Analysis and Research on the Application of Lightweight Physical Unclonable Function (PUF) Authentication Protocol for IoT Terminals

Ziqi Zhao *

Canmbrideg International School Litai College, Shanghai, China

* Corresponding Author Email:434267583@qq.com

Abstract. In this paper, we study a computation-efficient PUF-based authentication protocol suitable for resource-constrained IoT applications. Latency, energy consumption, and security trade-offs are critically important for the efficient and secure operation of IoT and the study addresses the same. We compare the performance characteristics of various PUF implementations and discuss hardware and software optimization techniques. The objective of this study is to conduct an extensive analysis to propose optimized PUF-based authentication protocols, in terms of performance, security, and cost for dedicated IoT applications. The outcomes will benefit both researchers and practitioners in understanding the nuances of PUF-based authentication protocols for various IoT applications, facilitating the design of secure and resource-efficient IoT ecosystems.

Keywords: PUF, loT terminals, authentication protocol.

1. Introduction

In 1995, Bill Gates published a book called The Road Ahead, which mentioned “The Internet of Things”. It was not taken seriously due to the limited development of Wi-Fi and hardware.

Since 2000 when Wi-Fi and Bluetooth evolved and have mature protocols (e.g.: ZigBee) of low energy-cost wireless connection technology. After that, with the assistance of techniques like cloud computing, implementation of IPv6, edge computing, and Artificial Intelligence, the Internet of Things is booming, and is widely used in fields such as household, medical care, and industry

Since the attack types keep emerging, and the global embodied artificial intelligence (AI) and artificial intelligence of things (AIoT) market experiences rapid growth, there is an increasing demand for edge devices that are low-power, lightweight and safe [1]. The security problems for embedded processors will become more and more severe. Here are the three primary security threats it faces. Tampering attack 2. 3. code injection. To further improve the security protection of the security processor, the existing mainstream solutions of the security processor include XOM architecture, SPEF framework Garbled CPU architecture, etc. In addition to these frameworks, a novel technique for protection is known as PUF, an acronym for physical unclonable functions. It’s a hardware security technique based on the physical components of hardware like CPU and GPU. It leverages the chance variance between the chips, and creates an exclusive “digital fingerprint”.

PUF is widely used in many aspects, attributed to its properties of random, anti-physical attack, low cost, and lightweight, which made it incredibly suitable for the embedded systems in the Internet of Things (IoT). It is mainly used in the generation of secret keys, Intellectual property protection, and verification of identity, for instance, smart cards and sensors.

This article intends to compare the optimal encryption methods, improve the security authentication efficiency of IoT terminals, promote the application of IoT in various fields, identify the shortcomings faced by PUFs, and make reasonable predictions for the future.

2. Analysis of Principles

PUF (Physical Unclonable Function) provides a unique digital fingerprint a stably secure technology that uses microscopic physical randomness in a hardware manufacturing step. The key techniques are to, extract the uncopiable characters while manufactured, including the fluctuation of

the threshold voltage of the transistor, the deviation of resistance of the wire, and the randomness of material in microcosmic, forming a projection of uncontrived physical diversity to the digital world as a special sign.

Here are some underlying level physical differences.

Material inhomogeneity: Doping concentration, crystal defects, etc. in semiconductor materials lead to differences in transistor threshold voltage (Vth) and carrier mobility.

Process deviation: Minor errors in manufacturing steps such as lithography and etching lead to random structural variations (e.g., gate length deviation).

Quantum effects: In nanoscale devices, quantum phenomena such as tunneling current introduce additional randomness.

The PUF's process can be broadly divided into the following three stages:1. The challenge,2. The response,3. The verification [2].

Step 1: The challenge

The first one is the physical excitation. The user sends an electric signal (usually a binary) generated by the system (such as a random number in 64-bit or 128-bit) via a digital interface to the PUF hardware. The PUF Circuit activates once it receives the challenge signal, and the lining functions to multiple paths in corresponding likenesses to amplify the physical differences, especially the route differences discrepancy through monitoring the fluctuation and electric potential difference between the gate and electric transistor.

Challenge signal types:

Numerical Challenge: Input a binary sequence (such as a random number or a specific pattern) and control the signal path through a multiplexer (such as an arbiter PUF).

Simulation challenge: Adjusting voltage, temperature, or timing parameters (such as dynamic voltage PUF, and temperature sensing PUF).

Mixed Challenge: Combining digital and analog excitation to enhance response complexity (such as PUF based on ring oscillators).

Step 2: The response

Then is the response generation. The challenge signal interacts with the internal structure of PUF, triggering random responses such as voltage fluctuations and delay differences. Each PUF instance generates a unique response (usually a binary string) to the same challenge due to physical differences.

Signal competition: In the arbiter PUF, the difference in signal propagation delay between two paths leads to metastable competition, resulting in the final output of 0 or 1.

Physical disturbance: forcing measurable changes in material properties (such as electron mobility) by altering environmental parameters (such as voltage fluctuations). Due to environmental interference, there may be slight fluctuations in the response, which requires stable output through error correction coding (such as LDPC, and BCH codes). The processed response can be used as a key or identifier to ensure consistent output under multiple identical challenges.

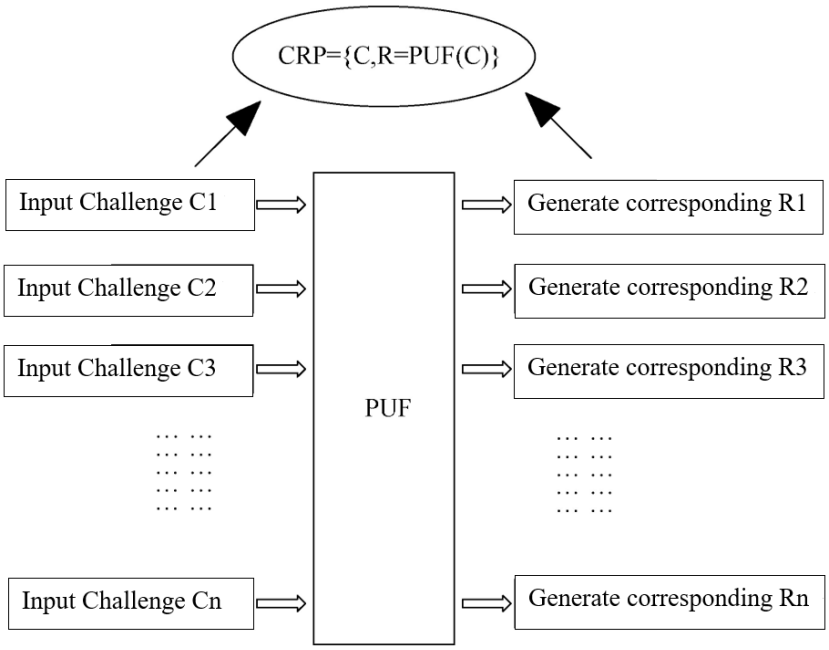

Figure 1. PUF Generation of challenge-response [3]

Step 3: Response verification

Last is the response verification, there are mainly two kinds: the local verification and the remote verification. The device uses a Fuzzy Extractor, refactoring the stable secret key.

3. Classification of PUF

Based on the CRP space, PUFs can be categorized into weak PUFs and strong PUFs. Weak PUFs have a limited number of CRPs that are linear or polynomial to the number of PUF cells, while strong PUFs can support an exponentially large CRP space. Therefore, in addition to realizing weak PUF applications, strong PUFs can take advantage of the large CRP space for deployment in advanced cryptographic protocols such as device authentication and multi-party computation [4].

The nonelectronic PUF.

Other types of Nonelectronic PUF are based on optics, mechanics, or chemical characteristics. When laser lighting coatings with randomly dispersed nanoparticles surface material in reactive and transmissive light excitation phase, scattering mode, or reflected light mode, the scattered light intensity changes will differ from the scattering phase spectrum according to the microstructure of the material due to differences in the microstructure. Optical features like spot distribution or pixel spectral characteristics are acquired by all sensors and mapped to digital responses. This property of exposure is utilized by the CMOS component in a camera. Although the non-magnetic PUF can protect against electromagnetic interference, has high physical unlovability, and is designed for harsh environments, it is very difficult to integrate and is often used only in military facilities.

The mechanical PUF

This kind of PUF is based on the mechanical characteristics such as resonance frequency, deformation response, or sound wave propagation mode of different microelectromechanical systems (MEMS) or microstructures for instance microcantilever beams, vibrating structures, and generates response through frequency detection.

This mode of PUF has a low production cost and can easily detect the physical damage of the microchips, due to these features, this kind of PUF can often be noticed in industrial systems.

Chemical PUF

It utilizes the random distribution or reaction characteristics differences of chemical materials such as polymers and nanoparticle mixtures. For example, the diffusion rate of specific chemical reagents or the color change of reaction products can serve as a response source.

It’s often designed by Coating chemical substances on the surface of chips and detecting random patterns of reaction products through electrochemical sensors.

The chemical PUF has strong resistance against reverse engineering and is suitable for a disposable token. Attribute to its high environmental sensitivity, it can be almost only manipulated in medicine anti-counterfeiting [5].

Optical PUF

Principle:

Optical PUFs utilize uncontrollable physical deviations in the material manufacturing process (such as random distribution of microstructures, optical scattering characteristics, etc.) to generate unique and unpredictable responses through optical signal excitation. Its core advantages lie in non-contact reading, high encoding capacity, and environmental stability [6].

Implementation method and type:

1. Total internal reflection type:

For example, the scheme proposed by Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, uses polymer beads to destroy the total internal reflection condition, and combines alumina protective layer to isolate environmental interference, so as to improve response contrast and stability.

Features: Strong mechanical, thermal, optical, and chemical stability, supporting portable certification (such as handheld microscopes and low-power lasers).

2. Perovskite phase separation type:

By utilizing the reversible phase separation phenomenon of mixed halide perovskite materials, the excitation light power density can be adjusted to generate unpredictable photoluminescence spectra.

Features: Adjustable key size, large encoding space, high security.

Quantum PUF

Principle:

Quantum PUF is based on the principles of quantum mechanics, such as entanglement and superposition, and generates a unique signature by measuring the quantum correlation (such as frequency and arrival time) between entangled photons and optical chaotic structures. Its security relies on the quantum unclonable theorem to resist quantum computer attacks.

Implementation method:

Entangled Photon Protocol:

Generate entangled photon pairs, input them separately into two devices (such as Alice and Bob's PUFs), and measure the correlation of the output (such as joint spectral intensity or time intensity).

Publicly store pre-measured quantum correlation signatures (such as ab, ac, bc), and verify them by comparing the real-time measurement results with the signatures during authentication.1

In addition to nonelectro PUF, there is electro PUF as well, it produces a response using the stochastic variation of resistance values in resistance networks, like polysilicon resistors, and metal line resistors. For example, by gauging the resistance ratio through a voltage divider circuit and quantifying that into digital bits. This type of PUF has a simple structure and high noise resistance, so they are often used in situations that require repetitive verification.

The most frequently used types are the digital-circuit PUF and Analog Circuit PUF, the first kind amplifies the randomness of the manufacturing process through digital logic structures, it can be divided into two categories: memory PUFs and delay propagation PUFs.

As for the Analog Circuit PUF, it is mainly divided into two types: Ring Oscillator PUF, which has a relatively simple design, is easy to implement, and offers a large space of Challenge-Response Pairs (CRPs), allowing it to be classified as a strong PUF.

And the resistance PUF. The principles of these two are similar to the previous, both based on comparing the frequency difference between two circuits to generate response bits.

4. Typical Protocol Process

1. Registration stage:

The device collects the excitation response of PUF and extracts stable features (such as generating keys through a fuzzy extractor).

The server stores the hash value or encrypted template of CRP to avoid storing sensitive information in plaintext.

2. Certification phase:

Challenge distribution: The server sends random numbers (Nonce) and incentives to the device.

Response generation: The device generates a response through PUF and uses error correction techniques to generate a key.

Dynamic signature: The device uses random numbers and challenge signatures to return the signature to the server.

Verification and key negotiation: The server verifies the legitimacy of the signature and generates the session key through a key derivation function (KDF).

Anti attack mechanism

Anti-modeling attacks: Using nonlinear PUF structures (such as lightweight obfuscation circuits) or dynamic CRP selection strategies to increase the difficulty of adversaries building mathematical models.

Prevent replay attacks: Introduce timestamps or random nonce to ensure the freshness of each authentication.

Forward security: The session key is generated based on temporary Nonce, and long-term key leakage does not affect historical communication security.

5. The Analysis of PUF Security under Different Attack Scenarios

The security and privacy of IoT devices are crucial due to their diversity, distribution, and ease of access. The inherent trade-off between hardware capabilities and security in limited-resource systems makes them vulnerable to different types of attacks, including physical attacks [7].

1. Physical attack

The PUF operation Machine learning methods can be used by attackers to utilize information leaked through side channels for modeling, which can reduce the number of CRP (Challenge Response Pair) significantly for the attack. In addition, CRP is used to fit the reliability analysis with few samples, while mixed attacks on side channels and machine learning give a significant threat against the arbiter PUF.

Fault injection attack: Using external interference (such as voltage fluctuations) to cause PUF response errors, and then modeling based on fault information. Noninvasive fault injection is the mainstream method, but the tamper-proof properties of PUF may limit its effectiveness.

Machine learning attacks

The attacker learns the response pattern of PUF by collecting a large number of CRP training models (such as neural networks). Research has shown that even if PUF designs have nonlinear structures such as XOR PUFs, they can still be modeled with high precision.

The process of attacks can be divided into 4 main steps

1. CRP collection stage: Attackers obtain 10^4-10^6 sets of CRPS through physical contact or protocol interaction (such as through replay attacks or device debugging interfaces).

2. Feature engineering: Perform binary bit segmentation on the challenge (C) and noise filtering (such as mean filtering) on the response (R).

3. Model selection: Use logistic regression (LR), support vector machine (SVM), or deep neural network (DNN).

4. Training optimization: Use cross-entropy loss function and Adam optimizer to prevent overfitting through the early stopping method.

The experimental case refers to R ü hair et al, 2010):

Target PUF type: Arbitrator PUF (64-bit challenge, 1-bit response)

Dataset: 50000 sets of CRPS (80% training, 20% testing)

Model structure: 3-layer MLP (64-32-1, ReLU activated)

Result: The accuracy of the test set reached 98.2%, proving that strong PUFs can be efficiently modeled [8].

Protocol layer attacks

Bad PUFs: Attackers maliciously construct PUF devices to compromise the security of the protocol. For example, tampering with the internal structure of PUF to bypass authentication protocols.

PUFs inside PUFs: By embedding PUF structures to hide the true response, traditional protocols are unable to detect attacks. The existing protocol has vulnerabilities under such attacks and requires the introduction of enhanced mechanisms such as interactive hashing.

6. Defense Measures

1. Structural enhancement

Introducing nonlinear structures (such as XOR PUF) or dynamically adjusting input excitations (such as feedforward loops) increases modeling difficulty.

Cross-path design (such as output crossover) can expand the signal delay range and improve response randomness.

Nonlinear PUF Design Examples:

1. Nonlinear PUF based on SRAM: Utilizing the threshold voltage difference of SRAM cells, the randomness of bit flipping is enhanced through nonlinear amplification circuits (such as Schmitt triggers).

2. Chaotic PUF based on ring oscillator: A ring oscillator is formed by cross-coupling inverters, and its frequency is highly sensitive to process deviations and exhibits chaotic behavior.

3. Nonlinear Arbitrator PUF: Introducing a nonlinear delay module (such as a varactor diode) based on the traditional arbiter PUF, so that the delay difference has a nonlinear relationship with the challenge input.

4. Confusion and dynamism

Hide real challenges or responses, such as reducing side channel leakage through masking techniques.

Combining PUF with other security mechanisms to actively disable upon detecting an attack.

There has already been a generous amount of encryption algorithms, but PUF has its unique advantage.

7. Comparison of advantages and disadvantages with other encryption methods

The core advantages of PUF:

1. Non Clonability

PUF generates unique identifiers using random differences in physical manufacturing processes, such as silicon process deviations and material properties, which cannot be accurately replicated. Traditional encryption relies on pre-stored keys, which are easily stolen or cloned.

2. No need for key storage

PUF dynamically generates keys without storing fixed keys in the chip, avoiding the risk of key leakage in traditional encryption (such as reading keys stored in EEPROM/OTP through physical attacks).

3. Anti-tampering ability

The response of PUF is bound to the physical structure, and any tampering behavior (such as temperature and voltage changes) will result in response failure, enhancing system security.

Traditional encryption relies on software or fixed hardware and is vulnerable to side-channel attacks (such as power consumption analysis).

4. Low power consumption and low cost

Some PUFs (such as SRAM PUFs) do not require additional circuits, have low integration costs, and are suitable for low-power devices (such as IoT sensors). Traditional encryption requires additional storage units or complex algorithms, increasing energy consumption and costs.

5. Dynamic key generation

PUF generates a new key ("one key at a time") every time it responds to a challenge and combines it with national encryption algorithms (such as SM7) to achieve dynamic encryption, which is more secure than traditional static keys.

Specific comparison

Table 1. Comparison of PUF with other mainstream encryption protocols/algorithms

Aspects	PUF	Hash/Symmetric Encryption/Digital Signature
Security Fundamentals	Non cloning and randomness based on physical structure	Based on mathematical problems such as large integer decomposition, discrete logarithm, etc
Key storage	No need for external storage of keys (keys implicitly exist in the physical structure)	Need to store keys (such as security chips, cryptographic modules)
Dynamic feature	Response depends on environmental conditions such as temperature and voltage	Each output may be different, with a fixed key and high output certainty
Resource consumption	Lightweight (requiring only physical structure and simple circuitry)	Requires complex computing units (such as CPU, DSP) or dedicated hardware
Resistance to physical attacks	Physical tampering may lead to PUF failure	Physical security relying on key storage (such as tamper proof encapsulation)

1. Comparison with Hash Functions

PUF advantages:

Able to generate unique identifiers (such as device fingerprints) directly without precomputing hash values.

The response is environment-dependent and difficult to be attacked by static modeling.

2. Comparison with symmetric encryption (such as AES)

No risk of key leakage (no need to store keys).

Suitable for resource-constrained devices such as Radio Frequency Identification tags.

3. Compared to Asymmetric Encryption (such as RSA)

No need for public-private key generation and management, avoiding key custody issues.

Potential to resist quantum attacks (relying on physical properties rather than mathematical principles).

Some schemes combine multiple encryption methods to achieve a stronger encryption intensity.

For instance, PUF+Hash, this combination uses PUF to generate a unique device identifier, which is hashed and used for quick verification.

In industrial control systems, we use PUF+digital signature as the coding method, as PUF provides device identity and digital signature ensures message nonrepudiation.

Practical Application of PUF Authentication Protocol:

1. Medical implantable devices [9]

Case: Safe Communication of Cardiac Pacemakers

Technical solution:

Generate device identifier (128 bits) using RO PUF.

Derive session keys through lightweight protocols such as HKDF-SHA256.

2. IoT sensor network [10] [11]

Application scenario: Industrial environment monitoring (such as temperature/humidity sensors)

Deployment plan:

Microchip ATECC608B chip: a hardware security module integrated with PUF, used for node identity authentication and data encryption.

Workflow:

When the node starts, PUF generates a unique key, then the key is used to sign sensor data (ECDSA).

The gateway verifies data integrity through pre-registered PUF responses.

Overall, the PUFs are commonly used in sensors, most of them have small physical dimensions, insufficient storage resources, high computational costs limited resources, and other situations[12].

8. Conslusion

PUF provides a solution that traditional encryption cannot replace in the fields of anti-counterfeiting, key management, and device authentication through its physical layer security features, especially suitable for scenarios that require high security and low power consumption. And it can promote the development of the IoT in many aspects. In the blockchain area, can provide physical random numbers for encryption algorithms to enhance the entropy value of key generation, which can ensure Blockchain node authentication to prevent Sybil attacks.

Although PUF has outstanding advantages, there are still problems that need to be solved in aspects of environmental sensitivity (temperature drift, and voltage fluctuation), reliability (stability after multiple responses), and resistance to machine learning attacks. With new features like stability improvement, ECC improvement, blockchain hardware security applications, and so on. PUFs are expected to apply to many practical fields, from data-sensitive fields such as healthcare and finance, digital identity management, and Privacy Protection and Data Sharing.

The most anticipated application area is a combination with blockchain technology. The integration of PUF and blockchain provides a "hardware level security decentralized trust" solution for fields such as the Internet of Things, supply chain, and finance, with significant advantages in device identity authentication, data privacy protection, and asset certification. With the standardization of technology and policy support (such as the standardized integration of commercial cryptography and blockchain), its application will further expand to more real economy scenarios.

References

[1] Yue, W., Wu, K., Li, Z., et al. Physical unclonable in-memory computing for simultaneous protecting private data and deep learning models. Nat Commun 16, 1031 (2025).

[2] Zhang Yuefei, Yuan zheng, et al. A lightweight authentication protocol based on PUF for power IoT devices. Application Research of Computers ISSN 1001 - 3695, CN 51 - 1196/TP

[3] Zhang Yuefei, Yuan zheng, et al. Comparative analysis of PUF-based secure authentication protocols Journal of Beijing Electronic Science and Technology Institute 1672 - 464X (2024) 3 - 82 - 94.

[4] Sukhrob Abdulazhanov, Guo, X., Müller, F., et al. Demonstration of high-reconfigurability and low-power strong physical unclonable function empowered by FeFET cycle-to-cycle variation and charge-domain computing. Nat Commun 16, 189 (2025).

[5] K. Bonawitz, et al. PUF-Secured Federated Learning for Medical Image Analysis. AAAI Conference on Artificial Intelligence, **2023**.

[6] C. Chen. Photonic Physical Unclonable Functions Using Silicon Microresonators. Optical Fiber Communication Conference (OFC), **2022**.

[7] Abulibdeh, E., Saleh, H., Mohammad, B., et al. Kernel-based response extraction approach for efficient configurable ring oscillator PUF. Sci Rep 15, 5938 (2025).

[8] Ulrich Rührmair, Jan Sölter, Frank Sehnke. Modeling Attacks on Physical Unclonable Functions. ACM Conference on Computer and Communications Security (CCS), **2010**.

[9] NISTIR 8309: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.

[10] Yansong Gao, Dieyu Chen, Feng Zhou, et al. A PUF-Based Unified Identity and Key Generation Algorithm for IoT Devices. IEEE Internet of Things Journal, **2020**.

[11] Fareena Saqib, Jaya Dofe, Jim Plusquellic. Quantum Threats and Countermeasures in Hardware Security: A Survey. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), **2022**.

[12] Wang Xiong et al. Lightweight Multi Gateway Authentication Protocol Based on PUF in Wireless Sensor Networks Application Research of Computers ISSN 1001 - 3695, CN 51 - 1196/TP.