IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 May 2024, accepted 10 June 2024, date of publication 13 June 2024, date of current version 20 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3413853

RESEARCH ARTICLE

A Lightweight Authentication Scheme for Power IoT Based on PUF and Chebyshev Chaotic Map

XIANJI JIN, NA LIN, ZHONGWEI LI, WENQI JIANG, YUGE JIA, AND QINGYANG LI
School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China
Corresponding author: Zhongwei Li (lzw@hit.edu.cn)

ABSTRACT With the wide application of IoT technologies in the power sector, power IoT faces serious security challenges, which can be severely affected by malicious attacks and unauthorised access. Meanwhile, devices in power IoT are usually resource-constrained and deployed in a decentralised manner, making them vulnerable to physical attacks. Therefore, a robust and reliable lightweight authentication scheme needs to be constructed to guarantee its information security. A lightweight authentication scheme for the power IoT based on Physical Unclonable Function (PUF) and Chebyshev chaotic map is proposed in this paper, which achieves two-way authentication and session key negotiation between gateways and terminal devices. Comparing with traditional authentication schemes, the PUF and Chebyshev chaotic map used in this scheme have high security and lower resource overhead. PUF is used to generate Challenge and Response Pairs (CRPs) for two-way authentication and key negotiation without storing any secret information about authentication in the device memory. At the same time, Chebyshev chaotic map is used to protect the transmission of secret information such as CRPs in insecure channels. The solution is therefore resistant to attacks such as physical, machine learning modelling and impersonation, ensuring the information security of the authentication process. The proposed scheme is analyzed and verified using the formal verification tool ProVerif and improved BAN logic along with informal methods. The verification results show that the scheme satisfies 12 security properties such as two-way authentication and user anonymity. Comparative analysis with existing related authentication schemes shows that the proposed scheme has low computation and communication costs while guaranteeing security, thus rendering it suitable for resource-constrained terminal devices in the power IoT.

INDEX TERMS Power Internet of Things, physical unclonable function, Chebyshev chaotic map, lightweight authentication.

I. INTRODUCTION

With the transformation of society to digitalization and intelligence, the wide application of Internet of Things (IoT) technology in various fields has become a trend that cannot be ignored. As an important part of the energy field, the power IoT, which integrates the power system with the IoT technology in depth, is designed to realize the intelligence and automation of the power system, which profoundly shapes the new pattern in the field of power and energy. Through intelligent perception, real-time data collection, etc., IoT transforms all aspects of the power system into highly manageable and monitorable intelligent nodes, which provides strong support for the efficient energy management of the power system.

Power IoT Supervisory Control And Data Acquisition (SCADA) system, which is responsible for monitoring, controlling, and collecting real-time data from the power system, is the basis for intelligent management and efficient operation of the power system. With the development of IoT technology, there is an exponential growth of devices in the field control layer of power IoT SCADA systems, with most of them being resource-constrained, deployed in a decentralized manner, being difficult to monitor and control [1], making them vulnerable to attacks such as physical, replay, and Denial of Service (DoS). At the same time, with the

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

increase of exposed interfaces in SCADA systems, attackers may attempt to capture sensitive data in the communication channel and tamper with it, which in turn poses a threat to the data security of the power IoT. To address these threats, power IoT needs to introduce authentication schemes for resource-constrained terminal devices to ensure that only authorized users or devices can access sensitive information. Traditional authentication schemes are based on symmetric or asymmetric cryptographic algorithms. Therefore these schemes do not apply to resource-constrained terminal devices. There is also the problem that keys and other secret information are stored in plain text within the device. When the device suffers from a physical attack, the attacker can access the memory of the device to obtain the keys as well as the secret information, which in turn poses a threat to data privacy and security. To overcome the limitations of existing schemes, lightweight security primitive Physical Unclonable Function (PUF) is applied for the authentication of resource-constrained devices. The PUF generates responses based on process deviations during the manufacturing of the device, which is unclonable and unpredictable, any attempt to tamper with the functionality of the PUF will result in the PUF being unavailable, thus making it resilient to physical attacks, cloning attacks, and side-channel attacks [2].

A. RELATED WORK

Currently, PUF-based authentication schemes primarily integrate techniques such as hash functions, elliptic curves, fuzzy extractors, and Chebyshev chaotic maps to provide a more comprehensive and effective solution for PUF-based authentication, thereby enhancing the security and reliability of the system. Gope et al. proposed a lightweight privacy-preserving scheme for radio frequency identification systems [3], utilizing hash functions, PUF, and fuzzy extractors to achieve two-way authentication between tags and servers. However, the scheme transmits challenge values as well as secret information in plain text, rendering it vulnerable to impersonation attacks and machine learning modeling attacks. A year later, Gope et al. proposed a lightweight dual-participant identity authentication scheme for IoT devices based on the scheme proposed in the literature [3], in which the PUF is considered to be the first participant in the authentication [4]. Furthermore, the secret value K is the second factor of authentication, yet this scheme stores the secret value K in plain text within the device. When an attacker accesses the device memory through a physical attack, the secret value will be obtained and the rest of the secret information will be leaked. In addition, This scheme does not improve the shortcomings of the plaintext transmission challenge value. Siddiqui et al. performed a security analysis of the scheme proposed by Gope et al. and found it vulnerable to attacks such as impersonation, tampering, and side-channel. They proposed an authentication scheme based on Public Key Infrastructure (PKI) and PUF [5], which improves on the shortcomings of Siddiqui et al. scheme but PKI does not apply to resource-constrained power IoT devices. Kim et al. proposed a PUF-based authentication scheme for IoT devices [6]. This scheme simplifies by storing and updating a single challenge and response pair, and encrypting interaction information through the response value of the PUF, thereby reducing complexity. However, it remains susceptible to machine learning modeling attacks. Nozaki and Yoshikawa proposed a secure PUF authentication scheme based on secret sharing for the problem that PUF-based authentication schemes are susceptible to machine learning modeling attacks [7], which splits the PUF response and improves the resistance to machine learning modeling attacks. However, secret sharing increases the computational cost of the device and the server, which does not apply to resource-constrained devices. Wang et al. proposed a lightweight anonymous authentication scheme based on PUF [8], which stores less information in IoT devices and has high efficiency in two-way authentication between IoT devices and servers. Although the scheme only achieves two-way authentication and does not negotiate a session key for subsequent communication. Wang et al. proposed a three-party authentication scheme for smart grids [9], leveraging PUF and hash functions without necessitating the input of biometric data like fingerprints. Nonetheless, this scheme relies on a third-party server during the two-way authentication process between the smart meter and the control center, potentially increasing system complexity. Bai and Jia proposed a lightweight anonymous authentication scheme for smart meters and neighborhood gateways by combining PUF, fuzzy extractor, and elliptic curve cryptography [10], which uses elliptic curve dot multiplication operations to protect secret information by using the elliptic curve dot multiplication operations with the secret information dissimilar to the secret information. However, the use of elliptic curve cryptography and fuzzy extractors imposes significant computational costs, making it unsuitable for resource-constrained devices. Moreover, this scheme remains vulnerable to machine learning modeling attacks. Tanveer et al. proposed an anonymous authentication scheme for smart grids [11], which not only achieves two-way authentication between the smart meter and the server but also negotiates the session key, but the scheme uses elliptic curve dot multiplication operations, so the scheme does not apply to resource-constrained devices. Ma et al. proposed an anonymous authentication scheme based on elliptic curve cryptography and PUF [12], but since the scheme stores a lot of secret information in the device, the scheme is vulnerable to physical attacks, machine learning modeling attacks, and impersonation attacks. The elliptic curve cryptography used in the scheme also burdens the system. Due to the computationally intensive elliptic curve cryptography algorithm, many scholars nowadays use Chebyshev chaotic map instead of elliptic curve cryptography algorithm to design authentication schemes. Wang et al. pointed out that the chaotic map-based multi-server authentication scheme proposed by Irshad et al. is vulnerable to session key recovery attacks and impersonation attacks and improved on this scheme [13]. However, the improved scheme requires a password to be entered to log in to the

device, which does not apply to power IoT terminal devices located in remote areas. Lee proposed an efficient single sign-on authentication scheme using an extended Chebyshev chaotic map, but the scheme is not resistant to physical attacks [14]. Zhang et al. proposed an efficient Chebyshev polynomial algorithm and based on it [15], they further constructed the electric vehicles authentication and session key negotiation scheme for a smart grid environment. However, this scheme also requires the device to enter a password for login to continue authentication. Wang et al. proposed an authentication scheme for smart grids, but the scheme has a high computational cost and cannot withstand physical attacks [16].

1) Unable to withstand physical attacks and machine learning modeling attacks. An attacker can obtain secret information such as Challenge and Response Pairs (CRPs) stored in the device's memory and simulate the original PUF with a machine learning algorithm based on the known CRPs, which destroys the unclonable and unpredictable nature of the PUF [17], [18], [19]. The schemes proposed in the literatures [3], [4], [6], [10], and [12] in which the attacker can directly or indirectly access the CRPs, rendering them vulnerable to machine learning modeling attacks. The schemes proposed in the literatures [12], [14], and [16] store secret values in the device in plain text, making them susceptible to physical attacks. Consequently, these schemes are not suitable for power IoT terminal devices.
2) Information such as passwords or fingerprints are required. Most of the devices in the power IoT are deployed in remote areas where operations such as password entry and entering fingerprint information are not possible.
3) High computational cost. Literatures [10], [11], and [12] uses elliptic curve cryptographic algorithms as well as symmetric encryption algorithms, which have high computational costs and do not apply to resource-constrained power IoT devices.

B. CONTRIBUTIONS

To address the above problems, this paper proposes a lightweight authentication scheme for power IoT based on PUF and Chebyshev chaotic map, which is suitable for resource-constrained power IoT devices. The main contributions of this paper are as follows:

1) A lightweight anonymous authentication scheme for power IoT devices is proposed. This scheme achieves two-way authentication and session key negotiation between the terminal device and the gateway without entering any password or biological information. The scheme uses PUF technology to generate unique device identifiers for two-way authentication and session key negotiation, does not store any secret information such as CRPs for authentication within the device. Additionally, it protects secret information such as CRPs transmitted within insecure channels by utilizing the Chebyshev chaotic map, so that the scheme can defend against attacks such as physical and machine learning modelling.
2) Formal and informal security analyses of the scenarios using improved BAN logic and the ProVerif tool to verify the rigour of the scheme's logical structure and protocol flow. This analysis comprehensively considers the scheme's ability to combat potential threats and effectively demonstrates its high reliability in protecting data integrity and privacy security.
3) Comparative analysis of the security performance, computational cost, and communication cost of the proposed scheme with the authentication schemes in the literatures [10], [11], [31], [32], and [33], after analysis, it can be seen that the proposed scheme in this paper satisfies the security attributes such as anonymity, untraceability, forward/backward confidentiality, etc. while possessing low computational and communication costs, which makes it suitable to be deployed in resource-constrained devices.

C. ORGANIZATION

This paper will describe some preparatory knowledge that needs to be used in this paper, including PUF, Chebyshev chaotic map, threat model, and system model in Section II. In Section III, a lightweight authentication scheme for power IoT based on PUF and Chebyshev chaotic map is proposed, including the registration phase and authentication phase. Formal and informal security analysis of the proposed scheme is performed in Section IV. In Section V the proposed scheme of this paper is compared with the schemes in literatures [10], [11], [31], [32], and [33] in terms of security performance, computational cost, and communication cost. Finally, Section VI concludes the paper.

II. PRELIMINARIES AND SYSTEM MODEL

A. PHYSICAL UNCLONABLE FUNCTION

Traditional authentication schemes typically store keys or other secret information in Electrically Erasable Programmable Read-Only Memory (EEPROM) or Static Random Access Memory (SRAM) and use cryptographic operations to protect this information. However, this storage method is vulnerable to a variety of attacks. PUF is a technique that uses the physical properties of small inhomogeneities in a chip or hardware device to generate unique identifiers, which plays an important role in the fields of authentication and key generation, etc. It does not require storing the key or secret information in memory, but obtains the response from the physical properties of the integrated circuits, and has the advantages of low power consumption and ease of fabrication. This unique working method makes it difficult for an attacker to obtain secret information from the memory, thus enhancing the security of the system. However, PUF is susceptible to environmental factors such as

temperature variations and circuit noise, which may cause PUF to respond differently to the same input challenge. Therefore, PUF need to take these factors into account in practical applications and take appropriate measures to reduce such effects to ensure the stability and reliability of the output response [20], [21].

The PUF works based on small differences in the manufacturing process of a device, which uses these small differences to map the input challenge $C = \{0, 1\}^{l_1}$ of the hardware to an output space $R = \{0, 1\}^{l_2}$ [8]. This mapping is unique and unclonable and can be used as a unique identifier for a device, this mapping can be expressed as:

$$R \leftarrow \mathrm{PUF}(C) \tag{1}$$

It is assumed in this paper for the proposed scheme that each terminal device is embedded with an ideal PUF chip, which is not affected by noise. The ideal PUF has the following properties [9]:

1) UNCLONABILITY

The unclonability of the PUF is manifested by the fact that it will have the same output response for any number of identical input excitations, different output responses for any number of different input excitations, and different output responses for the same input excitation from different devices.

2) UNPREDICTABILITY

The unpredictability of the PUF is demonstrated by the fact that given a set of excitation and response pairs, the corresponding response R_i cannot be predicted by randomly selecting the excitation C_i.

3) RANDOMNESS

The output of the PUF is random, and even small physical differences will cause large variations in response.

B. CHEBYSHEV CHAOTIC MAP

The highly random, sensitive and nonlinear properties of Chebyshev chaotic map make it promising for a wide range of applications in the field of authentication. Comparing with other cryptographic methods such as exponential and elliptic curve operations, Chebyshev chaotic map not only consumes less energy but also provides higher security, which makes Chebyshev chaotic map more advantageous in resource-constrained or power-sensitive environments. Obfuscation and encryption of secret information can be achieved by performing heterodyne operation with extended Chebyshev chaotic map polynomials. The randomness of the chaotic map ensures that the result of the heterodyne operation is highly unpredictable, and obtaining the extended Chebyshev polynomials will face mathematical difficulties, which increases the difficulty and cost of the attack. This section briefly introduces the definitions as well as properties related to Chebyshev chaotic map [15].

1) CHEBYSHEV POLYNOMIAL

Let n be a positive integer, $x \in [-1, 1]$, and the Chebyshev polynomial $T_n(x)$ of order n is shown below:

$$T_n(x) = cos(n \times arccos(x)) \tag{2}$$

The nth order Chebyshev polynomials also have the following equivalent recursive definition:

$$T_n(x) = \begin{cases} 1 & n = 0 \\ x & n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x) & n \geq 2 \end{cases} \tag{3}$$

2) CHAOTIC PROPERTY

When $n \geq 2$, $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ is a chaotic map with invariant density $f^*(x) = 1 \Big/ [\pi\sqrt{(1 - x^2)}]$ for positive Lyapunov exponents ln(n) > 0.

3) SEMIGROUP PROPERTY

When $x \in [-1, 1]$ and $r, s \in N$, Chebyshev polynomials have the following property:

$$T_r(T_s(x)) = T_{s \cdot r}(x) = T_s(T_r(x)) \tag{4}$$

Zhang [22] proved in 2008 that Chebyshev polynomials in the interval $x \in (-\infty, +\infty)$ still have the semigroup property.

4) EXTENDED CHEBYSHEV POLYNOMIAL

Let n be a positive integer, $x \in (-\infty, +\infty)$, n order extended Chebyshev polynomial is shown below:

$$T_n(x) = cos(n \times arccos(x)) \bmod p \tag{5}$$

Its equivalent recursion is defined as follows:

$$T_n(x) = \begin{cases} 1 & n = 0 \\ x \bmod p & n = 1 \\ (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p & n \geq 2 \end{cases} \tag{6}$$

5) EXTENDED CHEBYSHEV POLYNOMIAL SEMIGROUP PROPERTY

When $x \in (-\infty, +\infty)$ and $r, s \in N$, the extended Chebyshev polynomials have the following properties:

$$T_r(T_s(x)) = T_{s \cdot r}(x) = T_s(T_r(x)) \bmod p \tag{7}$$

In this paper, we are going to use the heterodyne operation of extended Chebyshev polynomials with secret information to secure the secret information in the proposed authentication scheme. However, an attacker will face the following three difficulties when trying to obtain the extended Chebyshev polynomials [14]:

6) CHAOTIC MAP DISCRETE LOGARITHM PROBLEM (CMDLP)

Given x, p, y, finding a positive integer r such that $T_r(x) \bmod p \equiv y$ holds is difficult.

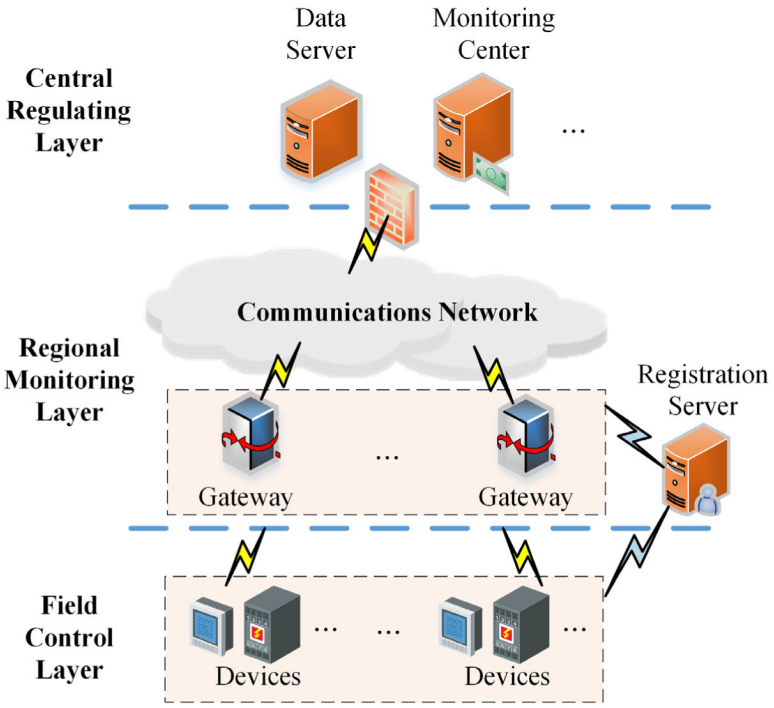

FIGURE 1. Power IoT SCADA system architecture.

7) CHAOTIC MAP COMPUTATIONAL DIFFIE-HELLMAN PROBLEM (CMCDHP)

Given x, p, $T_r(x)\text{mod } p$, and $T_s(x)\text{mod } p$ finding a positive integer y such that $T_{r\cdot s}(x) \bmod p \equiv y$ holds is difficult.

8) CHAOTIC MAP JUDGEMENTAL DIFFIE-HELLMAN PROBLEM (CMJDHP)

Given x, p, $T_r(x) \bmod p$, $T_s(x) \bmod p$, and $T_z(x) \bmod p$, where $r, s, z \geq 2$, $x \in (-\infty, +\infty)$, it is difficult to determine $T_{r\cdot s}(x) \equiv T_z(x) \bmod p$.

C. POWER IoT SCADA SYSTEM MODEL

Combined with the literatures [23], [24], [25], and [26], this paper gives the architecture of a typical power IoT SCADA system, as shown in Fig. 1, which is divided into the field control layer, the regional monitoring layer, and the central regulating layer. The field control layer includes smart meters, remote control units, and other terminal devices, which are responsible for field data collection and execution of control commands. The regional monitoring layer consists of gateways, programmable logic controllers, Registration Server (RS), and other devices, which are responsible for collecting data and uploading them to the upper server, as well as executing the commands issued by the central regulating layer and adjusting the operating parameters of the system. The central regulating layer consists of data servers, monitoring centers, and other equipment, responsible for monitoring and controlling the operating status of this system, real-time processing and analyzing data, thus carrying out alarm processing and troubleshooting. The scheme proposed in this paper takes the power IoT SCADA system as an example to achieve two-way authentication between the terminal device and the gateway, which consists of the following three parties:

1) REGISTRATION SERVER

It is located in the regional monitoring layer of the power IoT SCADA system and is responsible for the registration of gateways and devices, without participating in the subsequent authentication, which is completed by gateways and terminal devices.

2) GATEWAY

The gateway is located in the regional monitoring layer of the power IoT SCADA system and is responsible for uploading the data collected by the terminals to the data server or monitoring center in the central regulating layer.

3) TERMINAL DEVICE

Located in the field control layer of the power IoT SCADA system, it is responsible for collecting data from field devices and transmitting the collected data to the gateway in the upper layer.

D. DOLEV-YAO THREAT MODEL

The Dolev-Yao threat model [27] is widely used for the security analysis of authentication schemes. According to the Dolev-Yao threat model, this paper assumes that the attacker has the following capabilities [28]:

1) The gateways as well as RS computing and security protection are strong enough to secure the secret value

while completing complex computations, whereas the devices are weak enough to allow attackers to potentially access the device memory through physical attacks.

2) The registration phase is done within the secure channel, whereas in the two-way authentication phase between the device and the gateway, an attacker can steal, forge, and tamper with the transmitted messages as well as use the acquired messages to impersonate the legitimate devices and gateways through various attacks.
3) Attackers can model the structure of the PUF and predict the CRPs through machine learning algorithms. Attackers can access the information stored in the device through physical attacks and other means, but any attempt to destroy or tamper with the PUF will make it unavailable.

III. PROPOSED SCHEME BASED ON PUF AND CHEBYSHEV CHAOTIC MAP

This paper provides a reliable authentication scheme for resource-constrained terminal devices in the power IoT. The lightweight security primitive PUF is utilized to effectively resist physical attacks and ensure the security of the identity and secret information of the terminal devices. Since the Chebyshev chaotic map has the characteristics of lightweight, high randomness, and unpredictability. The proposed scheme in this paper adopts the Chebyshev chaotic map with secret information heterodyne to ensure the confidentiality and integrity of information transmission.

For the proposed scheme, we assume that each terminal device is embedded with a PUF chip. The PUF embedded in the device can meet indicators such as randomness, unpredictability, and unclonability. It is an ideal PUF, which is not affected by noise. The scheme includes a registration phase and a two-way authentication phase. Related symbols are shown in Table 1.

TABLE 1. Related symbol description.

Symbol	Description
D_i, GW_i	Device, gateway
AID_i, AID_{TM}	Pseudo-identity of the device in round i
ID_i, ID_{GWi}	The true identity of the device
$h()$	One-way hash function
$\|\|$	Connection operation
(C_i, R_i)	Challenge and response pair
$T_r(x)$	Chebyshev polynomial
N_d, N_u, N_s, r, s	Random number
T, T_u, T_s	Timestamp
$\oplus$	Heterodyne operation
SK	Session key

A. REGISTRATION PHASE

The device and gateway registration phase is shown in Fig. 2. In the registration phase, the device and the gateway register with the RS through the secure channel to obtain the required authentication parameters. The specific registration steps are as follows:

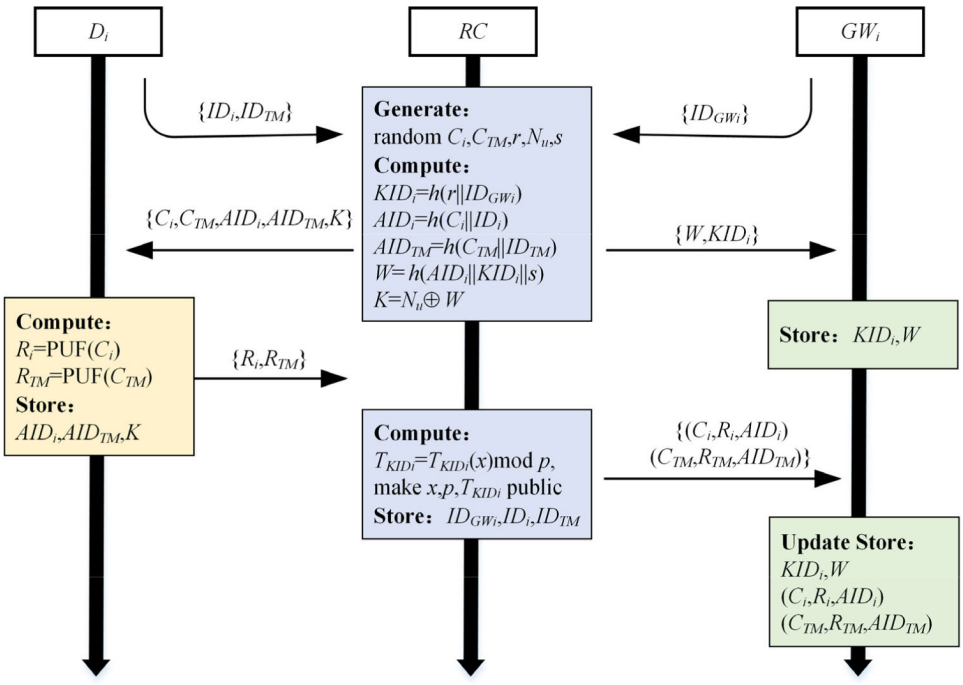

FIGURE 2. Registration phase.

1) STEP 1

D_i selects its own identity ID_i and temporary identity ID_{TM}, sending them to the RS; GW_i selects its own identity ID_{Gwi}, sending it to the RS.

2) STEP 2

RS generates random number C_i, C_{TM}, r, N_u, s, then computes pseudo-identity $AID_i = h(C_i||ID_i)$, synchronizes pseudo-identity $AID_{TM} = h(C_{TM}||ID_{TM})$ for D_i, pseudo-identity $KID_i = h(r||ID_{GWi})$ for GW_i, then computes shared secrets $W = h(AID_i||KID_i||s)$ and $K = N_u \oplus W$ for GW_i and D_i, which sends message $\{C_i, C_{TM}, AID_i, AID_{TM}, K\}$ to D_i and message $\{W, KID_i\}$ to GW_i.

3) STEP 3

D_i gets the message, stores $\{AID_i, AID_{TM}, K\}$ into the device, which uses C_i and C_{TM} in the message as inputs to the PUF, computes the responses R_i and R_{TM}, and sends the message $\{R_i, R_{TM}\}$ to the RS; GW_i stores the message $\{KID_i, W\}$ securely into the gateway memory.

4) STEP 4

RS computes $T_{KIDi} = T_{KIDi}(x) \bmod p$, then exposes x, p, T_{KIDi}. In addition, RS stores $\{ID_{Gwi}, ID_i, ID_{TM}\}$ and sends $\{(C_i, R_i, AID_i), (C_{TM}, R_{TM}, AID_{TM})\}$ to GW_i.

5) STEP 5

GW_i updates the stored information to $\{KID_i, W, (C_i, R_i, AID_i), (C_{TM}, R_{TM}, AID_{TM})\}$.

B. 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:

1) STEP 1

D_i generates random number N_d, then computes $T_{Nd} = T_{Nd}(x) \bmod p$, $T_{Nd\cdot KIDi} = T_{Nd}(T_{KIDi}) \bmod p$, $K^* = K \oplus T_{Nd\cdot KIDi}$, then generates request authentication message $\{T_{Nd}, AID_i, K^*\}$ and send to GW_i.

2) STEP 2.1

After receiving the authentication request from D_i, GW_i will first look for AID_i in the database, if AID_i is not in the database of the gateway, then GW_i will reject the authentication request from D_i, then D_i will initiate the authentication request again by using AID_{TM}. Meanwhile, GW_i will utilize $(C_{TM}, R_{TM}, AID_{TM})$ to authenticate the device. Otherwise, GW_i will read (C_i, R_i) and generate a random number N_s and timestamp T_s.

3) STEP 2.2

GW_i computes $T_{Nd\cdot KIDi} = T_{KIDi}(T_{Nd}) \bmod p$, $C_i^* = C_i \oplus T_{Nd\cdot KIDi}$, $N_u = K^* \oplus T_{Nd\cdot KIDi} \oplus W$, $T_{Ri\cdot Nd\cdot KIDi} = T_{Ri}(T_{Nd\cdot KIDi}) \bmod p$, $R_i \oplus W$, $N_s^* = N_s \oplus T_{Ri\cdot Nd\cdot KIDi}$, $V_0 = h(T_{Ri\cdot Nd\cdot KIDi}||N_u||N_s||T_s)$, then generates the message $\{C_i^*, N_s^*, R_i \oplus W, V_0, T_s\}$ and sends the message to D_i.

4) STEP 3.1

D_i checks if the transmission delay is less than Δt, i.e. $|T\text{-}T_s| < \Delta t$, if it is greater than or equal to Δt then end the authentication.

5) STEP 3.2

D_i computes $C_i = C_i^* \oplus T_{Nd\cdot KIDi}$, $T_{Ri\cdot Nd\cdot KIDi} = T_{Ri}(T_{Nd\cdot KIDi}) \bmod p$, $R_i = \mathrm{PUF}(C_i)$, $N_s = N_s^* \oplus T_{Ri\cdot Nd\cdot KIDi}$, gets $W = R_i \oplus W \oplus R_i$, $N_u = K \oplus W$, then computes V_0'. If V_0' is equal to V_0, D_i then the authentication to GW_i is successful, otherwise D_i fails to authenticate to GW_i.

6) STEP 3.3

D_i generates timestamp T_u, random number n, computes $C_{i+1} = h(C_i||N_u)$, $R_{i+1} = \mathrm{PUF}(C_{i+1})$, $SK = h(N_u||R_{i+1}||T_{Ri\cdot Nd\cdot KIDi})$, $AID_{i+1} = h(AID_i||R_i||N_s)$, $V_1 = h(N_s||SK||T_u)$, $R_{i+1}^* = R_{i+1} \oplus N_s$, $N_u' = n$, $K' = N_u' \oplus W$, and generates message $\{R_{i+1}^*, V_1, T_u\}$ and stores $\{AID_{i+1}, K'\}$ to D_i.

7) STEP 4.1

GW_i checks if the transmission delay is less than Δt, i.e. $|T\text{-}T_u| < \Delta t$, if it is greater than or equal to Δt then end the authentication.

8) STEP 4.2

GW_i computes $R_{i+1} = R_{i+1}^* \oplus N_s$, $SK = h(N_u||R_{i+1}||T_{Ri\cdot Nd\cdot KIDi})$, V_1', if V_1' is equal to V_1, then GW_i is successful in authenticating D_i, otherwise, GW_i fails in authenticating D_i.

9) STEP 4.3

GW_i computes $C_{i+1} = h(C_i||N_u)$, $AID_{i+1} = h(AID_i||R_i||N_s)$ and store $\{(C_{i+1}, R_{i+1}, AID_{i+1})\}$ into the gateway memory.

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME BASED ON PUF AND CHEBYSHEV CHAOTIC MAP

A. FORMAL SECURITY ANALYSIS USING IMPROVED BAN LOGIC

The BAN logic proposed by Burrows et al. [29] in 1989 has been widely used for security analysis of schemes. In this paper, we use the improved BAN logic [30] to analyze the proposed authentication scheme. We use A, B, P, and Q to denote the body of the communication, M and N to denote the message, X, Y, and Z to denote the formula. Table 2 shows the improved BAN logic expressions and descriptions.

In the improved BAN logic, the inference rules used in this paper are shown in Table 3.

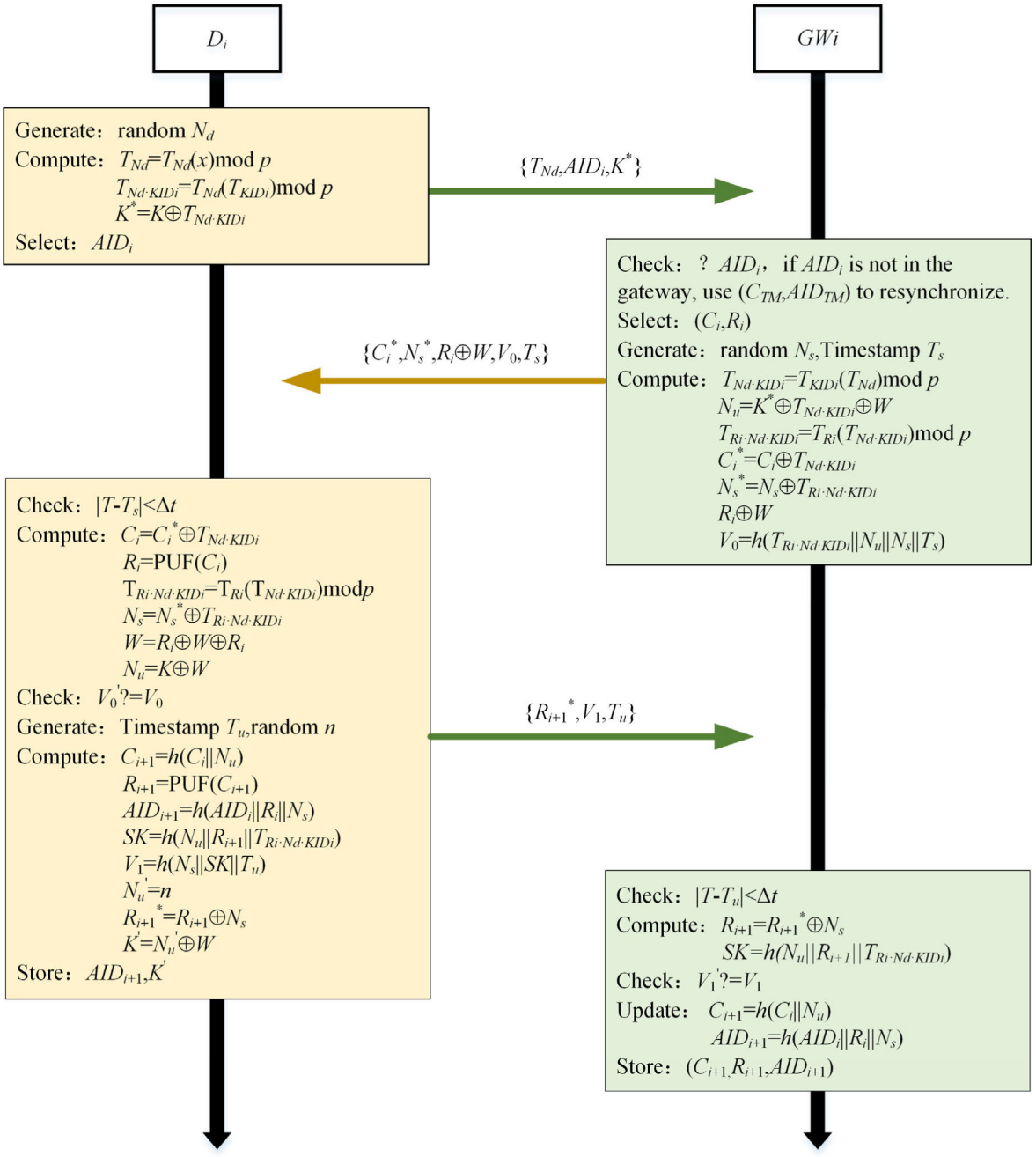

FIGURE 3. Authentication phase.

Utilize improved BAN logic to prove the secure sharing of N_s, R_{i+1}, $T_{Ri\cdot Nd\cdot KIDi}$ between the device and the gateway, ensuring that attackers cannot obtain these secrets. The security proof of N_s, R_{i+1}, $T_{Ri\cdot Nd\cdot KIDi}$ is illustrated in Fig. 4. First, idealize the communication messages between the device and the gateway. The idealized results are as follows:

1) $D \rightarrow GW : T_{Nd}, AID_i, N_u$.
2) $GW \rightarrow D : N_u \Re T_{Ri\cdot Nd\cdot KIDi} \Re N_s \Re T_s$.
3) $D \rightarrow GW : N_s \Re T_{Ri\cdot Nd\cdot KIDi} \Re R_{i+1} \Re T_u$.

The following assumptions are then made about the proposed authentication scheme:

1) $D| \equiv D \overset{Ri}{\leftrightarrow} GW, GW| \equiv D \overset{Ri}{\leftrightarrow} GW$: The gateway saves the CRPs of each device during the registration phase. The device can use the PUF to compute the response R_i.
2) $GW| \equiv \{D\}^C \triangleleft ||N_s$ and $D| \equiv GW| \equiv \{D\}^C \triangleleft ||N_s$: The gateway generates the random number N_s.
3) $D| \equiv \{GW\}^C \triangleleft ||R_{i+1}$ and $GW| \equiv D| \equiv \{GW\}^C \triangleleft ||R_{i+1}$: The device utilizes the PUF function to generate a new response R_{i+1}.
4) $D| \equiv GW| \equiv \{D\}^C \triangleleft ||T_{Ri\cdot Nd\cdot KIDi}$ and $GW| \equiv \{D\}^C \triangleleft ||T_{Ri\cdot Nd\cdot KIDi}$: The gateway computes $T_{Ri\cdot Nd\cdot KIDi}$.

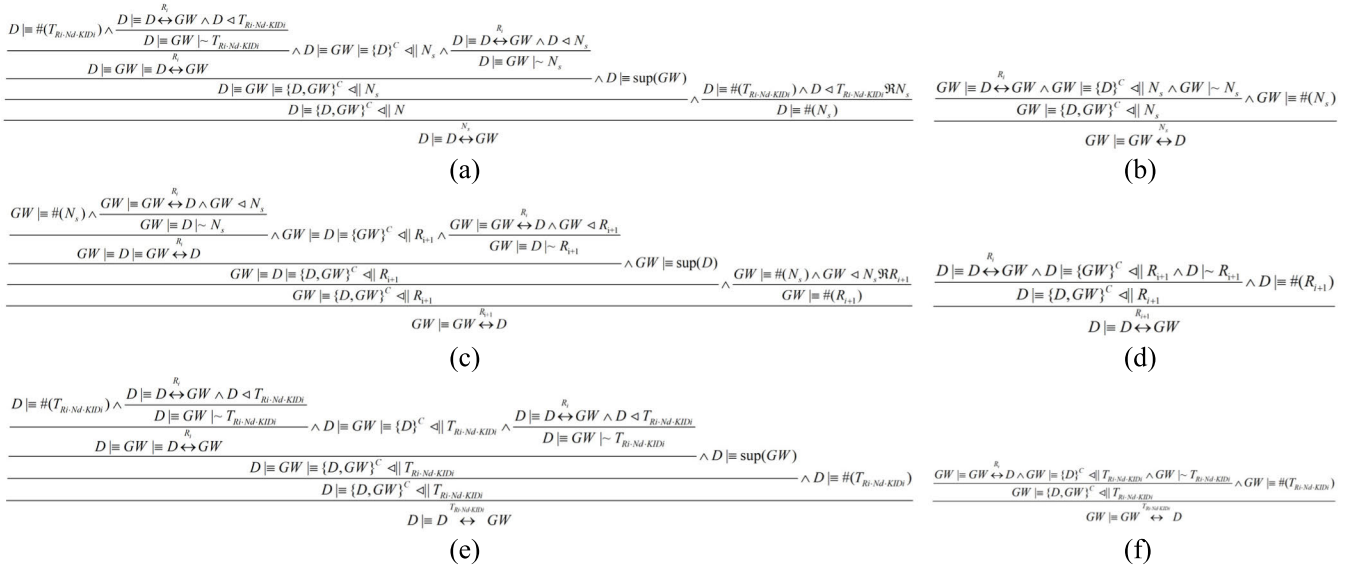

FIGURE 4. Security proof of N_s, R_{i+1}, $T_{Ri\cdot Nd\cdot KIDi}$ by improved BAN logic. (a) D believes that N_s is a shared secret between D and GW, (b) GW believes that N_s is a shared secret between GW and D, (c) GW believes that R_{i+1} is a shared secret between GW and D, (d) D believes that R_{i+1} is a shared secret between D and GW, (e) D believes that $T_{Ri\cdot Nd\cdot KIDi}$ is a shared secret between D and GW, and (f) GW believes that $T_{Ri\cdot Nd\cdot KIDi}$ is a shared secret between GW and D.

TABLE 2. Improved BAN logic expressions and descriptions.

Expression	Description
$P \mid\equiv X$	P believes that X is true.
$P \overset{K}{\mid\sim} X$	P encrypts message X using key K.
$P \overset{K}{<} X$	P has received a message X encrypted with K.
$P \overset{K}{\leftrightarrow} Q$	The key K is shared between P and Q.
$P \overset{X}{f} Q$	The secret X is shared between P and Q.
$\#(X)$	X is within the validity period.
$\sup(S)$	S is a credible party.
$P <\!\!\mid M$	P does not know the message M.
$P \mid\equiv X$	P believes that X is true.
$P \overset{K}{\mid\sim} X$	P encrypts message X using key K.
$P \overset{K}{<} X$	P has received a message X encrypted with K.
$P \overset{K}{\leftrightarrow} Q$	The key K is shared between P and Q.

5) $D\mid\equiv \#(N_d), D\mid\equiv \#(R_{i+1}), D\mid\equiv \#(n), D\mid\equiv \#(T_u), D\mid\equiv \#(T_{Ri\cdot Nd\cdot KIDi})$: N_d, R_{i+1}, n, T_u, $T_{Ri\cdot Nd\cdot KIDi}$, are within the validity period.
6) $GW\mid\equiv \#(N_s), GW\mid\equiv \#(T_{Ri\cdot Nd\cdot KIDi}), GW\mid\equiv \#(T_s)$: N_s, $T_{Ri\cdot Nd\cdot KIDi}$, T_s are within the validity period.
7) $D\mid\equiv \sup(GW), GW\mid\equiv \sup(D)$: Gateway and device trust each other.
8) $D \lhd N_u \Re N_s, D \lhd T_{Ri\cdot Nd\cdot KIDi} \Re N_s$: Message 2 in the idealized scenario.
9) $GW \lhd T_{Ri\cdot Nd\cdot KIDi} \Re R_{i+1}, GW \lhd N_s \Re R_{i+1}$: Message 3 in the idealized scenario.

TABLE 3. Improved BAN logic rules.

Rule	Expression
Authentication rule	$\dfrac{P\mid\equiv P\overset{K}{\leftrightarrow}Q \wedge P\overset{K}{<}M}{P\mid\equiv Q\overset{K}{\mid\sim}M}$
Confidentiality rule	$\dfrac{P\mid\equiv P\overset{K}{\leftrightarrow}Q \wedge P\mid\equiv S^C <\!\!\mid M \wedge P\overset{K}{\mid\sim}M}{P\mid\equiv (S\cup\{Q\})^C <\!\!\mid M}$
Nonce-verification rule	$\dfrac{P\mid\equiv \#(M) \wedge P\mid\equiv Q\overset{K}{\mid\sim}M}{P\mid\equiv Q\mid\equiv P\overset{K}{\leftrightarrow}Q}$
Super-principal rule	$\dfrac{P\mid\equiv Q\mid\equiv X \wedge P\mid\equiv \sup(Q)}{P\mid\equiv X}$
Fresh rule	$\dfrac{P\mid\equiv \#(M) \wedge P< M\Re N}{P\mid\equiv \#(N)}$
Good-key rule	$\dfrac{P\mid\equiv \{P,Q\}^C <\!\!\mid K \wedge P\mid\equiv \#(K)}{P\mid\equiv P\overset{K}{\leftrightarrow}Q}$
Derivation rule	$\dfrac{P\mid\equiv Q\mid\equiv P\overset{K}{\leftrightarrow}Q \wedge P\mid\equiv Q\mid\equiv S^C <\!\!\mid M \wedge P\overset{K}{\mid\sim}M}{P\mid\equiv Q\mid\equiv (S\cup\{P\})^C <\!\!\mid M}$
Intuitive rules	$\dfrac{P\overset{K}{<}M}{P<M}, \dfrac{P\overset{K}{\mid\sim}M}{P\mid\sim M}, \dfrac{P\mid\sim (M,Q)}{P\mid\sim M}$ $\dfrac{P<M\Re N}{P<M \wedge P<N}, \dfrac{P<M \mid N}{P<M \wedge P<N}$

B. FORMAL SECURITY VERIFICATION USING PROVERIF

ProVerif is an automated tool for formal verification of authentication schemes under the Dolev-Yao model for verifying security properties such as confidentiality, authentication, and anonymity as well as detecting whether the scheme is resilient to attacks such as replay, DoS, and session

```
(*----------------------------RS Registration Phase-------------------------*)
let RS =
    in (sch1,IDi:bitstring);
    in (sch2,(IDGWi:bitstring));
    new C:bitstring;
    new r:bitstring;
    new Nu:bitstring;
    new s:bitstring;
    let KID=h1(r,IDGWi) in
    let AID=h1(C,IDi) in
    let W=h2(AID,KID,s) in
    let K=xor(Nu,W) in
    out (sch1,(C,AID,K));
    out (sch2,(W,KID));
    in (sch1,R:bitstring);
    out (sch2,(C,R,AID));
    let T=Cheb(KID,x) in
    0.
```

FIGURE 5. Running code of the RS process.

```
(*---------------Device Registration and Authentication---------------*)
(*Device Registration Phase*)
let Device =
    out (sch1,IDi);
    in (sch1,(C:bitstring,AID:bitstring,K:bitstring));
    let R=PUF(C) in
    out (sch1,R);
(*Device Authentication Phase*)
    new Nd:bitstring;
    let X=Cheb(Nd,x) in
    let X1=Cheb(Nd,T) in
    let K_=xor(K,X1) in
    out (ch,(X,AID,K_));
    event StartDeviceAuth;
    in(ch,(xC_:bitstring,xNs_:bitstring,xV0:bitstring,
    xW_:bitstring,xTs:bitstring));
    let C'=xor(xC_,X1) in
    let R'=PUF(C') in
    let X2'=Cheb(R',X1) in
    let Ns'=xor(xNs_,X2') in
    let W'=xor(R',xW_) in
    let Nu'=xor(K,W') in
    let V0'=h3(X2',Nu',Ns',xTs) in
    if V0'=xV0 then
    event EndDeviceAuth;
    new Tu:bitstring;
    new n:bitstring;
    let C1=h1(C',Nu') in
    let R1=PUF(C1) in
    let AID1=h2(AID,R',Ns') in
    let SK=h2(Nu',R1,X2') in
    let V1=h2(Ns',SK,Tu) in
    let Nu1=n in
    let R1_=xor(R1,Ns') in
    out(ch,(R1_,V1,Tu));
    0.
```

FIGURE 6. Running code of the device process.

key leakage. In this paper, ProVerif is used to simulate the registration, authentication, and key exchange processes as well as to verify the security of the proposed scheme. Under the Dolev-Yao model, the proposed scheme consists of three processes: Device, Gateway, and RS. Fig. 5 shows the running code of the RS process of the simulated proposed scheme, Fig. 6 shows the running code of the Device process of the simulated proposed scheme, and Fig. 7 shows the running code of the Gateway process of the simulated proposed scheme.

```
(*----------------Gateway Registration and Authentication-------------*)
(*Gateway Registration Phase*)
let Gateway=
    out (sch2,IDGWi);
    in (sch2,(W:bitstring,KID:bitstring));
    in (sch2,(C:bitstring,R:bitstring,AID:bitstring));
(*Gateway Authentication Phase*)
    in (ch,(xX:bitstring,xAID:bitstring,xK_:bitstring));
    new Ns:bitstring;
    new Ts:bitstring;
    let X1'=Cheb(KID,xX) in
    let K'=xor(X1',xK_) in
    let Nu=xor(K',W) in
    let X2=Cheb(R,X1') in
    let C_=xor(C,X1') in
    let Ns_=xor(Ns,X2) in
    let W_=xor(R,W) in
    let V0=h3(X2,Nu,Ns,Ts) in
    out(ch,(C_,Ns_,W_,V0,Ts));
    event StartGatewayAuth;
    in(ch,(xR1_:bitstring,xV1:bitstring,xTu:bitstring));
    let R1'=xor(xR1_,Ns) in
    let SK'=h2(Nu,R1',X2) in
    let V1'=h2(Ns,SK',xTu) in
    if V1'=xV1 then
    event EndGatewayAuth;
    let C1'=h1(C,Nu) in
    let AID1'=h2(AID,R,Ns) in
    0.
```

FIGURE 7. Running code of the gateway process.

```
Verification summary
Quary not attacker(SK[]) is true.
Quary not attacker(SK'[]) is true.
Quary not attacker(W[]) is true.
Quary not attacker(K[]) is true.
Quary not attacker(IDi[]) is true.
Quary not attacker(IDGWi[]) is true.
Quary inj-event(EndDeviceAuth) ==> inj-event(StartDeviceAuth) is true.
Quary inj-event(EndGatewayAuth) ==> inj-event(StartGatewayAuth) is true.
```

FIGURE 8. Output of ProVerif query for device process.

When simulating this scheme, the security of the session keys SK, SK', device identity ID_i, gateway identity ID_{GWi}, secrets K, W between the device and the gateway, and the identity authentication attributes of the device and the gateway were queried. Fig. 8 and Fig. 9 show the results of ProVerif querying the Device and Gateway processes. From the query results, we can see that the proposed scheme has security attributes such as confidentiality, authentication, and anonymity.

C. INFORMAL SECURITY ANALYSIS

1) TWO-WAY AUTHENTICATION

The proposed scheme in this paper enables two-way authentication between the device and the gateway. The device authenticates the gateway by verifying whether $V_0' = V_0$ is valid, and the gateway authenticates the device by verifying whether $V_1' = V_1$ is valid. Since the expressions of V_0 and V_1 contain secret values such as $T_{Ri\cdot Nd\cdot KIDi}$, N_u, N_s, R_{i+1}, obtaining $T_{Nd\cdot KIDi}$ and $T_{Ri\cdot Nd\cdot KIDi}$ will face the chaotic map discrete logarithm problem and the chaotic map computational Diffie-Hellman problem. In addition, N_u, N_s, and R_{i+1} are not transmitted in plain text, so it is impossible for an attacker to obtain any secret values, and thus cannot impersonate a

```
Verification summary
Quary not attacker(SK[]) is true.
Quary not attacker(SK'[]) is true.
Quary not attacker(W[]) is true.
Quary not attacker(K[]) is true.
Quary not attacker(IDi[]) is true.
Quary not attacker(IDGWi[]) is true.
Quary inj-event(EndDeviceAuth) ==> inj-event(StartDeviceAuth) is true.
Quary inj-event(EndGatewayAuth) ==> inj-event(StartGatewayAuth) is true.
```

FIGURE 9. Output of the gateway process ProVerif query.

legitimate terminal device to participate in the authentication with the gateway.

2) ANONYMITY AND UNTRACEABILITY

The device and the gateway use pseudo-identity in the authentication process, which is updated after each authentication. The attacker cannot obtain the real identities ID_i and ID_{TM}, thus the proposed scheme is anonymous and untraceable.

3) RESISTANCE TO TAMPER ATTACKS

Attackers can capture the message transmitted in an insecure channel and tamper with it, whereas the information interacted during the authentication process of the proposed scheme in this paper is protected by hash function or bitwise heterodyne operation, so the attacker cannot access the secret values in the message. Therefore, the proposed scheme in this paper can resist tampering attacks.

4) RESISTANCE TO CLONING AND PHYSICAL ATTACKS

An attacker can access the device memory to obtain sensitive information through physical attacks, but the device only stores pseudo-identity and K, which cannot obtain authentication-related secret values such as N_u. In addition, PUF has characteristics such as unclonability. An attacker's attempt to obtain a PUF response will destroy the function of the original PUF. Hence, the attacker cannot execute a cloning attack to impersonate a legitimate device during authentication or obtain sensitive information through physical attacks.

5) RESISTANCE TO MACHINE LEARNING MODELING ATTACKS

The attacker uses the collected CRPs and machine learning algorithms to construct a PUF response model to predict the CRPs. In the proposed scheme in this paper, the attacker can only capture the CRPs from the insecure channel, yet obtaining the challenge value C_i needs to obtain $T_{Nd\cdot KIDi}$ first, the calculation of $T_{Nd\cdot KIDi}$ will face the problem of chaotic map discrete logarithm problem, thus the attacker is unable to obtain C_i. The response value R_i is hashed by a hash function, due to the unidirectionality of the hash function, the attacker cannot obtain R_i either. Therefore the attacker cannot collect the CRPs generated by the PUF, so the proposed scheme is resistant to machine learning modeling attacks.

6) RESISTANCE TO IMPERSONATION ATTACKS

When attackers want to pretend to be a legitimate device, they need to send the correct AID_i, K^*, V_1, R^*_{i+1} to the gateway. However, generating the correct V_1 requires the correct $T_{Ri\cdot Nd\cdot KIDi}$, N_u, N_s, R_{i+1}. From the above analysis, it is clear that the attacker cannot obtain the correct $T_{Nd\cdot KIDi}$, $T_{Ri\cdot Nd\cdot KIDi}$, R_{i+1}, N_u, N_s. Therefore, the attacker cannot impersonate a legitimate device to authenticate with the gateway.

When attackers want to pretend to be a gateway, they need the correct CRPs and send V_0, C^*_i, N^*_s, and $R_i \oplus W$ to the device. From the above analysis, it can be seen that the attacker is unable to obtain the correct CRPs, $T_{Nd\cdot KIDi}$ and $T_{Ri\cdot Nd\cdot KIDi}$. Therefore the attacker is unable to disguise as a legitimate gateway to authenticate with the device.

7) RESISTANCE TO REPLAY ATTACKS

The proposed scheme introduces timestamps to check whether the transmission delay meets the requirements before authentication, thus the attacker cannot launch a replay attack by resending messages. In addition, this scheme also adds timestamps to V_0 and V_1. Therefore, if the attacker launches an attack by changing timestamps, it will lead to authentication failure. Meanwhile, the secret values in V_0 and V_1 will be updated after each authentication, thus the proposed scheme can resist replay attacks.

8) RESISTANCE TO DoS ATTACKS AND DESYNCHRONIZATION ATTACKS

When an attacker sends a large amount of useless information to block the communication between the device and the gateway, the device and the gateway will first check the validity of the transmission delay before verifying the value of V_0 or V_1. Failure to meet the requirements of any one of them will result in denial of authentication. When the communication between the device and the gateway is interrupted, the device will use the temporary pseudo-identity AID_{TM} to initiate the authentication request again, and the gateway will use (C_{TM}, R_{TM}) to authenticate the device. Therefore, the proposed scheme in this paper can resist DoS and desynchronization attacks.

9) FORWARD/BACKWARD SECURITY

Since the negotiated session key in the proposed scheme in this paper is $SK = h(N_u||R_{i+1}||T_{Ri\cdot Nd\cdot KIDi})$, where N_u, R_{i+1}, $T_{Ri\cdot Nd\cdot KIDi}$ will be updated after each authentication, even if the attacker obtains the secret values of the current device as well as the CRPs attackers will not be able to track the past and future communication data of the device. Therefore, the proposed scheme in this paper has forward/backward security.

TABLE 4. Comparison of security features.

Scheme	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7	SF_8	SF_9	SF_{10}	SF_{11}	SF_{12}
Bai *et al.*[10]	√	√	√	√	√	√	√	×	√	×	√	√
Tanveer *et al.*[11]	√	√	√	√	√	√	×	×	√	√	√	√
Hu *et al.*[31]	√	√	√	√	√	√	×	√	×	×	√	×
Qi *et al.*[32]	√	√	√	√	√	√	√	√	√	×	√	√
Soni *et al.*[33]	√	√	√	√	√	√	√	√	×	√	×	√
Proposed scheme	√	√	√	√	√	√	√	√	√	√	√	√

Note: SF_1: Two-way authentication, SF_2: Untraceability, SF_3: Anonymity, SF_4: Forward/Backward safety, SF_5: DoS attack, SF_6: Replay attack, SF_7: Physical attack, SF_8: Machine learning modeling attack, SF_9: Impersonation attack, SF_{10}: Desynchronization attack, SF_{11}: Man-in-the-middle attack, SF_{12}: Transient secret disclosure attack, √: Signifies available feature, ×: Indicates the feature not available.

V. PERFORMANCE ANALYSIS OF PROPOSED SCHEME BASED ON PUF AND CHEBYSHEV CHAOTIC MAP

In this section, the proposed scheme is evaluated regarding security features, computational cost, and communication cost. And it is compared with some existing schemes.

A. COMPARISON OF SECURITY FEATURES

Table 4 shows the comparison of security features between the scheme proposed in this paper and existing schemes. The literatures [11] and [31] explicitly stores the challenge values or the remaining secret values in the device, rendering it vulnerable to physical attacks. In contrast, this paper only stores the pseudo-identity of the device and the secret value K within the device. Thus, even if an attacker obtains K, they cannot access the secret information. Consequently, the scheme in this paper ensures that secret information remains secure and also enhances the physical security of the device through PUF. In the literatures [10] and [11], attackers obtain CRPs through eavesdropping, impersonation, and other attacks, leaving them susceptible to machine learning modeling attacks. As demonstrated in the previous analysis, the proposed scheme in this paper prevents attackers from acquiring CRPs, thereby fortifying its resilience against machine learning modeling attacks. In the literatures [31] and [33], the authentication value is computationally generated from the secret values stored in the device or the random values generated temporarily by the user, once the device suffers from a physical attack resulting in the leakage of the secret information, the attacker can destroy the authentication through the impersonation attack and man-in-the-middle attack. From the previous analysis, it can be seen that the proposed scheme in this paper can resist the impersonation attack and man-in-the-middle attack. In the schemes in the literatures [10], [31], and [32], the attacker can forge an identity message and send it to the server to interrupt the authentication between the device and the server, so it is susceptible to desynchronization attacks. The proposed scheme in this paper sets up a temporary pseudo-identity AID_{TM} to resynchronize the device, so it is resistant to desynchronization attacks. Literature [31] is vulnerable to transient secret disclosure attacks, when the temporary secret and the information stored in the device are disclosed, the attacker can reproduce the negotiated session key. The negotiated session key of the proposed scheme in this paper requires the attacker to know the PUF responses R_i and R_{i+1} in addition to the temporary secret information N_u. The attacker cannot access the CRPs, so it can resist the transient secret disclosure attack.

B. COMPUTATIONAL COST

In this paper, we use the ZYNQ7000 series FPGA development board to simulate the terminal device, this development board is also equipped with a dual-core ARM Cortex-A9 with a CPU frequency of 767 MHz and 1 GB of RAM. We use a system Core-i5 with a processor of 2.5 GHz and 16 GB of RAM to simulate the gateway, and we use the OpenSSL library to implement the various operations, Table 5 shows the description and execution time of the operations on the device side and the gateway side.

TABLE 5. Operation execution time.

Operation	Device side	Gateway side
T_h	2.7324 µs	0.1315 µs
T_{PUF}	6.7 µs	/
T_{Che}	91.2600 µs	10.6604 µs
T_{Mul}	426.4887 µs	103.8660 µs
T_{Add}	64.0929 µs	16.4640 µs
T_{Enc}	32.6680 µs	2.0434 µs
T_{Dec}	31.3809 µs	2.0133 µs
T_{bh}	140.195 µs	33.5120 µs
$T_{FE.Gen}$	278.0889 µs	74.7562 µs
$T_{FE.Rep}$	696.1048 µs	157.4092 µs

Where, T_h, T_{PUF}, T_{Che}, T_{Mul}, T_{Add}, T_{Enc}, T_{Dec}, T_{bh}, $T_{FE.Gen}$, $T_{FE.Rep}$ is the time to perform a hash function, the time to perform a PUF, the time to perform a Chebyshev polynomial, the time to perform an elliptic curve dot multiplication, the time to perform an elliptic curve dot addition, the time to perform an AES-256 encryption algorithm, time to perform an AES-256 decryption algorithm, time to perform

TABLE 6. Computational cost.

Scheme	Device side	Gateway side	Total time
Bai *et al.*[10]	$5T_h+T_{FE.Gen}+T_{FE.Rep}+5T_{Mul}+2T_{PUF}\approx 3133.9492$ µs	$4T_h+4T_{Mul}\approx 415.99$ µs	3549.8392 µs
Tanveer *et al.*[11]	$6T_{bh}+3T_{Enc}+2T_{Mul}+T_{PUF}\approx 1798.8514$ µs	$6T_{bh}+3T_{Enc}+T_{Mul}\approx 311.0682$ µs	2109.9196 µs
Hu *et al.*[31]	$5T_h+6T_{Mul}+2T_{Add}\approx 2700.78$ µs	$5T_h+2T_{Mul}+6T_{Add}\approx 656.7815$ µs	3357.5615 µs
Qi *et al.*[32]	$6T_h+T_{Dec}+2T_{Che}+T_{PUF}\approx 303.6184$ µs	$10T_h+T_{FE.Rep}+T_{Dec}+T_{Che}\approx 171.3979$ µs	475.0163 µs
Soni *et al.*[33]	$11T_h+T_{FE.Rep}+6T_{Mul}\approx 3285.2434$ µs	$6T_h+6T_{Mul}\approx 623.985$ µs	3909.2284 µs
Proposed scheme	$7T_h+3T_{Che}+2T_{PUF}\approx 306.3068$ µs	$6T_h+2T_{Che}\approx 22.1098$ µs	328.4166 µs

a modulo power operation, time to perform a fuzzy extractor generation, time to perform a fuzzy extractor recovery.

Table 6 presents a comparison of computational costs between various schemes in the literature and the scheme proposed in this article. From the table, it can be observed that literatures [10] and [33] utilize resource-intensive fuzzy extractor functions in their schemes, resulting in the largest computational costs of 3549.8392 μs and 3909.2284 μs, respectively. Literatures [11] and [31] involve a significant number of elliptic curve point multiplication operations, leading to higher computational costs compared to literature [32] and the scheme proposed in this paper. Literature [32], although avoiding elliptic curve dot multiplication operations, still incurs substantial computational costs on the gateway side due to the use of fuzzy extractor function operations. Consequently, its total computational cost exceeds that of the solution proposed in this article. The proposed scheme in this article, on the other hand, relies solely on hash functions, lightweight security primitives such as PUF, and the Chebyshev chaos map, resulting in a total computational cost of 328.4166 μs. Compared to the schemes proposed in other literature, the proposed scheme in this article achieves significant reductions in computational costs, with reductions of 84.435%, 90.219%, 30.862%, 91.6%, and 90.748%, respectively. Therefore, the proposed scheme is resource-efficient and suitable for power IoT terminal devices with constrained resources.

C. COMMUNICATION COST

Before comparing communication costs, it is assumed that the lengths of various data elements are fixed: the pseudo-identity is 128 bits long, the identity mark is 64 bits, the CRPs are 128 bits, the nonce for random numbers is 64 bits, the output of symmetric encryption/decryption is 128 bits, the output of the Hash function is 128 bits, the output of elliptic curve dot multiplication is 256 bits, the output of the Chebyshev chaotic map is 128 bits, the output of timestamps is 32 bits, the input-output data length for fuzzy extractors is 128 bits, and the output length of modulo power operations is 128 bits.

A comparison of communication costs between the proposed scheme and schemes from the literature is presented in Table 7. The communication cost of the proposed scheme in this paper is 1216 bits, slightly higher than the literature [11] but lower than other schemes. However, literature [11] incurs a computational cost as high as 2109.9196 μs, making it vulnerable to physical attacks and machine learning modeling attacks, rendering it unsuitable for resource-constrained power IoT devices. In contrast, the proposed scheme reduces both computational and communication costs while maintaining high security, rendering it suitable for resource-constrained terminal devices to establish anonymous authentication and negotiate session keys with gateways.

TABLE 7. Comparison of communication cost.

Scheme	Number of messages	Communication cost
Bai *et al.*[10]	3	1472bit
Tanveer *et al.*[11]	2	1088bit
Hu *et al.*[31]	4	1856bit
Qi *et al.*[32]	4	1824bit
Soni *et al.*[33]	2	2304bit
Proposed scheme	3	1216bit

VI. CONCLUSION

A lightweight authentication scheme based on PUF and Chebyshev chaotic map is proposed in this paper, which can achieve two-way authentication and session key negotiation between devices and gateways. The security of the shared secret is verified by the ProVerif tool and improved BAN logic, and a informal security analysis of the scheme proposed in this paper is conducted, which shows that the scheme is effective against a variety of attacks such as physical, machine-learning modelling, and impersonation. Comparing the proposed scheme with existing related authentication schemes, the results show that it satisfies 12 security features such as two-way authentication and user anonymity, with a computational cost of only 328.4166 μs and a communication cost of 1216 bits. Comparative analysis with existing authentication schemes shows that the proposed scheme in this paper has obvious advantages in two-way authentication, user anonymity and other key security features, and also has low computation and communication overheads, which effectively reduces the consumption of resources and is more suitable for deployment in resource-constrained

power IoT environments. Future research can further explore the deployment and application of the proposed scheme in real-power IoT environments to verify its effectiveness and scalability in practice.

REFERENCES

[1] J. Xuan, L. Li, L. Zhang, and Y. Fang, "Lightweight network security protection strategy for power IoT in micro-grid," in *Proc. Int. Conf. Power Ectr. Eng. Ectr. Contr. (PEEEC)*, Sep. 2023, pp. 901–905, doi: 10.1109/PEEEC60561.2023.00176.

[2] B. Zahednejad and C.-Z. Gao, "A secure and efficient AKE scheme for IoT devices using PUF and cancellable biometrics," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100937, doi: 10.1016/j.iot.2023.100937.

[3] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.

[4] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019, doi: 10.1109/JIOT.2018.2846299.

[5] Z. Siddiqui, J. Gao, and M. Khurram Khan, "An improved lightweight PUF–PKI digital certificate authentication scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19744–19756, Oct. 2022, doi: 10.1109/JIOT.2022.3168726.

[6] B. Kim, S. Yoon, Y. Kang, and D. Choi, "PUF based IoT device authentication scheme," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2019, pp. 1460–1462, doi: 10.1109/ICTC46691.2019.8939751.

[7] Y. Nozaki and M. Yoshikawa, "Secret sharing schemes based secure authentication for physical unclonable function," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Feb. 2019, pp. 445–449, doi: 10.1109/CCOMS.2019.8821698.

[8] Z. Y. Wang, Y. Guo, S. Q. Li, S. Hou, and D. Deng, "Design of an efficient anonymous authentication scheme for lightweight IoT devices," *J. Commun.*, vol. 43, no. 7, pp. 49–61, Jun. 2022, doi: 10.11959/j.issn.1000-436x.2022125.

[9] S. Wang, X. Zhou, K. Wen, and B. Weng, "Tripartite authenticated key exchange protocol for smart grid," *J. Commun.*, vol. 44, no. 2, pp. 210–218, Feb. 2023, doi: 10.11959/j.issn.1000-436x.20230369.

[10] H. D. Bai and X. Y. Jia, "A smart grid device authentication scheme based on physically unclonable functions," *J. South-Cent. Univ. Natl., Nat. Sci. Ed.*, vol. 42, no. 3, pp. 382–386, Mar. 2023, doi: 10.20056/j.cnki.ZNMDZK.20230313.

[11] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "ARAP-SG: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143366–143377, 2021, doi: 10.1109/ACCESS.2021.3121291.

[12] 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 Syst. J.*, vol. 17, no. 4, pp. 6425–6436, Dec. 2023, doi: 10.1109/JSYST.2023.3289492.

[13] H. Wang, D. Guo, Q. Wen, and H. Zhang, "Chaotic map-based authentication protocol for multiple servers architecture," *IEEE Access*, vol. 7, pp. 161340–161349, 2019, doi: 10.1109/ACCESS.2019.2948851.

[14] T.-F. Lee, "Provably secure anonymous single-sign-on authentication mechanisms using extended Chebyshev chaotic maps for distributed computer networks," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1499–1505, Jun. 2018, doi: 10.1109/JSYST.2015.2471095.

[15] L. Zhang, Y. Zhu, W. Ren, Y. Wang, K. R. Choo, and N. N. Xiong, "An energy-efficient authentication scheme based on Chebyshev chaotic map for smart grid environments," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 17120–17130, Dec. 2021, doi: 10.1109/JIOT.2021.3078175.

[16] C. Wang, X. Li, M. Ma, and Y. Zhang, "A novel and efficient anonymous authentication scheme based on extended Chebyshev chaotic maps for smart grid," in *Proc. IEEE 23rd Int. Symp. a World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2022, pp. 288–293, doi: 10.1109/WoWMoM54355.2022.00055.

[17] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the Internet of Things," in *Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Oct. 2016, pp. 1–4, doi: 10.1109/MWSCAS.2016.7870046.

[18] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013, doi: 10.1109/TIFS.2013.2279798.

[19] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 1004–1015, doi: 10.1145/2810103.2813679.

[20] A. Yadav, S. Kumar, and J. Singh, "A review of physical unclonable functions (PUFs) and its applications in IoT environment," *Ambient. Commun. Comput. Syst.*, vol. 356, pp. 1–13, May 2022, doi: 10.1007/978-981-16-7952-0_1.

[21] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[22] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, Aug. 2008, doi: 10.1016/j.chaos.2006.09.047.

[23] C. Sheng, Y. Yao, Q. Fu, and W. Yang, "A cyber-physical model for SCADA system and its intrusion detection," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107677, doi: 10.1016/j.comnet.2020.107677.

[24] J. Tao, M. Umair, M. Ali, and J. Zhou, "The impact of Internet of Things supported by emerging 5G in power systems: A review," *CSEE J. Power Energy Syst.*, vol. 6, no. 2, pp. 344–352, Jun. 2020, doi: 10.17775/CSEEJPES.2019.01850.

[25] A. N. Pramudhita, R. A. Asmara, I. Siradjuddin, and E. Rohadi, "Internet of Things integration in smart grid," in *Proc. Int. Conf. Appl. Sci. Technol. (iCAST)*, Oct. 2018, pp. 718–722, doi: 10.1109/iCAST1.2018.8751518.

[26] R. J. Tom and S. Sankaranarayanan, "IoT based SCADA integrated with Fog for power distribution automation," in *Proc. 12th Iber. Conf. Inf. Syst. Technol. (CISTI)*, Jul. 2017, pp. 1–4, doi: 10.23919/CISTI.2017.7975732.

[27] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983, doi: 10.1109/TIT.1983.1056650.

[28] Z. Chen, Z. Cheng, W. Luo, J. Ao, Y. Liu, K. Sheng, and L. Chen, "FSMFA: Efficient firmware-secure multi-factor authentication protocol for IoT devices," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100685, doi: 10.1016/j.iot.2023.100685.

[29] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990, doi: 10.1145/77648.77649.

[30] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *Proc. Comput. Secur. Found. Workshop*, Jun. 1993, pp. 147–158, doi: 10.1109/CSFW.1993.246631.

[31] S. Hu, Y. Chen, Y. Zheng, B. Xing, Y. Li, L. Zhang, and L. Chen, "Provably secure ECC-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5985–5994, Apr. 2023, doi: 10.1109/TII.2022.3191319.

[32] R. Qi, S. Ji, J. Shen, P. Vijayakumar, and N. Kumar, "Security preservation in industrial medical CPS using Chebyshev map: An AI approach," *Future Gener. Comput. Syst.*, vol. 122, pp. 52–62, Sep. 2021, doi: 10.1016/j.future.2021.03.008.

[33] P. Soni, J. Pradhan, A. K. Pal, and S. H. Islam, "Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 830–840, Jan. 2023, doi: 10.1109/TII.2022.3179429.

XIANJI JIN received the B.S., M.S., and Ph.D. degrees in electrical engineering from Harbin Institute of Technology, Harbin, China, in 2005, 2007, and 2013, respectively. His research interests include the industrial Internet/Internet of Things technology and its applications, artificial intelligence, smart grid monitoring, and communication technology.

NA LIN was born in Inner Mongolia, China, in 1999. She received the B.S. degree from Northeast Electric Power University, China, in 2021. She is currently pursuing the M.S. degree with Harbin Institute of Technology, China. Her research interests include novel power system communications, information security, and industrial internet security.

ZHONGWEI LI received the B.S. and M.S. degrees in electrical engineering from Northeast Normal University, Changchun, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical engineering from Harbin Institute of Technology, Harbin, China, in 2006. His research interests include industrial internet security, smart grid communications, and its information security.

WENQI JIANG received the B.S. and M.S. degrees in electrical engineering from Harbin Institute of Technology, Harbin, China, in 2019 and 2021, respectively, where he is currently pursuing the Ph.D. degree in electrical engineering with the Department of Electrical Engineering. His research interests include industrial robot security, industrial control system security, and risk assessment.

YUGE JIA was born in Henan, China, in 2000. She received the B.S. degree from Harbin Institute of Technology, China, in 2022, where she is currently pursuing the M.S. degree. Her research interests include new power system communications, information security, and industrial internet security.

QINGYANG LI received the B.Sc. degree in astronautics from Harbin Institute of Technology, Harbin, China, in 2017, the M.Sc. degree from Lehigh University, Bethlehem, PA, USA, in 2019, and the Ph.D. degree from the Department of Electronics, Carleton University, Ottawa, Canada, in 2024. Her research interests include machine learning and reinforcement learning-based wide-area control systems for large-scale power system stability and security.