Features	DTLS [40]	HIP [40]	MAP [40]	Ref [30]	Proposed EMBR PUF
Lightweight for IoT	✕	✕	-	✓	✓
Hardware-based Security	✕	✕	✕	✓	✓
Mutual Authentication	✓	✓	✓	✕	✓
Session Key Establishment	✓	✓	✓	✕	✓
Replay Attack Resistance	✓	✓	-	Partial	✓
MITM Attack Resistance	✓	✓	-	Limited	✓
Modeling Attack Resistance	✕	✕	✕	✓	✓
CRP Dependency Optimization	✕	✕	✕	✕	✓
Computational Overhead	High	High	Medium	Low	Low
Energy Efficiency	✕	✕	-	✓	✓
FPGA/Hardware Validation	✕	✕	✕	✕	✓

6.Applicability of the proposed authentication protocol to other PUF architectures

Although the proposed authentication protocol is implemented using the EMBR-PUF architecture, the protocol itself is not limited to this specific design. The proposed framework primarily relies on four key mechanisms: challenge transformation, response obfuscation, session-specific nonce integration, and lightweight cryptographic operations.

These mechanisms are generally compatible with strong PUF architectures that support challenge–response-based authentication. Therefore, the protocol can potentially be extended to other PUF types, including Arbiter PUF, XOR Arbiter PUF, Feed-Forward Arbiter PUF, Ring Oscillator PUF, and other delay-based PUF structures. Furthermore, the proposed architecture-aware obfuscation framework may also be adapted for certain memory-based PUF architectures,

such as SRAM PUF and Butterfly PUF, particularly in scenarios where challenge-dependent response generation or helper-data-assisted authentication mechanisms are employed.
In the proposed EMBR-PUF implementation, the obfuscation process incorporates internal architecture-dependent parameters such as encoder output and signal path information. For other PUF architectures, equivalent internal parameters or configurable structural features may be utilized to achieve similar architecture-aware obfuscation.
Therefore, the proposed protocol should be viewed as a generalized lightweight authentication framework that can be adapted to multiple PUF architectures, while the EMBR-PUF serves as the primary implementation example demonstrating its effectiveness.

7.CONCLUSION

This paper introduced a low-cost and scalable IoT authentication protocol based on an Encoder–Mux Based Bistable Ring Physical Unclonable Function (EMBR PUF). The protocol replaces traditional key storage and computationally intensive cryptographic operations with the intrinsic unclonable and unpredictable aspects of the EMBR PUF. The proposed protocol operates robustly, enabling secure device identification, mutual authentication, and session key creation while protecting against replay and modeling attacks. The protocol's implementation on an FPGA (Artix-7 evaluation board) achieved near-ideal performance on all key dimensions-related metrics, including 48.91% uniqueness, 97.22% reliability, and 50.63% uniformity. The protocol produced distinctly unique responses for identical challenges, validating strong device differentiation. Additionally, in terms of communication overhead, the proposed protocol had minimal communication latency of 450 bits, which positively outperformed existing efforts, including DTLS, HIP, MAP and other IoT authentication protocols. In addition to lightweight mutual authentication and session-key establishment, the proposed work introduces an architecture-aware challenge and response obfuscation mechanism integrated directly within the EMBR-PUF structure. Unlike conventional PUF-based authentication schemes that primarily rely on standard CRP verification, the proposed framework incorporates nonce-assisted challenge transformation, encoder-dependent signal processing, and path-aware response obfuscation to introduce hidden propagation dynamics and increased non-linearity into the authentication process. As a result, the generated authentication responses become significantly more resistant to replay attacks and machine-learning-based modeling attacks while preserving lightweight hardware complexity suitable for resource-constrained IoT environments. The proposed obfuscation framework therefore enhances both the security robustness and practical applicability of the EMBR-PUF-based authentication system. The findings collectively provide confirmation that the EMBR PUF protocol at the application-layer provides a strong, energy efficient and scalable hardware-assisted security of resource-constrained IoT-network paradigms. Future avenues of work may advance the EMBR PUF protocols to include group authentication, dynamic ephemeral key update protocols, and other edge-cloud security architectures.

REFERENCES

1. S. Reddy, A. K. Tyagi, K. Naithani, and S. Kumari. "Blockchain-empowered Internet of Things (IoTs) platforms for automation in various sectors," *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, Wiley, 2024, pp. 443–477, doi:10.1002/9781394303601.ch20.
2. O. A. Ibrahim, S. Sciancalepore, and R. D. Pietro. "MAG-PUFs: Authenticating IoT devices via electromagnetic physical unclonable functions and deep learning," *Computers & Security*, vol. 143, 2024. https://doi.org/10.1016/j.cose.2024.103905.
3. M. M. Rahman, F. Bouhafs, S. A. Hoseini, and F. D. Hartog. "UNSW HomeNet: A network traffic flow dataset for AI-based smart home device classification," *Computers & Industrial Engineering*, vol. 204, 2025. https://doi.org/10.1016/j.cie.2025.111041.
4. S. Yu, F. Carroll, and B. L. Bentley. "Insights Into Privacy Protection Research in AI," *IEEE Access*, vol. 12, pp. 41704–41726, 2024. doi:10.1109/ACCESS.2024.3378126.
5. Munir, I. A. Sumra, R. Naveed, and M. A. Javed. "Techniques for authentication and defense strategies to mitigate IoT security risks," *Journal of Computing & Biomedical Informatics*, vol. 7, no. 1, pp. 377–388, 2024. doi:10.13140/RG.2.2.31448.71684.
6. R. Khan, H. B. Eldeeb, B. Mefgouda, O. Alhussein, H. Saleh, and S. Muhaidat. "Encoder decoder-based Virtual Physically Unclonable Function for Internet of Things device authentication using split-learning," *Computers & Security*, vol. 148, 2025. https://doi.org/10.1016/j.cose.2024.104164.
7. K. Hussain, A. R. Rahmatyar, B. Riskhan, Md. A. Ullah Sheikh, and S. R. Sindiramutty. "Threats and vulnerabilities of wireless networks in the Internet of Things (IoT)," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, pp. 1–8, IEEE, 2024.
8. M. Sheikh, Md. R. Islam, M. H. Habaebi, S. A. Zabidi, A. R. B. Najeeb, and A. Kabbani. "Integrating Physical Unclonable Functions with Machine Learning for the Authentication of Edge Devices in IoT Networks," *Future Internet*, vol. 17, no. 7, Art. 275, 2025. https://doi.org/10.3390/fi17070275.
9. S. W. Shende, J. V. Tembhurne, and N. A. Ansari. "Deep learning based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions," *Multimedia Tools and Applications*, vol. 83, no. 28, pp. 71451–71493, 2024. https://doi.org/10.1007/s11042-024-18350-5.
10. G. Krzysztof. "Security primitives for memoryless IoT devices based on Physical Unclonable Functions and True Random Number Generators," *Scientific Reports*, vol. 14, no. 1, Art. 24060, 2024. https://doi.org/10.1038/s41598-024-75373-6.

11. F. Amsaad, O. Ahmed, Md. Y. Niamat, A. Razaque, S. Kose, M. Mahmoud, W. Alasmary, and F. Alsolami. "Enhancing the performance of lightweight configurable PUF for robust IoT hardware-assisted security," *IEEE Access*, vol. 9, pp. 136792–136810, 2021. doi:10.1109/ACCESS.2021.3117240.
12. Z. Wang. *High-Performance Process-in-Memory Architectures Design and Security Analysis*. PhD Thesis, Electrical and Computer Engineering, University of Michigan, 2024.
13. Felicetti, A. Rullo, A. Tagarelli, and D. Saccà. "IoT Device Security Using PUF-Based Tags: A Lightweight Protocol for Preventing Hardware Substitution," in *Future of Information and Communication Conference*, pp. 607–624, Springer Nature Switzerland, 2025.
14. V. K. V. V. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos. "QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things," in *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, pp. 296–301, 2023. doi:10.1109/iSES58672.2023.00067.
15. P. Zhang, Y. Yang, Y. Zheng, and Y. Sun. "Multiplexed Internet of Things Data Transmission and Visualization Utilizing Wireless LAN Authentication and Privacy Infrastructure Protocol in Smart Factories," *Sensors*, vol. 25, no. 10, Art. 3134, 2025. https://doi.org/10.3390/s25103134.
16. Alotaibi, H. Aldawghan, and A. Aljughaiman. "A review of the authentication techniques for Internet of Things devices in smart cities: opportunities, challenges, and future directions," *Sensors*, vol. 25, no. 6, Art. 1649, 2025. https://doi.org/10.3390/s25061649.
17. S. G. Aarella, V. P. Yanambaka, S. P. Mohanty, and E. Kougianos. "Fortified-Edge 2.0: Advanced Machine-Learning-Driven Framework for Secure PUF-Based Authentication in Collaborative Edge Computing," *Future Internet*, vol. 17, no. 7, Art. 272, 2025. https://doi.org/10.3390/fi17070272.
18. K. Khalil, H. Idriss, T. Idriss, and M. Bayoumi. "Lightweight hardware security and physically unclonable functions," *Journal of Hardware Security*, 2025.
19. Al-Meer and S. Al-Kuwari. "Physical unclonable functions (PUF) for IoT devices," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–31, 2023. https://doi.org/10.1145/3591464.
20. Cirne, P. R. Sousa, J. S. Resende, and L. Antunes. "Hardware Security for Internet of Things Identity Assurance," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1041–1079, 2024. doi:10.1109/COMST.2024.3355168.
21. T. Naing and M. Masahiro. "Secure PUF-Based Authentication Systems," *Sensors*, vol. 24, no. 16, Art. 5295, 2024. doi:10.3390/s24165295.
22. K. Sasikumar and S. Nagarajan. "Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 392–402, 2025. doi:10.1109/OJCS.2025.3538557.
23. M. Grossi, M. Omaña, C. Metra, and A. Acquaviva. "Novel Physical Unclonable Function Implementation for Microcontrollers and Field Programmable Gate Arrays," *IEEE Access*, vol. 13, pp. 55970–55983, 2025. doi:10.1109/ACCESS.2025.3555438.
24. U. M. Mbachu, R. Fatima, A. Sherif, E. Dockery, M. Mahmoud, M. Alsabaan, and K. Khalil. "Hardware Acceleration-Based Privacy-Aware Authentication Scheme for Internet of Vehicles Using Physical Unclonable Function," *Sensors*, vol. 25, no. 5, Art. 1629, 2025.
https://doi.org/10.3390/s25051629.
25. V. Nyangaresi, A. A. Al Rababah, G. K. Yenurkar, R. Chinthaginjala, and M. Yasir. "Anonymous authentication scheme based on physically unclonable function and biometrics for smart cities," *Engineering Reports*, vol. 7, no. 1, pp. 1–15, 2025. doi:10.1002/eng2.13079.
26. Williamson, K. A. Simpson, D. J. Paul, and D. P. Pezaros. "Quantum Well-Based Physical Unclonable Functions for IoT Device Attestation," *IEEE Access*, vol. 13, pp. 115079–115089, 2025. doi:10.1109/ACCESS.2025.3583881.
27. S. K. Chandrasekaran and V. A. Rajasekaran. "Blended clustering energy efficient routing and PUF based authentication in IoT enabled smart agriculture systems," *Scientific Reports*, vol. 15, no. 1, Art. 24682, 2025. https://doi.org/10.1038/s41598-025-07917-3.
28. J. Zhang, C. Shen, Z. Guo, Q. Wu, and W. Chang. "CT PUF: Configurable Tristate PUF against Machine Learning Attacks for IoT Security," *IEEE Internet of Things Journal*, 2021. doi:10.1109/JIOT.2021.3090475.
29. M. Thirumoorthi, M. Jovanovic, M. Mirhassani, and M. Khalid. "Design and Evaluation of a Hybrid Chaotic-Bistable Ring PUF," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 11, pp. 1912–1921, 2021. doi:10.1109/TVLSI.2021.3111588.
30. K. Annapurna and D. Koppad. "A Lightweight Hardware Secure and Reliable Framework using Secure and Provable PUF for IoT Devices against the Machine Learning Attack," *International Journal of Circuits, Systems and Signal Processing*, vol. 16, pp. 699–709, 2022. doi:10.46300/9106.2022.16.86.
31. Oun and M. Niamat. "PUF-Based Authentication for the Security of IoT Devices," in *2023 IEEE International Conference on Electro Information Technology (eIT)*, pp. 67–70, 2023. doi:10.1109/eIT57321.2023.10187363.

32. M. Mustapa, M. Y. Niamat, A. P. Deb Nath, and M. Alam. "Hardware-Oriented Authentication for Advanced Metering Infrastructure," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1261–1270, 2018. doi:10.1109/TSG.2016.2582423.

33. Maiti, V. Gunreddy, and P. Schaumont. "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design with FPGAs*, pp. 245–267, Springer, 2013. https://doi.org/10.1007/978-1-4614-1362-2_11.

34. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair. "The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 134–141, 2011. doi:10.1109/HST.2011.5955011.
35. G. Li, J. Zhou, P. Wang, X. Ma, B. Chen, and X. Shao. "A 154 F² Bistable Physically Unclonable Function with Independent Responses Based on Dynamic Division Multiplexing Technique," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 33, no. 11, pp. 3156–3165, 2025. doi:10.1109/TVLSI.2025.3592933.
36. Han, Jiho, and Changyong Shin. "An Extensive PUF of Bistable Rings Feed-forward Chains with Lightweight Secure Architecture for Enhanced ML Attack Resistance," *Journal of Semiconductor Technology and Science*, vol. 24, no. 2, pp. 76–83, 2024. https://doi.org/10.5573/JSTS.2024.24.2.76.
37. Z. Huang, F. Zeng, Y. Chi, Y. Lin, Y. Lu, H. Liang, J. Bian, Y. Ouyang, T. Ni, and X. Wen. "BF PUF: A Modeling Attack-Resistant Strong PUF Based on Bent Functions," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 33, no. 8, pp. 2299–2311, 2025. doi:10.1109/TVLSI.2025.3569587.
38. J. Zhenjie, S. Chen, and L. Yan. "Low-overhead XOR Multi-PUF against machine learning attacks," *Microelectronics Journal*, vol. 141, 2023.
https://doi.org/10.1016/j.mejo.2023.105964.
39. P. Lokhande and S. Nakhate. "Modeling Attack Resistant Encoder-Mux Based Bistable Ring PUF," *Journal of Integrated Circuits and Systems*, vol. 20, no. 2, pp. 1–9, 2025.
https://doi.org/10.29292/jics.v20i2.948.
40. M. A. Muhal, X. Luo, Z. Mahmood, and A. Ullah. "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things," in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 160–165, 2018. doi:10.1109/SmartIoT.2018.00037.
41. S. Li, T. Zhang, B. Yu, and K. He. "A Provably Secure and Practical PUF-Based End-to-End Mutual Authentication and Key Exchange Protocol for IoT," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5487–5501, 2021. doi:10.1109/JSEN.2020.3028872.
42. S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo. "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017. doi:10.1109/ACCESS.2017.2676119.
43. L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu. "Lightweight IoT based authentication scheme in cloud computing circumstance," *Future Generation Computer Systems*, vol. 91, pp. 244–251, 2019. https://doi.org/10.1016/j.future.2018.08.038.
44. F. Wu, L. Xu, S. Kumari, and X. Li. "An improved and anonymous two-factor authentication protocol for healthcare applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23, no. 2, pp. 195–205, 2017. https://doi.org/10.1007/s00530-015-0476-3.
45. S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park. "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," *IEEE Access*, vol. 7, pp. 85627–85644, 2019. doi:10.1109/ACCESS.2019.2926578.
46. J. Srinivas, A. K. Das, M. Wazid, and N. Kumar. "Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133–1146, 2020. doi:10.1109/TDSC.2018.2857811.
47. S. Khalfaoui, J. Leneutre, A. Villard, I. Gazeau, J. P. Ma, and P. Urien. "Security Analysis of Machine Learning-Based PUF Enrollment Protocols: A Review," *Sensors*, vol. 21, no. 24, Art. 8415, 2021. doi:10.3390/s21248415.
48. Yang, Y. Zhang, W. Cao, Z. Tong, and Z. He. "A Lightweight and Practical Anonymous Authentication Protocol Based on Bit-Self-Test PUF," *Electronics*, vol. 11, no. 5, Art. 772, 2022. https://doi.org/10.3390/electronics11050772.
49. Y. Jameel and M. H. Hasan. "A Unique PUF Authentication Protocol Based Fuzzy Logic Categorization for Internet of Things (IoT) Devices," pp. 246–252, 2023. doi:10.1145/3587828.3587865.
50. Sajadi, A. Shabani, and B. Alizadeh. "DC-PUF: Machine learning-resistant PUF-based authentication protocol using dependency chain for resource-constrained IoT devices," *Journal of Network and Computer Applications*, vol. 217, Art. 103693, 2023. doi:10.1016/j.jnca.2023.103693.
51. J. Xianji, N. Lin, L. Zhongwei, W. Jiang, Y. Jia, and L. Qingyang. "A Lightweight Authentication Scheme for Power IoT Based on PUF and Chebyshev Chaotic Map," *IEEE Access*, 2024. doi:10.1109/ACCESS.2024.3413853.
52.. Zhuang and L. Gaoxiang. "A lightweight PUF-based authentication protocol," arXiv, 2024. doi:10.48550/arXiv.2405.13146.
53. T. Naing and M. Masahiro. "Secure PUF-Based Authentication Systems," *Sensors*, vol. 24, no. 16, Art. 5295, 2024. doi:10.3390/s24165295.