A Lightweight Anonymous Identity Authentication Scheme for the Internet of Things

Zhengdong Deng[1], Xuannian Lei[2], Junyu Liang[3], Hang Xu[4], Zhiyuan Zhu[5], Na Lin[6], Zhongwei Li[7]*, Jingqi Du[8]
Chuxiong Power Supply Bureau, Yunnan Power Grid Co., Ltd., Chuxiong, China[1, 2, 4, 5]
Yunnan Electric Power Research Institute, Yunnan Power Grid Co., Ltd., Kunming, China[3]
School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin, China[6, 7]
Industrial Control Expansion Department, CLP Great Wall Internet System Application Co., Ltd., Beijing, China[8]

***Abstract*—With the rapid growth of Internet of Things (IoT) devices, many of which are resource-constrained and vulnerable to attacks, current identity authentication methods are often too resource-intensive to provide adequate security. This paper proposes an efficient identity authentication scheme that integrates Physical Unclonable Functions (PUFs), Chebyshev chaotic maps, and fuzzy extractors. The scheme enables mutual authentication and key agreement without the need for passwords or smart cards, while providing effective defense against various attacks. The security of the proposed scheme is formally analyzed using an improved BAN logic. A comparison with existing related protocols in terms of security features, computational overhead, and communication overhead demonstrates the security and efficiency of the proposed scheme.**

Keywords—Internet of Things; identity authentication; Physical Unclonable Functions; fuzzy extractors; chaotic maps

I. Introduction

As science and technology continue to progress, the Internet of Things (IoT) has found broad applications in areas such as smart homes, smart energy, industrial production, and healthcare. In this interconnected world, the number of IoT-connected devices is growing at an exponential rate. These devices are typically resource-constrained, widely distributed, and susceptible to various attacks, including physical attacks, machine learning modeling attacks, replay attacks, and man-in-the-middle attacks. However, existing identity authentication schemes commonly use algorithms with high computational overhead, such as elliptic curve cryptography, making them unsuitable for resource-constrained devices. Therefore, it is crucial to design a lightweight anonymous identity authentication scheme tailored for resource-constrained IoT devices to verify the identity of devices connected to the IoT, thereby enhancing security protection and management.

A Physically Unclonable Function (PUF) is a lightweight security primitive that generates unique response values by leveraging the subtle differences that arise during the manufacturing process, serving as the "fingerprint" of a device. Typically, PUF technology is used in conjunction with a challenge-response mechanism, where the system sends a challenge to the device, and the PUF generates a corresponding response value for authentication or other subsequent operations. However, due to the susceptibility of PUFs to noise interference, many current schemes employ fuzzy extractors to mitigate the impact of noise on PUF output responses, thereby enhancing the robustness and reliability of PUF-based systems [1, 2].

Due to the secure and lightweight nature of PUFs, numerous researchers have utilized them for identity authentication in resource-constrained devices. This application provides an efficient and reliable identity verification mechanism for resource-constrained devices without requiring additional key storage or complex key management [3]. Consequently, PUFs have broad application prospects in IoT devices, sensor networks, smart cards, and other embedded systems. Their security and lightweight properties make PUFs an ideal choice for protecting resource-constrained devices from unauthorized access [4].

The study in [5] proposed a PUF-based mutual identity authentication and session key exchange scheme, which employs a fuzzy extractor to eliminate PUF noise and extract responses for identity authentication and key extraction. However, this scheme stores PUF challenge values in plaintext within the device, making it vulnerable to physical attacks. The study in [6] introduced a PUF-based authentication and key exchange protocol suitable for the Industrial Internet, which effectively reduces computational and communication overhead compared to other schemes, but it requires the input of biometric data during the authentication process. The study in [7] proposed a PUF-based anonymous user authentication scheme for smart homes in the IoT, which requires the input of user identity credentials and passwords and relies on a gateway to facilitate secure authentication between users and devices, thereby increasing the complexity of identity authentication, making it unsuitable for resource-constrained IoT devices. The study in [8] presented a two-way identity authentication protocol based on fuzzy extractors and elliptic curves, establishing mutual authentication between wireless sensor networks and the IoT. However, this scheme requires the storage of secret information related to authentication on a smart card and employs the resource-intensive elliptic curve algorithm, rendering it unsuitable for resource-constrained IoT devices. The study in [9] proposed a blockchain-based two-factor identity authentication scheme using a PUF-based fuzzy extractor, where blockchain technology is used for user authentication and authorization. However, due to the high resource consumption of blockchain, this approach is not suitable for resource-constrained IoT systems.

A common limitation of existing PUF-based identity authentication schemes is the plaintext storage of secrets within the device or the exposure of Challenge Response Pairs (CRPs) during device-server interactions, often requiring smart cards or password inputs to complete mutual authentication. Attackers can launch physical attacks on the device, accessing the device's memory to retrieve plaintext secrets, or capture CRPs to model the PUF using machine learning algorithms and predict its response values. Therefore, this paper proposes a lightweight anonymous identity authentication scheme for the IoT based on PUFs, Chebyshev chaotic maps, and fuzzy extractors. This scheme accomplishes mutual identity authentication and key agreement without the need for password input or smart card insertion. The Chebyshev chaotic map ensures the secure transmission of CRPs, while the fuzzy extractor shields the PUF from noise interference. Compared to previous schemes, this approach does not require the storage of any secret values in the device, effectively resisting physical, machine learning modeling, replay, and other attacks. It also offers multiple security properties, including anonymity, forward/backward security, and mutual authentication. Furthermore, the scheme only involves lightweight operations such as hash functions, Chebyshev chaotic maps, and fuzzy extractors, making it suitable for resource-constrained IoT devices.

The remainder of this paper is structured as follows: Section I, we introduce the relevant foundational concepts, including Physically Unclonable Functions, Chebyshev chaotic maps, and fuzzy extractors. Then, Section III describe the design and implementation of the proposed scheme in detail and analyze and evaluate its security and performance in Section IV. Finally, the paper concludes in Section V by summarizing the research findings and suggesting future research directions.

II. Related Knowledge

A. Physically Unclonable Functions

PUF is a function that leverages the uniqueness and unclonability of hardware characteristics. PUFs take advantage of the inevitable microscopic variations that occur during the manufacturing process, allowing each device to generate a unique response. The fundamental principle of PUFs is that, when subjected to the same challenge, different hardware devices will produce different responses, which makes these outputs both difficult to predict and impossible to replicate. Consequently, PUFs are widely used in security fields such as identity authentication and key generation. The main characteristics of PUFs include [10]:

- Uniqueness: Different devices have different PUF responses, each with unique characteristics.
- Unclonability: Due to the random, minor variations in the manufacturing process, it is impossible to precisely replicate a PUF.
- Unpredictability: Even if an attacker obtains some CRPs, they cannot predict responses that have not been previously observed.

B. Chebyshev Chaotic Map

The Chebyshev chaotic map is a mathematical mapping based on chaos theory, characterized by both determinism and chaotic behavior. The Chebyshev polynomial $T_n(x)$ can be defined recursively as follows:

$$T_n(x) = \begin{cases} 1 & n = 0 \\ x & n = 1 \\ 2xT_n(x) - T_{n-1}(x) & n \geq 2 \end{cases} \tag{1}$$

where n denotes the order of the polynomial. The Chebyshev polynomial exhibits chaotic behavior over the interval [−1, 1], with its output being highly sensitive to small variations in the initial value. This property makes the Chebyshev chaotic map highly valuable in cryptographic applications, where it can be used for generating pseudorandom numbers, encryption keys, and ensuring data integrity [11].

C. Fuzzy Extractor

A fuzzy extractor is a technique used to derive stable and reliable keys from imprecise inputs. Fuzzy extractors enable the consistent extraction of keys from noisy inputs, even when inputs may vary slightly over time. Fuzzy extractors typically involve two processes [12]:

- Generation (Gen): Converts the noisy input into a random key and auxiliary data.
- Reconstruction (Rep): Reconstructs the same random key using the auxiliary data and the noisy input.

Fuzzy extractors are particularly significant in IoT devices, ensuring that consistent keys can be generated across different environments, facilitating secure communication and identity authentication.

III. The Proposed Lightweight Anonymous Identity Authentication Scheme

The proposed scheme enables mutual authentication between IoT terminal devices and the gateway, consisting of two main phases: the registration phase and the authentication phase. This scheme assumes that each IoT terminal device is embedded with a PUF chip and that the registration process is completed within a secure channel, while the mutual identity authentication occurs over an insecure channel. The relevant symbols used in the scheme are described in Table I.

TABLE I. SYMBOL DESCRIPTIONS

Symbol	Description
AID_i	Pseudorandom identity of the device in the i-th round
ID_i	Real identity of the device
$h()$	One-way hash function
$\|\|$	Concatenation operation
$CRP(C_i, R_i)$	Challenge Response Pair
$T_r(x)$	Chebyshev polynomial
N_d, N_u, N_g	Random number
T, T_g, T_d	Timestamp
FE.Gen	Fuzzy extractor generation function
FE.Rec	Fuzzy extractor recovery function
hd	Helper data generated by the fuzzy extractor
k	Key generated by the fuzzy extractor
⊕	XOR operation
SK	Session key between the device and the gateway

A. Identity Authentication Model

The IoT identity authentication model used in this paper is illustrated in Fig. 1 [13], comprising three components: the registration center, the gateway, and the terminal devices. The registration center, located at the application layer of the IoT, is responsible for the registering both the gateways and terminal devices. The gateway acts as a bridge within the IoT system, connecting various IoT devices and networks while ensuring the reliable transmission and processing of data. Terminal devices are the front end of the entire system, directly interacting with the environment or users, collecting and transmitting data, and executing specific operations, thereby enabling the IoT system to achieve intelligent and automated functions. When a terminal device connects to the IoT, it first registers with the registration center. Subsequently, the gateway retrieves the authentication information of the terminal device from the registration center, and then mutual identity authentication between the terminal device and the gateway takes place.

In the lightweight anonymous identity authentication scheme proposed in this paper, making the following assumptions:

- Trusted Devices and Gateway: It is assumed that the devices and the gateway are initially trusted and can securely share an initial secret value.
- Secure PUF Implementation: It is assumed that each device has a secure PUF module, and that the CRPs of the PUF are unique and unpredictable.
- Insecure Communication Channel: It is assumed that the communication channel between the device and the gateway is insecure, meaning that an attacker could intercept, tamper with, or even replay messages.
- Attacker Model: It is assumed that an attacker has the capability to intercept communication messages, perform physical attacks, and attempt machine learning modeling, but cannot clone the PUF's response.

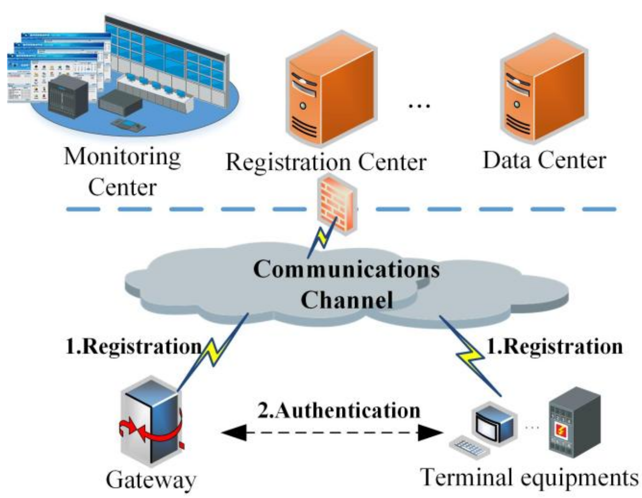

Fig. 1. IoT identity authentication model.

B. Registration Phase

The device registration phase to the gateway is shown in Fig. 2. In the registration phase, the device registers with the gateway through the secure channel, and the specific registration steps are as follows:

Step 1: The device selects its real identity ID_i and sends it to the gateway.

Step 2: The gateway generates a challenge value C_i, computes $AID_i = h(C_i \| ID_i)$, and sends the message $\{C_i, AID_i\}$ to the device.

Step 3: The device computes R_i = PUF(C_i), stores AID_i, and sends the message $\{R_i\}$ back to the gateway.

Step 4: The gateway generates $T_{Ri} = T_{Ri}(x) \bmod p$, publishes x, p, T_{Ri}, and stores (C_i, R_i, AID_i).

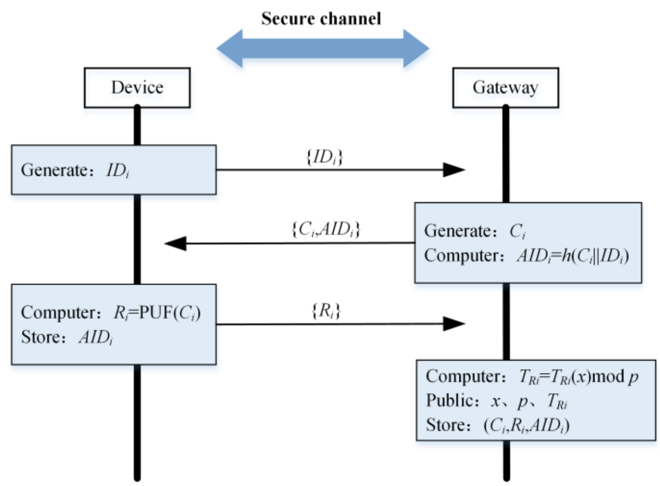

Fig. 2. Device and gateway registration phase.

C. Authentication Phase

The device and gateway authentication phase is shown in Fig. 3. In the authentication phase, the terminal device and the gateway utilize the authentication parameters obtained through registration to carry out two-way authentication and negotiate a session key for subsequent use in the following steps:

Step 1: The device generates a random number N_d, N_u, computes $T_{Nd} = T_{Nd}(x) \bmod p$, $T_{Nd\cdot Ri} = T_{Nd}(T_{Ri}) \bmod p$, and $N_u^* = N_u \oplus T_{Nd\cdot Ri}$, and creates a message $\{T_{Nd}, AID_i, N_u^*\}$ which it then sends to the gateway.

Step 2.1: The gateway checks its memory for AID_i. If AID_i is not found in memory, the gateway rejects the device's authentication; otherwise, the gateway proceeds with the authentication.

Step 2.2: The gateway generates a random number N_g, a timestamp T_g, and computes $T_{Nd\cdot Ri} = T_{Ri}(T_{Nd}) \bmod p$, $N_u = N_u^* \oplus T_{Nd\cdot Ri}$, $C_i^* = C_i \oplus T_{Nd\cdot Ri}$, $N_g^* = N_g \oplus N_u$, $V_0 = h(T_{Nd\cdot Ri} \| N_u \| R_i \| T_g)$. It then sends the message $\{C_i^*, N_g^*, V_0, T_g\}$ to the device.

Step 3.1: The device computes $C_i = C_i^* \oplus T_{Nd\cdot Ri}$, $N_g = N_g^* \oplus N_u$, and R_i = PUF(C_i).

Step 3.2: The device verifies $|T - T_g| < \Delta t$. If the verification fails, the authentication fails. Otherwise, it checks whether V_0' matches V_0. If they do not match, the authentication fails.

Step 3.3: The device generates a timestamp T_d, and computes(k, hd) = FE.Gen(R_i), $C_{i+1} = h(C_i \| N_u)$, R_{i+1} = PUF(C_{i+1}), $AID_{i+1} = h(AID_i \| k \| N_g)$, $R_{i+1}^* = R_{i+1} \oplus N_g$, $SK = h(N_u \| R_{i+1} \| T_{Nd \cdot Ri})$, $hd^* = hd \oplus h(R_{i+1} \| T_{Nd \cdot Ri})$, $V_1 = h(N_g \| k \| SK \| T_d)$. It stores AID_{i+1} and sends the message $\{R_{i+1}^*, hd^*, V_1, T_d\}$ to the gateway.

Step 4.1: The gateway verifies $|T - T_d| < \Delta t$. If the verification fails, the authentication fails. Otherwise, it computes $R_{i+1} = R_{i+1}^* \oplus N_g$, $hd = hd^* \oplus h(R_{i+1} \| T_{Nd \cdot Ri})$, k = FE.Rec$(R_i \| hd)$, $SK = h(N_u \| R_{i+1} \| T_{Nd \cdot Ri})$, $T_{Ri+1} = T_{Ri+1}(x) \bmod p$, and publishes x, p, T_{Ri+1}.

Step 4.2: The gateway verifies whether V_1' matches V_1. If they do not match, the authentication fails.

Step 4.3: The gateway updates $C_{i+1} = h(C_i \| N_u)$, $AID_{i+1} = h(AID_i \| k \| N_g)$, and stores $(C_{i+1}, R_{i+1}, AID_{i+1})$.

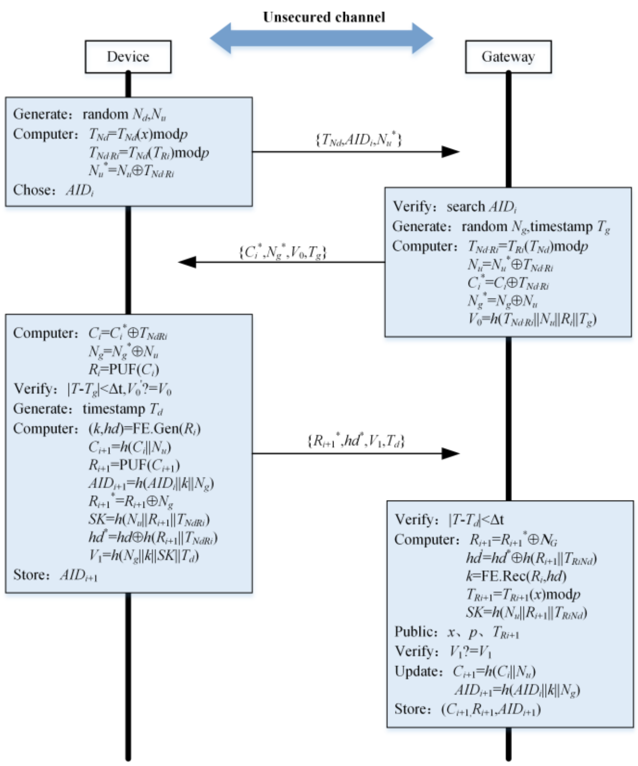

Fig. 3. Device and gateway authentication phase.

IV. Security Analysis of the Proposed Scheme

A. *Formal Security Analysis Using Improved BAN Logic*

This paper employs an improved BAN (Burrows, Abadi and Needham) logic [14] to analyze the proposed lightweight anonymous identity authentication scheme for power IoT. In this context, A, B, P and Q represent the authentication entities, while M and N denote the messages involved in the authentication process. J and Q represent formulas. Table II provides the symbols and meanings used in the improved BAN logic.

TABLE II. Symbols in Improved BAN Logic

Symbol	Meaning
$P \mid\equiv J$	P believes J is true
$P \mid\overset{K}{\sim} J$	P encrypts message J with key K
$P \overset{K}{\triangleleft} J$	P has received a message J encrypted with key K
$P \overset{K}{\leftrightarrow} Q$	P and Q share key K
$P \overset{J}{\square} Q$	P and Q share secret J
$\#(J)$	J is within its validity period
sup(S)	S is a trusted party
$P \triangleleft\| M$	P does not know message M

Table III shows the inference rules used by the improved BAN logic:

TABLE III. Improved BAN Inference Rules

Rule Name	Expression
Authentication Rule	$\dfrac{P \mid\equiv P \overset{K}{\leftrightarrow} Q \wedge P \triangleleft \overset{K}{M}}{P \mid\equiv Q \mid\overset{K}{\sim} M}$
Confidentiality Rule	$\dfrac{P \mid\equiv P \overset{K}{\leftrightarrow} Q \wedge P \mid\equiv S^C \triangleleft\| M \wedge P \mid\overset{K}{\sim} M}{P \mid\equiv (S \cup \{Q\})^C \triangleleft\| M}$
Freshness Rule	$\dfrac{P \mid\equiv \#(M) \wedge P \mid\equiv Q \overset{K}{\leftrightarrow} M}{P \mid\equiv Q \mid\equiv P \overset{K}{\leftrightarrow} Q}$
Super Subject Rule	$\dfrac{P \mid\equiv Q \mid\equiv X \wedge P \mid\equiv \text{sup}(Q)}{P \mid\equiv X}$
Randomness Validation Rule	$\dfrac{P \mid\equiv \#(M) \wedge P \triangleleft N \Re M}{P \mid\equiv \#(N)}$
Security Key Rule	$\dfrac{P \mid\equiv \{P,Q\}^C \triangleleft\| K \wedge P \mid\equiv \#(K)}{P \mid\equiv P \overset{K}{\leftrightarrow} Q}$
Derivation Rule	$\dfrac{P \mid\equiv Q \mid\equiv P \overset{K}{\leftrightarrow} Q \wedge P \mid\equiv Q \mid\equiv S^C \triangleleft\| M \wedge P \mid\overset{K}{\sim} M}{P \mid\equiv Q \mid\equiv (S \cup \{P\})^C \triangleleft\| M}$

Using the improved BAN logic, we have proven that the authentication process for N_g, R_{i+1}, $T_{Nd \cdot Ri}$ is secure. The proof process is shown in Fig. 4. Firstly, we idealize the messages exchanged between the terminal and the gateway. The results of this idealization are as follows:

- $D \to GW : T_{Nd}, AID_i, N_u$.
- $GW \to D : N_u \Re T_{Nd \cdot Ri} \Re N_g \Re T_g$.
- $D \to GW : N_g \Re T_{Nd \cdot Ri} \Re R_{i+1} \Re T_d$.

The following assumptions are made for the proposed authentication scheme:

- $D \mid\equiv D \overset{Ri}{\leftrightarrow} GW$, $GW \mid\equiv D \overset{Ri}{\leftrightarrow} GW$: During the registration phase, the gateway stores the CRPs for each terminal, and the device can use the PUF function to compute responses R_i.
- $GW \mid\equiv \{D\}^C \triangleleft\| N_g$. $D \mid\equiv GW \mid\equiv \{D\}^C \triangleleft\| N_g$: The gateway generates random numbers N_g.

- $D\mid\equiv\{GW\}^C \lhd\| R_{i+1}$, $GW\mid\equiv D\mid\equiv\{GW\}^C \lhd\| R_{i+1}$: The device uses the PUF function to generate new responses R_{i+1}.
- $D\mid\equiv\{GW\}^C \lhd\| T_{Nd\cdot Ri}$, $GW\mid\equiv D\mid\equiv\{GW\}^C \lhd\| T_{Nd\cdot Ri}$: The device computes and generates $T_{Nd\cdot Ri}$.
- $D\mid\equiv\#(N_d)$, $D\mid\equiv\#(T_{Nd\cdot Ri})$, $D\mid\equiv\#(N_u)$, $D\mid\equiv\#(T_d)$, $D\mid\equiv\#(R_{i+1})$: N_d, $T_{Nd\cdot Ri}$, N_u, T_d, R_{i+1} are within their validity periods.
- $GW\mid\equiv\#(N_g)$, $GW\mid\equiv\#(T_{Nd\cdot Ri})$, $GW\mid\equiv\#(T_g)$: N_g, $T_{Nd\cdot Ri}$, T_g are within their validity periods.
- $D\mid\equiv \sup(GW)$, $GW\mid\equiv \sup(D)$: The gateway and device trust each other.
- $D\lhd N_u\Re N_g$, $D\lhd T_{Nd\cdot Ri}\Re N_g$: Messages in the idealized scheme for Message 2.
- $GW\lhd T_{Nd\cdot Ri}\Re R_{i+1}$, $GW\lhd N_g\Re R_{i+1}$: Messages in the idealized scheme for Message 3.

B. Informal Security Analysis

1) Bidirectional authentication: The proposed scheme enables bidirectional identity authentication between devices and gateways. Devices authenticate the gateway by verifying $V_0'=V_0$, while the gateway authenticates the device by verifying $V_1'=V_1$. Since the expressions for V_0 and V_1 include secret values such as $T_{Nd\cdot Ri}$, N_u, and R_i, obtaining $T_{Nd\cdot Ri}$ would require solving the chaotic mapping Diffie-Hellman problem. Additionally, N_u and N_g are not transmitted in plaintext, preventing making the scheme resistant to tampering attacks by resending messages an attacker to acquire any secret values and thus preventing impersonation of legitimate devices or gateways during authentication.

2) Anonymity and untraceability: During the authentication process, both the device and the gateway utilize pseudonyms, which are updated after each authentication. As a result, attackers are unable to obtain the real identity ID_i, ensuring both anonymity and untraceability.

3) Tamper resistance: Although attackers may intercept and tamper with messages transmitted over insecure channels, the information exchanged in the proposed scheme is protected by hash functions or bitwise XOR operations. Consequently, attackers cannot extract secret values from the messages, enabling the scheme to resist tampering attacks.

4) Resistance to cloning and physical attacks: While attackers could use physical methods to access a device's memory and obtain sensitive information, the device only stores pseudonyms and not the secret values related to authentication. Furthermore, PUFs possess characteristics such as unclonability, meaning any attempt by an attacker to obtain a PUF response would compromise its functionality, thus preventing impersonation of legitimate devices through cloning or physical attacks.

5) Resistance to machine learning modeling attacks: Attackers may attempt to construct a PUF response model using collected CRPs and machine learning algorithms to predict CRPs. However, in the proposed scheme, attackers can only capture CRPs from insecure channels, and acquiring the challenge values necessitates obtaining $T_{Nd\cdot Ri}$. As such, they cannot obtain the response values, which are hashed, making it impossible to reverse-engineer them due to the one-way nature of hash functions. Therefore, the proposed scheme effectively mitigates machine learning modeling attacks.

6) Resistance to spoofing attacks: If an attacker seeks to impersonate a legitimate device, they must send the correct AID_i, N_u^*, R_{i+1}^*, V_1, and hd^*. However, generating valid values requires correct N_g, k, N_u, R_{i+1}, and $T_{Nd\cdot Ri}$. As established, attackers cannot access valid $T_{Nd\cdot Ri}$ and R_{i+1}, preventing them from acquiring N_g and N_u. Similarly, if an attacker attempts to impersonate the gateway, they would require valid CRPs and $T_{Nd\cdot Ri}$, making it impossible to authenticate as a legitimate gateway.

$$\frac{\dfrac{\dfrac{\dfrac{D\mid\equiv\#(T_{Nd\cdot Ri})\wedge\dfrac{D\mid\equiv D\overset{R_i}{\leftrightarrow}GW\wedge D\lhd T_{Nd\cdot Ri}}{D\mid\equiv GW\mid\sim T_{Nd\cdot Ri}}}{D\mid\equiv GW\mid\equiv D\overset{R_i}{\leftrightarrow}GW}\wedge D\mid\equiv GW\mid\equiv\{D\}^C\lhd\| N_g\wedge\dfrac{D\mid\equiv D\overset{R_i}{\leftrightarrow}GW\wedge D\lhd N_g}{D\mid\equiv GW\mid\sim N_g}}{D\mid\equiv GW\mid\equiv\{D,GW\}^C\lhd\| N_g}\wedge D\mid\equiv\sup(GW)}{D\mid\equiv\{D,GW\}^C\lhd\| N_g}\wedge\dfrac{D\mid\equiv\#(T_{Nd\cdot Ri})\wedge D\lhd T_{Nd\cdot Ri}\Re N_g}{D\mid\equiv\#(N_g)}}{D\mid\equiv D\overset{N_g}{\leftrightarrow}GW}$$

(a)

$$\frac{\dfrac{GW\mid\equiv D\overset{R_i}{\leftrightarrow}GW\wedge GW\mid\equiv\{D\}^C\lhd\| N_g\wedge GW\mid\sim N_s}{GW\mid\equiv\{D,GW\}^C\lhd\| N_g}\wedge GW\mid\equiv\#(N_g)}{GW\mid\equiv GW\overset{N_g}{\leftrightarrow}D}$$

(b)

$$\frac{\dfrac{\dfrac{\dfrac{GW\mid\equiv\#(N_g)\wedge\dfrac{GW\mid\equiv GW\overset{R_i}{\leftrightarrow}D\wedge GW\lhd N_g}{GW\mid\equiv D\mid\sim N_g}}{GW\mid\equiv D\mid\equiv GW\overset{R_i}{\leftrightarrow}D}\wedge GW\mid\equiv D\mid\equiv\{GW\}^C\lhd\| R_{i+1}\wedge\dfrac{GW\mid\equiv GW\overset{R_i}{\leftrightarrow}D\wedge GW\lhd R_{i+1}}{GW\mid\equiv D\mid\sim R_{i+1}}}{GW\mid\equiv D\mid\equiv\{D,GW\}^C\lhd\| R_{i+1}}\wedge GW\mid\equiv\sup(D)}{GW\mid\equiv\{D,GW\}^C\lhd\| R_{i+1}}\wedge\dfrac{GW\mid\equiv\#(N_g)\wedge GW\lhd N_g\Re R_{i+1}}{GW\mid\equiv\#(R_{i+1})}}{GW\mid\equiv GW\overset{R_{i+1}}{\leftrightarrow}D}$$

(c)

$$\frac{\dfrac{D\mid\equiv D\overset{R_i}{\leftrightarrow}GW\wedge D\mid\equiv\{GW\}^C\lhd\| R_{i+1}\wedge D\mid\sim R_{i+1}}{D\mid\equiv\{D,GW\}^C\lhd\| R_{i+1}}\wedge D\mid\equiv\#(R_{i+1})}{D\mid\equiv D\overset{R_{i+1}}{\leftrightarrow}GW}$$

(d)

$$\dfrac{\dfrac{\dfrac{\dfrac{D \mid\equiv \#(T_{Nd\cdot Ri}) \wedge \dfrac{D \mid\equiv D \overset{R_i}{\leftrightarrow} GW \wedge D \triangleleft T_{Nd\cdot Ri}}{D \mid\equiv GW \mid\sim T_{Nd\cdot Ri}}}{D \mid\equiv GW \mid\equiv D \overset{R_i}{\leftrightarrow} GW} \wedge D \mid\equiv GW \mid\equiv \{D\}^{C} \triangleleft\| T_{Nd\cdot Ri} \wedge \dfrac{D \mid\equiv D \overset{R_i}{\leftrightarrow} GW \wedge D \triangleleft T_{Nd\cdot Ri}}{D \mid\equiv GW \mid\sim T_{Nd\cdot Ri}}}{D \mid\equiv GW \mid\equiv \{D, GW\}^{C} \triangleleft\| T_{Nd\cdot Ri}} \wedge D \mid\equiv \sup(GW)}{D \mid\equiv \{D, GW\}^{C} \triangleleft\| T_{Nd\cdot Ri}} \wedge D \mid\equiv \#(T_{Nd\cdot Ri})}{D \mid\equiv D \overset{T_{Nd\cdot Ri}}{\leftrightarrow} GW}$$

(e)

$$\dfrac{\dfrac{GW \mid\equiv GW \overset{R_i}{\leftrightarrow} D \wedge GW \mid\equiv \{D\}^{C} \triangleleft\| T_{Nd\cdot Ri} \wedge GW \mid\sim T_{Nd\cdot Ri}}{GW \mid\equiv \{D, GW\}^{C} \triangleleft\| T_{Nd\cdot Ri}} \wedge GW \mid\equiv \#(T_{Nd\cdot Ri})}{GW \mid\equiv GW \overset{T_{Nd\cdot Ri}}{\leftrightarrow} D}$$

(f)

Fig. 4. Security Proof of the Improved BAN Logic for N_g, R_{i+1}, $T_{Nd\cdot Ri}$. (a) D believes that N_g is a shared secret between D and GW; (b) GW believes that N_g is a shared secret between GW and D; (c) GW believes that R_{i+1} is a shared secret between GW and D; (d) D believes that R_{i+1} is a shared secret between D and GW; (e) D believes that $T_{Nd\cdot Ri}$ is a shared secret between D and GW; (f) GW believes that $T_{Nd\cdot Ri}$ is a shared secret between GW and D.

7) Resistance to replay attacks: The proposed scheme incorporates a timestamp mechanism, requiring verification of transmission delays before authentication. This prevents attackers from initiating replay attacks through message resending. Additionally, timestamps are included in V_0 and V_1; any attempt by an attacker to change the timestamp will result in authentication failure. Moreover, the secret values in V_0 and V_1 are updated after each authentication, effectively resisting replay attacks.

8) Resistance to Denial-of-Service (DoS) attacks: When attackers send excessive invalid information to disrupt communication between devices and gateways, the devices and gateways will first validate the transmission delays and then verify the values of V_0 or V_1. Any failure to meet these criteria will result in a rejection of authentication.

9) Forward and backward security: In the proposed scheme, the session key negotiated is $SK = h(N_u \| R_{i+1} \| T_{Nd\cdot Ri})$. Since N_u, R_{i+1}, and $T_{Nd\cdot Ri}$ are updated after each authentication, even if an attacker acquires the current device's secret values and CRPs, they cannot trace past or future communications of the device, thus ensuring both forward and backward security.

V. PERFORMANCE ANALYSIS

A. Security Feature Analysis

Table IV compares the security features of the proposed scheme with those of existing solutions. In study [15], attackers can obtain CRPs through eavesdropping or spoofing, which makes the system vulnerable to machine learning modeling attacks. In contrast, the proposed scheme stores only pseudonymous identities on the device, preventing attackers from obtaining plaintext CRPs through physical attacks. Furthermore, the CRPs are protected by XOR or hash functions during the authentication process, which helps safeguard against machine learning modeling attacks. The study in [16] describes a system where authentication values are generated from secret values stored on the device or randomly generated by users. If this secret information is compromised, attackers could potentially impersonate legitimate devices or gateways. In the proposed scheme, however, attackers would need to access secret information such as N_u, N_g, R_{i+1}. These secrets are protected by Chebyshev polynomials or hash functions, making it difficult for attackers to access them and thus defending against spoofing and man-in-the-middle attacks.

B. Computational Overhead Analysis

Based on the execution times for various operations outlined in study [14], the following time parameters are considered: T_h for executing a hash function, T_{PUF} for executing a PUF, T_{che} for executing a Chebyshev polynomial, T_{Mul} for performing an elliptic curve point multiplication, $T_{FE.Gen}$ for generation with a fuzzy extractor, and $T_{FE.Rep}$ for recovery with a fuzzy extractor. The execution times for these operations are listed in Table V.

Table VI compares the computational overhead of the proposed scheme with those of other schemes in the literature (Fig. 5). As shown in the table, the schemes in studies [15] and [16] use resource-intensive elliptic curve point multiplication, resulting in the highest computational overheads of 3909.2284 μs and 3549.8392 μs, respectively. In contrast, the proposed scheme utilizes lightweight Chebyshev chaotic mappings, resulting in a total computational overhead of 1396.3521 μs. This represents a reduction of 60.664% and 64.281%, respectively, compared to the computational overheads of the schemes proposed in the other references.

C. Communication Overhead Analysis

Before comparing the communication overhead, the lengths of the various variables are referenced from [14]. Table VII presents a comparison of the communication overhead between the proposed scheme and those in the literature. The table shows that the communication overhead of the proposed scheme is 1216 bits, which is lower than that of the schemes proposed in studies [15] and [16]. Therefore, the proposed scheme is well-suited for anonymous identity authentication and session key negotiation for resource-constrained terminal devices and gateways.

TABLE IV. COMPARISON OF SECURITY FEATURES

Security Attribute	Bai Haodong et al. [15]	Soni [16]	Proposed Scheme
Mutual Authentication	✓	✓	✓
Untraceability	✓	✓	✓
User Anonymity	✓	✓	✓
Forward/Backward Security	✓	✓	✓
DoS Attack	✓	✓	✓
Replay Attack	✓	✓	✓
Machine Learning Modeling Attack	×	✓	✓
Spoofing Attack	✓	×	✓
Man-in-the-Middle Attack	✓	×	✓
Mutual Authentication	✓	✓	✓

TABLE V. EXECUTION TIMES FOR VARIOUS OPERATIONS

Operation	Operation execution time	
	Device Side	***Gateway Side***
T_h	2.7324μs	0.1315μs
T_{PUF}	6.7μs	/
T_{che}	91.2600μs	10.6604μs
T_{Mul}	426.4887μs	103.8660μs
$T_{FE.Gen}$	278.0889μs	74.7562μs
$T_{FE.Rep}$	696.1048μs	157.4092μs

TABLE VI. COMPARISON OF COMPUTATIONAL OVERHEAD

Scheme	Device Side	Gateway Side	Total Time
Bai et al. [15]	$5T_h + T_{FE.Gen} + T_{FE.Rep} + 5T_{Mul} + 2T_{PUF} \approx 3133.8492\mu s$	$4T_h + 4T_{Mul} \approx 415.99\mu s$	$3549.8392\mu s$
Soni et al. [16]	$11T_h + T_{FE.Rep} + 6T_{Mul} \approx 3285.2434\mu s$	$6T_h + 6T_{Mul} \approx 623.985\mu s$	$3909.2284\mu s$
Proposed Scheme	$8T_h + 2T_{Che} + 2T_{PUF} + T_{FE.Gen} \approx 495.8681\mu s$	$8T_h + 2T_{Che} + T_{FE.Rep} \approx 900.484\mu s$	$1396.3521\mu s$

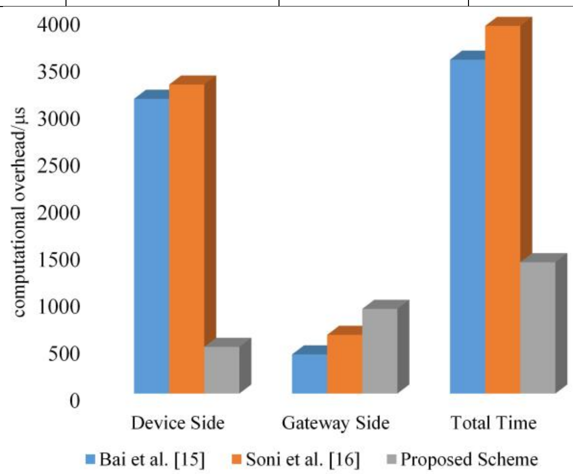

Fig. 5. Comparison of computation overhead.

TABLE VII. COMPARISON OF COMMUNICATION OVERHEAD

Scheme	Number of messages	Communication cost
Bai et al. [15]	3	1472bit
Soni et al. [16]	2	2304bit
Proposed Scheme	3	1216bit

The experimental results confirm that the proposed scheme offers significant improvements in both security and efficiency compared to existing solutions. As shown in Table IV, the scheme effectively mitigates the vulnerabilities of previous methods, such as machine learning attacks and impersonation, by storing only pseudonymous identities and using XOR/hash functions to protect CRPs. This is a clear advantage over reference [15], where CRPs can be intercepted, and reference [16], where compromised secrets may lead to spoofing.

In terms of computational overhead, our scheme, utilizing Chebyshev chaotic mappings, significantly reduces processing time by approximately 60-64% compared to the elliptic curve-based methods in studies [15] and [16]. This makes it more suitable for resource-constrained IoT devices. Furthermore, as seen in Table VII, the communication overhead of our scheme is lower than that of existing solutions, making it ideal for devices with limited bandwidth.

Overall, our scheme provides a balanced approach, offering robust security and efficiency, which is essential for resource-constrained IoT environments.

VI. CONCLUSION

This paper presents a lightweight identity authentication scheme designed for resource-constrained IoT devices, which has been verified for security using an improved BAN logic. The results indicate that the proposed scheme is capable of resisting attacks such as physical attacks, machine learning modeling attacks, replay attacks, and man-in-the-middle attacks. Compared to existing solutions, the computational overhead of the proposed scheme is only 1396.3521 μs, and the communication overhead is only 1216 bits, making it suitable for efficient and secure authentication in IoT environments. Future work will focus on further optimizing the performance of the scheme, reducing system overhead, and conducting more extensive testing and validation in complex application scenarios to enhance the overall security and reliability of the scheme.

REFERENCES

[1] W. Che, F. Saqib, and J. P. Plusquellic, "PUF-based authentication," in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Austin, TX, USA, November 2015, pp. 337–344, doi: 10.1109/ICCAD.2015.7372589.

[2] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, 2018, doi: 10.3390/sym10080352.

[3] J. Zou, B. Zhao, X. Li, Y. Liu, and J. Li, "tPUF-based secure access solution for IoT devices," *Computer Engineering and Applications*, vol. 57, no. 02, pp. 119–126, 2021.

[4] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, pp. 1–42, 2015, doi: 10.1145/2818186.

[5] Z. He, H. Li, M. Wan, and T. Wu, "A two-party authentication and session key exchange protocol based on PUF," *Computer Engineering and Applications*, vol. 54, no. 18, pp. 17–21, 2018.

[6] Y. Xia, R. Qi, and S. Ji, "Research on lightweight key exchange protocol based on PUFs in industrial Internet of Things," *Computer Applications and Software*, vol. 39, no. 03, pp. 316–321, 2022.

[7] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A secure and anonymous user authentication scheme for IoT-enabled smart home environments using PUF," *IEEE Access*, vol. 10, pp. 101330–101346, 2022, doi: 10.1109/ACCESS.2022.3208347.

[8] A. K. Maurya and V. N. Sastry, "Fuzzy extractor and elliptic curve based efficient user authentication protocol for wireless sensor networks and Internet of Things," *Information*, vol. 8, no. 4, p. 136, 2017, doi: 10.3390/info8040136.

[9] N. Singh and A. K. Das, "TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor," *The Journal of Supercomputing*, vol. 80, no. 1, pp. 865–914, 2024, doi: 10.1007/s11227-023-05507-6.

[10] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020, doi: 10.1038/s41928-020-0372-5.

[11] D. Dharminder and P. Gupta, "Security analysis and application of Chebyshev Chaotic map in the authentication protocols," *International Journal of Computers and Applications*, vol. 43, no. 10, pp. 1095–1103, 2021, doi: 10.1080/1206212X.2019.1682238.

[12] C. Herder, L. Ren, M. Van Dijk, M. D. Yu, and S. Devadas, "Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 65–82, 2016, doi: 10.1109/TDSC.2016.2536609.

[13] H. Ma, C. Wang, G. Xu, Q. Cao, G. Xu, and L. Duan, "Anonymous authentication protocol based on physical unclonable function and elliptic curve cryptography for smart grid," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6425–6436, 2023, doi: 10.1109/JSYST.2023.3289492.

[14] X. Jin, N. Lin, Z. Li, W. Jiang, Y. Jia, and Q. Li, "A lightweight authentication scheme for Power IoT based on PUF and Chebyshev Chaotic Map," *IEEE Access*, vol. 12, pp. 83692–83706, 2024, doi: 10.1109/ACCESS.2024.3413853.

[15] H. Bai and X. Jia, "A smart grid equipment authentication scheme based on physically unclonable functions," *Journal of South-Central Minzu University (Natural Science Edition)*, vol. 42, no. 3, pp. 382–386, 2023, doi: 10.20056/j.cnki.ZNMDZK.20230313.

[16] P. Soni, J. Pradhan, A. K. Pal, and S. H. Islam, "Cybersecurity Attack-Resilience Authentication Mechanism for Intelligent Healthcare System," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 830–840, 2022, doi: 10.1109/TII.2022.3179429.