Lightweight and Anonymous Group Authentication Scheme Based on PUF in the Smart Grid

Yang Zhou[1], Bing Yang[1], Dengzhi Liu[2]*

[1] School of Computer Science, Nanjing University of Information Science & Technology, China
[2] School of Computer Engineering, Jiangsu Ocean University, China
zy747501734@163.com, yangbing6882@163.com, liudz@jou.edu.cn

Abstract

As a new generation of electricity system, smart grid significantly improves electricity services' efficiency, reliability, and sustainability. The smart meters, which are the essential terminals, help establish two-way communication between users and electricity providers. While enjoying the convenience of smart meters, users face many challenges. On the one hand, malicious adversaries could attack the smart meters and thus steal the users' privacy. On the other hand, the computational overhead of electricity data verification is high for lightweight smart meters. To address above issues, a lightweight authentication and group key management scheme is proposed. In the proposed scheme, the physical properties of the Physical Unclonable Function (PUF) are exploited to defend against external attacks from adversaries. Moreover, the Chinese Remainder Theorem (CRT) is used to broadcast the updated group keys for the legitimate smart meters in the community. In addition, the aggregated signature is utilized to reduce the overhead of the data verification. Finally, the Random Oracle Model (ROM) is used to demonstrate that the proposed scheme meets many security requirements. Performance analysis shows that the proposed scheme is more suitable for smart grid compared to previous schemes.

Keywords: Smart grid, Authentication, Chinese Remainder Theorem (CRT), Physical Unclonable Function (PUF), Aggregated signature

1 Introduction

The smart power grid is a new type of power grid developed on the basis of the physical power grid [1], which not only improves energy utilization efficiency but also takes into account environmental protection.

Compared to traditional grids, it integrates advanced modern technology, such as sensing and measurement technology, communication technology, information technology, computer technology, and control technology. The smart grid provides users with an economical, clean, and interactive electricity supply and establishes two-way communication between users and electricity providers. As the terminal equipment of the smart grid, the smart meters undertake some essential tasks–helping to collect, measure and transmit electricity data in real time and uploading the accumulated electricity consumption information to the control center. Based on these data, the control center can analyze electricity conditions to increase energy consumption efficiency and optimize the services provided by the smart grid (generation, transmission, distribution, and electricity utilization).

In the process of constantly enhancing the smart grid construction, a large number of various smart terminals are installed in various parts of the smart grid system. The structure of the power system is more complex. Although it has improved the intelligence of the system to some extent, it makes the system derive a huge amount of power information data. Since this type of data often contains critical privacy and strategic corporate information, we need to ensure that it would not be leaked during the transmission, collection and storage stages. Due to the large-scale application of cloud IoT technologies, the security risks faced by power systems have increased significantly. Therefore, it is important to carry out research on the data protection of the smart grid.

In the future, we can consider applying blockchain [2-4] to the smart grid. Given the decentralized and distributed nature of blockchain, the power management system can improve data traceability. The use of blockchain can help to weaken the influence of the central node on data interaction and data storage performance, thus improving the security and scalability of the smart grid data management platform and making the platform more compatible with the social demand for electricity.

Smart meters bring much convenience to users and the control center, but frequent data interactions [5] also bring additional challenges to smart meters. Firstly, smart meters are lightweight terminal equipment [6]. Without hardware protection [7], an adversary may physically attack the smart meters to modify the electricity data or obtain the smart meters' private keys through a side-channel attack [8], thereby disguising it as a legitimate meter. Secondly, if the adversary can steal fine-grained data from smart meters, it could become a potential threat to the users' privacy. For example, it could try to guess when a user is at home/not at home by their electricity habits, and so on. Moreover, due to the large number of smart meters in the community, multiple data integrity verifications [9-10] are required, which results in high computational overhead. In this work, we first consider

*Corresponding Author: Dengzhi Liu; E-mail: liudz@jou.edu.cn
DOI: 10.53106/160792642023092405004

some private data stored in smart meters. It increases the risk of keys and electricity data leakage. Therefore, we equip each smart meter with the PUF to resist physical attacks to protect users' privacy. We find that some signature schemes [19-21, 23] have been proposed to address the security and privacy issues present in the smart grid, but there still exist some unsolvable problems. For example, a malicious meter can successfully forge a new signature to pass authentication, or different meters can launch coordinated attacks. Since smart meters have limited computing ability, we have better use CRT to help legitimate smart meters execute dynamical operations with less computational overhead. In addition, we find that the dynamic operations of smart meters also increase computational complexity and affect communication performance. Therefore, we take advantage of the aggregated signature to reduce the computation overhead during the verification phase by changing the verification operation from multiple times to once.

1.1 Contributions

•First of all, in our scheme, users can conduct one-to-one authentication with the smart meter through their mobile phone when they move in. And the smart meter does not need to store any private key for authentication, so it can resist the adversary's internal attacks to obtain the private key stored in non-volatile storage.

•Secondly, a provably secure aggregated signature scheme is used to sign the electricity data of the smart meters, and the calculation overhead of the control center is reduced during the verification process.

•Thirdly, the proposed group key management scheme uses the Chinese Remainder Theorem to reduce the computational complexity of the smart meters when joining or leaving the group.

•Finally, our scheme meets the proposed security requirements and is highly efficient, so it can be well applied to the smart grid environment.

1.2 Related Work

In recent years, many authentication schemes have been proposed for the smart grid. Tsai et al. [11] proposed an identity-based signature and encryption scheme to realize anonymous mutual authentication between smart meters and service providers, which reduced the computing overhead of smart meters. Odelu et al. [12] pointed out that Tsai et al. [11] can neither guarantee the security of the session key nor resist the impersonation attack of a malicious smart meter under the Canetti-Krawczyk adversary (CK-adversary) model [13]. Therefore, in order to solve the above problems, Odelu et al. [12] proposed an authentication key distribution scheme based on the elliptic curve ElGamal-type digital signature technology and IBE (identity-based encryption) technology, which realized several security functions. As we all know, the Elliptic Curve Cryptography (ECC) schemes have a smaller key size and computational overhead, so many authentication schemes based on elliptic curves have emerged as the times require [14-18]. However, none of the above proposals consider the possibility of the adversaries' physical attack on the smart meter during the communication process, which may reveal some session keys and private data stored in the device. This paper uses PUF, a hardware facility built into a smart meter that does not need to store any long-term authentication keys to resist physical attacks. At the same time, users' private data should also be protected from eavesdropping attacks or other attacks. Usually, the data can be signed and then sent to the service provider to verify the validity of the data. Many studies show that the aggregate signature technology can be used to implement the batch verification of signatures and thus reduce the verification overhead. Gentry et al. [19] proposed an identity-based aggregate signature scheme, which significantly reduced the total computation cost of signature verification. Boldyreva et al. [20] pointed out that if the adversary could find the repeated random number in the two signatures in Gentry et al. [19], he could carry out adaptive selection information attacks to forge a legitimate signature. To resist this attack, Boldyreva et al. [20] introduced an ordered multi-signature, including the order of the signature, which improved the scalability of the scheme. Still, the scheme lacked some random oracle inquiries. Lu et al. [21] aggregated the signatures of multiple nodes and sent them to the base station. All information can be authenticated by verifying the aggregated signatures, and it is probably safe under the random oracle model. At the same time, Guan et al. [23] realized data aggregation based on secret sharing technology to support batch verification of power data. Therefore, to improve the efficiency of signing and verification. This paper uses an identity-based aggregate signature technology to achieve the integrity and non-repudiation of power data and prevent the disclosure of user privacy. In addition, we discuss some methods of management of group keys [22]. Li et al. [24] proposed a scheme based on homomorphic encryption technology to achieve privacy protection, which supports forward security but also increases a lot of computational overhead. Lim et al. [25] proposed a group key distribution scheme based on group signature authentication, which has scalability but cannot meet the forward security and the backward security. Therefore, to meet the requirement of the forward security and the backward security, Mansour et al. [26] added the operation that the group needs to broadcast the key after a group member joined or left the group in the scheme, which only brought a small amount of overhead to TA. Funderburg et al. [27] pointed out that Mansour et al. [26] might be attacked by malicious group members by encrypting inter-group communication information using only one symmetric key, so Funderburg et al. [27] proposed a layered key management system to track malicious group member. However, the proposed schemes have a relatively large computational overhead for key management. Therefore, our solution uses the Chinese Remainder Theorem. Thus, the updated group key can be calculated with only one modular operation, reducing the computational overhead.

1.3 Organization

Section 2 introduces the preliminaries, mathematical backgrounds, system model, security model, and threat model. Then our concrete scheme is proposed in Section 3. In section 4, the security analysis is shown in detail. The

performance comparison with several other schemes is in section 5. Finally, Section 6 summarizes our proposed scheme.

2 Preliminaries and Background

This section mainly introduces some relevant background knowledge of cryptography, including the Elliptic Curve computational Diffie-Hellman (ECCDH) Problem, Physical Unclonable Function (PUF), aggregated signature, and the Chinese Remainder Theorem. The system model and security model of our solution and the security goals that need to be achieved are also shown in this section.

2.1 Elliptic Curve Computational Diffie-Hellman

Elliptic curve cryptography (ECC) is an effective method for implementing public key cryptography. An elliptic curve can be defined as follows: An elliptic curve (E) over a finite field (F_q) denoted as $E(F_q)$ has q elements. The equation of the elliptic curve over a prime field p is defined as $y^2 \equiv x^3 + ax + b$ ($mod\ p$). Let G be a cyclic group on an elliptic curve, given that P, aP, $bP \in G$, it is hard to compute $abP \in G$. Since there is no polynomial-time algorithm for solving this problem, we can take advantage of this hard problem to design secure protocols.

2.2 Physical Unclonable Functions

Since the concept of PUF was formally proposed by Pappu in [28], it has been widely used for the secure storage of keys in cryptography. Currently, PUF is usually implemented with integrated circuits, and the circuit generates a unique output value that can remain constant under any external conditions. Also, any attempt to detect or observe the operation of the PUF will change the characteristics of the underlying circuit and make the PUF fail.

PUF is a physical challenge-response pair (CRP), not a purely abstract mathematical concept. The input of PUF is generally called a challenge, and $c \in C$ usually represents the challenge; the output is traditionally called response and is characterized by $r \in R$. So, we can get such an equation $R = PUF(C)$.

The basic application of PUF is mainly to help realize the authentication process. It is inevitable that some wrong authentication will be encountered. Therefore, people often use the concepts of inter hamming distance and intra hamming distance to describe this problem. For a PUF, the intra-distance and the inter-distance are defined as follows:

Intra-distance. Because the uniqueness and unclonability of PUF will cause two different PUF entities to produce two completely different responses, the inter-distance refers to the two separate PUF entities generated after a specific stimulus is an input. The distance between responses.

Inter-distance. Commonly, the response of PUF is inevitably affected by some external factors. Therefore, inter-distance refers to a single PUF after a specific stimulus is repeatedly input twice—the distance between the responses it produces. Therefore, users hope that the intra-distance of the PUF entity is small enough and the inter-distance should be close to 1/2.

2.3 Aggregated Signature

A signature aggregation scheme [29] is composed of multiple signers, a signature aggregator, and a signature verifier, and the scheme mainly consists of five algorithms. The specific process is as follows:

Setup: Input security parameter k and output system public parameters *params*.

Key-Extract: Input $x_i \in \mathbb{Z}_q^*$, calculate the public $y_i = x_i \cdot P$, and generate the user key pair (x_i, y_i).

Sign: Input the system parameter *params*, wait for the electricity data message m_i, and output a single signature σ_i for the message m_i.

Aggregate-Sign: Input n valid message signature pairs $(m_i, \sigma_i)(1 \le i \le n)$, and the aggregator outputs Aggregate signatures for these n valid signatures σ.

Aggregate-verify: Input *params*, n messages m_i, and the aggregate signature σ. Output 1 if the aggregate signature is accepted, and output 0 if the aggregate signature is invalid.

2.4 Chinese Remainder Theorem

Sun Tzu's theorem is an ancient Chinese method for solving linear congruence expression series, playing a pivotal role in number theory.

$$(S): \begin{cases} x = a_1 (\mathrm{mod}\, m_1) \\ x = a_2 (\mathrm{mod}\, m_2) \\ \vdots \\ x = a_n (\mathrm{mod}\, m_n) \end{cases}. \tag{1}$$

Suppose that integers $m_1, m_2, ..., m_n$ are mutually prime in pairs, then for any integer: $a_1, a_2, ..., a_n$, the equation set (S) has a solution, and the general solution can be constructed in the following manner: Compute $M = m_1 \times m_2 \times ... \times m_n = \prod_{i=1}^{n} m_i$, let M be the product of integers $m_1, m_2, ..., m_n$, and $M_i = \frac{M}{m_i}$, $\forall\ i \in \{1, 2, ..., n\}$ be the product of $n - 1$ integers other than m.

Set $t_i = M_i^{-1}$ as the number theoretic inverse (inverse element) of the module, $M_i t_i \equiv 1 (mod m_i)$, $\forall\ i \in \{1, 2, ..., n\}$.

Therefore, the general solution of the system (S) is of the form

$$\begin{aligned} x &= a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots a_n t_n M_n + kM \\ &= kM + \sum_{i=1}^{n} a_i t_i M_i, k \in \mathbb{Z}. \end{aligned} \tag{2}$$

Finally, after the general solution is modulo M, the system (S) has only one solution: $x = (\sum_{i=1}^{n} a_i t_i M_i) \bmod M$.

3 The Overview of System and Security

3.1 System Model

The whole system model mainly includes the user's mobile Device (D), Smart Meter (SM), Local Aggregator (LA), and Control Center (CC), as shown in Figure 1.

Device: The smart phone is a device for legal authentication between the user and the smart meter. The primary function is to distribute a piece of complete identity information for the smart meter and to ensure the legitimacy of the connected meter.

Smart Meter: Smart meter is a terminal device for the smart grid, measuring information about the user's electricity consumption. There are n smart meters in the entire power grid area. After receiving the authentication request from the user, it can use its physical characteristics to conduct secure one-to-one authentication with the user. After receiving the response request from the control center, it can encrypt the data and send it to the control center.

Local Aggregator: The local aggregator is a bridge connecting the smart meter and the control center. It can verify the validity of the signature of the electricity data from each smart meter and aggregate these signatures into an aggregated signature and then send it to the control center.

Control Center: In our proposed system model, CC is a secure and reliable entity. In the communication process, CC needs to generate corresponding system parameters and is responsible for the online registration of meters and users and local collection. After receiving the aggregated signature of the users' electricity data from the local aggregator, it can verify whether the smart meters in the entire group are legal.

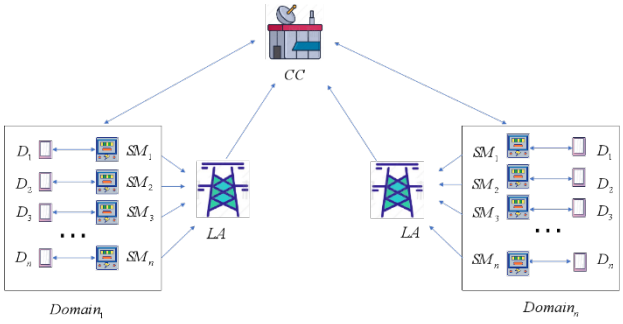


Figure 1. System model

3.2 Security Model

The challenger C runs the setup algorithm $Setup(1^k)$, generates system parameters $params$, and sends the parameters to the adversary. The adversary executes the following queries.

Hash query: Due to the one-way nature of the hash function, at any time C gets the input of a variable-length number, C will return a fixed-length value to A.

Key-Extract query: According to the identity ID_{SM_i}, C runs the Key-Extract algorithm, calculates the corresponding private key sk_i, and returns it to A.

Sign query: For an arbitrary tuple (m_i / ID_{SM_i}), the challenger C performs the sign algorithm to generate the corresponding signature σ_i, and send it to the adversary A.

Then A forges a signature, which is the aggregated signature σ generated by n smart meters $SM = \{SM_1, SM_2, ..., SM_n\}$ for n different information m_i. If the following situations occur, we would say that the adversary A wins: The adversary outputs a valid aggregate signature σ^* for message $m = \{m_1, m_2, ..., m_n\}$ and the adversary does not execute the Sign query for all ID_{SM_i}.

3.3 Threat Model

In the solution proposed in this paper, the adversaries faced can be divided into internal adversaries and external adversaries. The inner enemies are entities directly involved in communication, including user equipment and smart meter terminals, and the external adversaries are entities that are not directly involved in the communication process. As described in the Dolev-Yao threat model [30], both internal and external adversaries can eavesdrop, tamper [31], replay, forge, delete or even inject some inaccurate data into the information. In this paper, we assume that D_i and SM_i are untrusted participants, while LA and CC are wholly trusted.

4 Construction

Table 1. Notations

Notations	Definitions
CC	Control center
D_i, SM_i	i^{th} device and smart meter
ID_{SM_i}	Real identities of smart meter
N_1, N_2, N_3	Random number, whose size is 64 bits
ΔT	Validity period of message
λ	The master secret key of CC
P_{pub}	The public key of CC
k_d	Smart meter group key
T_1, T_2, T_3	Timestamp in authentication phase
t_i	Valid period of electricity data
H_1, H_2, H_3, H_4	Four secure hash functions

In this section, we describe the solutions proposed for the smart grid. Our scheme mainly includes the following phases: 1) the registration phase of the user's mobile phone and the smart meter in the home, 2) the one-to-one authentication phase between the user and the smart meter, 3) the signature and verification phase of electricity data, 4) the group key calculation, and 5) the group key update phase. Table 1 lists the main notations and their related definitions used in this paper.

4.1 Smart Meter Registration Phase

In the secure registration phase, each smart meter can obtain its own identity ID_{SM_i} from the user through the secure channel.

1) When the user moves into the community, they need to use their mobile phone D_i to apply to CC for a legal identity ID_{SM_i} of the smart meter SM_i at home, and to generate a random number C_i, and compute $AU_0 = (ID_{SM_i}, C_i)$, which will be transmitted to SM_i through the secure channel.

2) After receiving AU_0, SM_i stores the ID_{SM_i} in its own

memory, and then uses the internal physical structure PUF to calculate $R_i = PUF(C_i)$ to obtain $ID_{SM_i} \rightarrow CRP[(C_i, R_i)]$, $CRP[(C_i, R_i)]$ will be sent to the user's mobile phone D_i through a secure channel, and then deleted from the memory of the SM_i, only ID_{SM_i} saved.

4.2 User-Smart Meter Authentication Phase

Figure 2 shows the one-to-one authentication process between the user and the smart meter.

1) The smart meter SM_i generates a 64-bit random number N_1, sends its own identity ID_{SM_i} and N_1 to D_i, then D_i checks whether there is a mapping $ID_{SM_i} \rightarrow CRP[(C_i, R_i)]$ in the local database. If it does not exist, we need to resend a new one ID_{SM_i}, otherwise, the authentication phase continues.

2) D_i chooses a 64-bit random number N_2, and generates a current timestamp T_1 at that time, encrypts it with R_i to get $AU_1 = Enc_{R_i}\{N_2 \,||\, H_1\,(N_1 \,||\, R_i \,||\, N_2)\}$, and send T_1, C_i, AU_1 to SM_i.

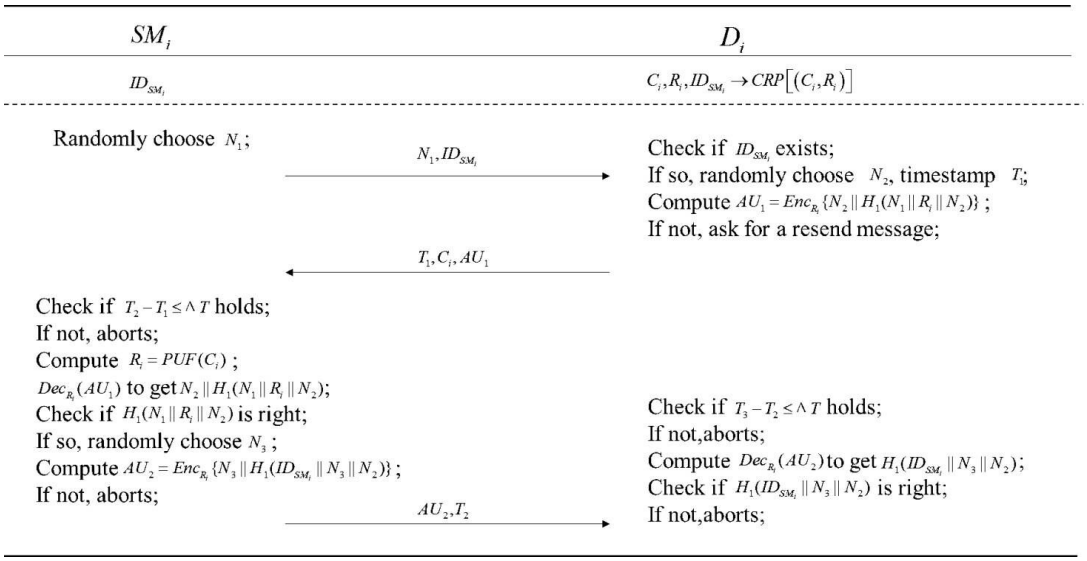


Figure 2. $U_i - SM_i$ authentication

3) After receiving the above information, SM_i selects a new timestamp T_2, firstly check if $T_2 - T_1 \le \Delta T$ (an allowable maximum transmission delay) holds. Then use PUF to calculate $R_i = PUF(C_i)$, and then use the R_i decrypt AU_1 to get $N_2 \,||\, H_1\,(N_1 \,||\, R_i \,||\, N_2)$. Since N_2 is a 64-bit random number, we divide the decrypted information into two parts, the first 64 bits and the remaining part, so we can use the parameters that have been obtained to verify whether $H_1\,(N_1 \,||\, R_i \,||\, N_2)$ is equal to the decrypted one. If they are equal, the authentication process continues. Choose a 64-bit random number N_3, and then encrypt with the R_i to get the ciphertext $AU_2 = Enc_{R_i}\{N_3 \,||\, H_1\,(ID_{SM_i} \,||\, N_3 \,||\, N_2)\}$, and then send AU_2 and T_2 to D_i; otherwise, end the authentication phase.

4) After receiving this information, D_i firstly generates a new timestamp T_3, checks if $T_3 - T_2 \le \Delta T$ (an allowable propagation delay) holds, then perform a decryption operation $Dec_{R_i}(AU_2)$, take the first 64 bits to get N_3, and then use the parameters that have been obtained to verify whether $H_1\,(ID_{SM_i} || N_3 || N_2)$ is equal to the decrypted one. If it is not equal, the authentication fails. Otherwise, the authentication is passed, and the mutual authentication process between each user's mobile phone U_i and the corresponding household smart meter SM_i is also completed.

4.3 Group Key Calculation Phase

During the group key calculation phase, each legal smart meter will obtain the group key.

1) CC selects random numbers $rn_i \in \mathbb{Z}^*_q$ for n smart meters during the offline registration phase.

2) CC undergoes the calculation operations of $\beta = \prod_{i=1}^{n} rn_i$, $a_i = \dfrac{\beta}{rn_i}$.

3) Then chooses b_i to satisfy $a_i \times b_i \equiv 1 \bmod rn_i$.

4) CC calculates all the multiplied values of a_i and b_i, $val_i = a_i \times b_i$, and calculates $\tau = \sum_{i=1}^{n} val_i$.

5) CC chooses a random number $k_d \in \mathbb{Z}^*_q$ as the group key and calculates $\delta_d = k_d \times \tau$.

6) CC signs δ_d to get $SIG_{sk_{cc}}(\delta_d)$ with its own private key sk_{cc}, and calculate $K_{pub} = k_d \cdot P$ and broadcasts the above information to each smart meter in the group.

7) After the smart meter obtains δ_d from the CC, any legal SM_i that has passed the authentication can obtain the group key k_d through a modular operation $\delta_d \bmod rn_i = k_d$.

4.4 Electricity Data Signature and Verification Phase

After the smart meter collects electricity data for a certain period of time, it needs to generate its own signature information for the data and then send these signatures to the local aggregator. After verifying the validity of each signature, an aggregate signature will be generated and sent to the control center. The entire signing and verification process is as follows:

Setup: Given a secure parameter k, CC selects two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with prime order $q > 2^k$ of elliptic curve over a finite field. Then choose a generator g of $\mathbb{G}_1$, three secure hash functions H_2, H_3, $H_4(H_2, H_4:\{0, 1\}^* \rightarrow \mathbb{G}_1, H_3: \{0, 1\}^* \rightarrow \mathbb{Z}^*_q)$, and a random number $\lambda \in \mathbb{Z}^*_q$ as the system secret key, and CC calculates $P_{pub} = \lambda g$ and announces the system parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, g, e, P_{pub}, H_2, H_3, H_4\}$.

Key-Extract: *CC* generates the corresponding public/private key pair for each SM_i, where $pk_i = k_i = H_2(ID_{SM_i})$, $sk_i = \lambda \cdot k_i$.

Sign: SM_i random selects $r_i \in \mathbb{Z}^*_q$, computes $V_i = r_i \cdot g$. Then calculates $h_i = H_3(ID_{SM_i} \| t_i \| m_i)$ and $T = H_4(P_{pub})$, where m_i refers to the electricity consumption data of household users in a certain period of time t_i. After that, SM_i calculates $U_i = h_i \cdot sk_i + r_i \cdot T$. Therefore, $\sigma_i = (V_i, U_i)$ is the signature of the electricity data m_i collected during the time period t_i.

Aggregate-Sign: LA performs the operation $h_i = H_3(ID_{SM_i} \| t_i \| m_i)$, $T = H_4(P_{pub})$ and LA obtains σ_i only if the following n equations are all true: $e(g, U_i) = e(V_i, T) \cdot e((h_i \cdot k_i), P_{pub})$. After verifying that n single signature σ_i are valid, calculates $V = \sum_{i=1}^{n} V_i$ and $U = \sum_{i=1}^{n} U_i$. Then $\sigma = (V, U)$ is the aggregate signature of the power data m_i of n smart meters in the time period t_i.

Aggregate-Verify: Given ID_{SM_i} $(1 \le i \le n)$, t_i, m_i and $\sigma = (V, U)$, CC performs the following operations.

CC first calculates $h_i = H_3(ID_{SM_i} \| t_i \| m_i)$, $(1 \le i \le n)$ and $T = H(P_{pub})$. Then checks whether the following equation holds.

$$e(g,U) = e(V,T) \cdot e(\sum_{i=1}^{n} (h_i \cdot k_i), P_{pub}) . \quad (3)$$

If the above equation holds, the n signatures are all legal, and the resulting aggregate signature σ is legal. Otherwise, at least one of the transmitted signatures is invalid. The control center can use the quick search invalid signature algorithm in [32] to find the invalid signature. The specific operation is not shown in this paper.

4.5 Group Members Join and Leave

When the smart meter joins or leaves the group, the key update operation needs to be performed. When a new smart meter enters the group, CC needs to broadcast the new group key to each legal member to prevent the newly added member from accessing the previous communication. Similarly, when a smart meter leaves the group, the group key must be updated to ensure that the leaving meter cannot access the updated group key.

For example, when a corrupted SM_t $(1 < t < i)$ needs to leave the group, CC needs to perform the following operations.

CC uses the previously saved γ to minus the meter's val_t that left the group to get the new γ' that $\gamma' = \gamma - val_t$. Then, CC needs to choose a new random number k'_d and multiply it with the obtained γ' above to get the updated group key $\delta'_d = k'_d \times \gamma'$. After that, the CC can broadcast the updated group key information, so each legal smart meter in the group only needs to execute a modulo operation to get the new group key k'_d. In addition, since the meters $\{SM_a, SM_b, SM_c\}(a, b, c \le i)$ left the group, val_a, val_b, val_c are not included in the new γ', so the meter that has left cannot correctly calculate the updated group key. In addition, since the val_t of the smart meter $SM_t's$ leaving the group is no longer included in the new γ', it cannot correctly calculate the updated group key.

Adding a smart meter to a group is similar to the above, so we will not describe it in detail. Next, we discuss the situation of two batch operations.

Case 1: Batch leave

Suppose a group of smart meters $\{SM_a, SM_b, SM_c\}\{a, b, c \le i\}$ need to leave the group. After the meters leave the group, the process for CC to update the group key is shown below. CC uses the previously saved γ to minus the removed meters' val_a, val_b, val_c to get $\gamma' = \gamma - val_a - val_b - val_c$. Then, CC needs to choose a new random number k'_d and multiply it with the obtained γ' above to get $\delta'_d = k'_d \times \gamma'$. After that, the CC can broadcast the updated group key information, so each legal smart meter in the group only needs to perform a modulo operation to get the new group key k'_d.

When a new smart meter joins the group, CC needs to broadcast the new group key to each legal member so as to prevent the newly added member from accessing the previous communication.

Case 2: Batch join

Suppose a group of smart meters $\{SM_a, SM_b, SM_c\}(a, b, c \le i)$, need to be added to the group. After the smart meters are added to the group, the process for CC to update the group key is shown below.

1) Use the previously saved γ plus the newly added meters' value val_a, val_b, val_c to get $\gamma' = \gamma + val_a + val_b + val_c$.

2) Then, CC needs to choose a new random number k'_d and multiply it with the obtained γ' above to get $\delta'_d = k'_d \times \gamma'$.

3) After that, the CC can broadcast the updated group key information, so every legal smart meter in the group, including the newly added meter, only needs to execute a modulo operation to get the new group key k'_d. Therefore, we can conclude that no matter whether n smart meter join or leave the group, CC only needs to broadcast an updated δ'_d to all legal meters in the group, which significantly reduces the computational overhead of CC.

5 Correctness and Security Analysis

5.1 Correctness

The correctness of the single signature verification process is given as follows.

$$\begin{aligned} e(g,U_i) &= e(g, h_i \cdot sk_i + r_i \cdot T) \\ &= e(g, h_i \cdot sk_i) \cdot e(g, r_i \cdot T) \\ &= e(r_i \cdot g, T) \cdot e(g, h_i \cdot sk_i) \\ &= e(V_i, T) \cdot e(h_i \cdot k_i, P_{pub}). \end{aligned} \quad (4)$$

The correctness of the batch signatures verification process is shown as follows.

$$\begin{aligned} e(g,U) &= e(g,\sum_{i=1}^{n}(h_i \cdot sk_i) + \sum_{i=1}^{n} r_i \cdot T) \\ &= e(g,\sum_{i=1}^{n}(h_i \cdot sk_i)) \cdot e(g,\sum_{i=1}^{n} r_i \cdot T) \\ &= e(\sum_{i=1}^{n} r_i \cdot g, T) \cdot e(g,\sum_{i=1}^{n}(h_i \cdot sk_i)) \\ &= e(V,T) \cdot e(\sum_{i=1}^{n}(h_i \cdot k_i), P_{pub}). \end{aligned} \quad (5)$$

5.2 Security Proof

Theorem 1: Under the random oracle model (ROM), suppose an adversary can break this scheme within $t' < t + (q_{H_2} + 2q_E + 3q_S + n + 2) \cdot t_{sm}$, where q_{H_i}, q_E, q_S, n, ε represent the number of times the adversary executes the H_i ($i = 2, 3, 4$) query, the private key extract query, and the signature query respectively. Then there is a challenger C that can deal with the ECCDH hardness problem with the advantage $\varepsilon \cdot \mu^{q_E+q_S} \cdot (1-\mu^n)$ within $t' < t + (q_{H_2} + 2q_E + 3q_S + n + 2) \cdot t_{sm}$, where t_{sm} indicates the time taken to calculate a scalar multiplication in the group G_1.

Proof: Suppose the adversary A wants to solve the ECCDH difficult problem instance by constructing a challenger C, that is, given an instance (g, xg, yg) in the group G_1, C can output the solution xyg of the ECCDH problem. C first executes the system initialization algorithm, defines the system public key $P_{pub} = xg$, generates the public parameters $params$: = { k, e, $\mathbb{G}_1$, $\mathbb{G}_2$, g, P_{pub}, H_2, H_3, H_4} then sends them to the adversary. A conducts the following query:

H_2 - query: When A sends an identity information ID_{SM_i} to C, if there exists (ID_{SM_i}, k_i) in the list H_2List, C will return k_i to A; otherwise, C performs the following operations: C chooses $l_i \in \mathbb{Z}^*_q$, flips a coin b to get the value, if $b = 1$, computes $k_i = l_i(yg)$ and sends it to the adversary, then add the record (ID_{SM_i}, k_i) to the list. Define the probability of occurrence of this event as $1 - \mu_1$. If b = 0, C computes $k_i = l_i g$, sends it to A, and adds the record (ID_{SM_i}, k_i) to the list. Define the probability of this event as μ_1.

H_3 - query: A inputs (ID_{SM_i}, m_i), then C queries the list H_3List, if there exists the corresponding record, return it to A. Otherwise, C randomly selects $h_i \in \mathbb{Z}^*_q$, adds the record to the list H_3List and transmits it to A.

H_4 - query: When A queries for the hash value of P_{pub}, C queries the list H_4List, if there exists the corresponding record, returns it to A. Otherwise, lets $T = zg$, adds the record to the list H_4List, and sends T to A.

Private key extract query: When C enters ID_{SM_i}, the private key extract query will be performed, and the value of b in the list will be queried in the list H_2List, then the following operations will be performed: If $b = 0$, C calculates $sk_i = l_i(xg)$, adds (ID_{SM_i}, sk_i) to the list $ExeList$ and delivers sk_i to A. If $b = 1$, C terminates the simulation.

Signature query: When A asks C for the signature of the electricity data m_i and smart meter's identity ID_{SM_i}, C will extract the corresponding hash value from H_3List and H_4List, then performs the following operations: If $b = 0$, C obtains the corresponding record from the list, selects $U_i \in G_1$, and calculates $V_i = \frac{U_i - h_i l_i P_{pub}}{z}$. If $b = 1$, C stops the simulation. After stopping the query, A obtains the single signatures of n users and then calculates a valid aggregate signature. If the query is not terminated, we can get the following equation:

$$\begin{aligned} &e(g,U) = e(V,T)e(\sum_{i=1}^{n} h_i k_i, P_{pub}) \\ &e(g,U) = e(V,zg) \cdot e(\sum_{i=1,i\neq j}^{n} h_i l_i g + h_j l_j yg, xg) \\ &e(g, U - zV - \sum_{i=1,i\neq j}^{n} h_i l_i xg) = e(P, h_j l_j xyg). \end{aligned} \quad (6)$$

Therefore, C can calculate $xyp = \frac{U - zV - \sum_{i=1,i\neq j}^{n} h_i l_i xg}{h_j l_j}$ as a solution to the ECCDH difficult problem, and thus C solves an example of the ECCDH difficult problem. Let's analyze the probability of the challenger's success in this game. Define four independent events E_1, E_2, E_3, E_4.

E_1 : C successfully passes the private key extract query.

E_2 : C successfully passes the signature query.

E_3 : A generates a valid aggregate signature σ for (ID_{SM_i}, m_i).

Table 2. Features comparison

	Ours	[24]	[34]	[22]	[10]
Key management	√	√	-	×	×
Message verification	√	√	√	√	√
Data integrity	√	√	√	√	√
Forward secrecy	√	√	-	×	×
Backward secrecy	√	×	-	×	×
Authentication	√	√	√	√	√
Unlikability	√	×	√	×	×
Physical attacks	√	×	×	×	×
Replay attacks	√	×	√	√	×

E_4 : There is at least one ID_{SM_i} in E_3 that satisfies $b = 1$.

We can get $\Pr[E_1] \geq \mu_1^{q_E}$, $\Pr[E_2] \geq \mu_1^{q_S}$ $\Pr[E_3] \geq \varepsilon$, $\Pr[E_4] \geq (1 - \mu_1^{n})$.

Then we can obtain the following inequality $\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] \geq \varepsilon\mu_1^{q_E+q_S}(1 - \mu_1^{n})$. Obviously, it is a non-negligible probability, so it contradicts the hardness of the ECCDH problem. Therefore, no adversary can forge a legal signature to pass the verification.

5.3 Security Analysis

Here, we analyze the security achieved in our scheme. The security analysis of our scheme includes the following aspects.

1) Data Confidentiality and Data Integrity [35]: Due to the difficulty of the ECCDH problem, if the equation $e(g,U) = e(V,T) \cdot e(\sum_{i=1}^{n}(h_i \cdot k_i), P_{pub})$ about the message m_i and the signature σ holds, then no adversary can forge a legal aggregate signature in polynomial time to pass the verification, so our scheme can satisfy data confidentiality and data integrity.

2) Resistance to existential forgery: For an aggregate signature σ composed of n single signatures, even if the adversary can obtain the signature of $n - 1$ electricity information, it cannot successfully forge the legal aggregate signature. Therefore, our scheme can resist existential forgery attacks.

3) Anonymity/Identity privacy-preserving: During the one-to-one communication between the user and the smart meter, due to the existence of the PUF in the smart meter, even if the adversary performs a cloning attack or a physical attack, the correct ID_{SM_i} cannot be obtained, and in the signature aggregation phase, the information about ID_{SM_i} is transmitted by a hash value, even if the adversary obtains all the information on the insecure channel, he cannot calculate the user's identity information. Therefore, our solution achieves anonymity/identity privacy protection.

4) Forward/Backward secrecy: The smart meter that has been removed cannot decrypt the subsequent broadcast ciphertext with the previous key to calculate the legal group key k_d ; at the same time, the newly added smart meter cannot decrypt the previous broadcast ciphertext with the current key to obtain a valid group key k_d . Therefore, our solution achieves forward/backward security.

5) Resistance to reply attacks: We assume that adversary A can monitor the communication of D_i , SM_i and CC and intercept the information in the communication. But this information contains some randomly selected numbers and a timestamp that marks the freshness of the message. Therefore, our scheme can resist replay attacks [33].

6 Performance Evaluation

In this section, we analyze the performance of the proposed protocol. Firstly, we compare our scheme with [10, 22, 24, 34] and find that our scheme meets many security requirements. Then, we analyze the proposed scheme of computing cost in detail and compare it with other schemes.

6.1 Features Comparison

In this section, we perform the comparison of our scheme with [10, 22, 24, 34] in the field of key management, message verification, data integrity, forward security, backward security, authentication, and unlinkability. As shown in Table 2, [22] and [10] cannot update the group key, therefore cannot guarantee the forward and backward secrecy of the group key. And [24] can only achieve forward secrecy. In addition, in [10, 22, 24], the adversary can get two messages that can be linked to the same smart meter. These schemes [10, 24] cannot resist replay attacks. Finally, only our scheme can resist physical attacks.

6.2 Computation Cost Analysis and Comparison

In this section, we show the computational cost of our scheme and compare it with several other schemes. In addition, the execution time of some cryptographic operations is defined as Table 3. The simulation uses Java Pairing-Based Cryptography Library-2.0.0. Among them, the time required to perform a PUF operation is from the reference [36].

- T_{AG}: Time required to perform the points addition operation $A + B$, where $A, B \in G$.
- T_{MG}: Time required to perform the scale multiplication operation $x \cdot C$, where $C \in G, x \in Z^*_p$.
- T_P: Time required to perform bilinear pairing operation $e(A, B)$, where $A, B \in G$.
- $T_{AES-Enc}$: Time required to perform a symmetric encryption operation.
- $T_{AES-Dec}$: Time required to perform a symmetric decryption operation.
- T_m: Time required to perform a modular exponential operation.
- T_{HE}: Time required to perform a homomorphic encryption operation.
- T_{PUF}: Time required to perform a PUF operation.
- T_{H_1}: Time required to perform a hash operation, where H_1: $\{0, 1\}^* \rightarrow Z^*_p$.
- T_{H_2}: Time required to perform a hash operation, where H_2: $\{0, 1\}^* \rightarrow G$.

Table 3. Time required to perform cryptography operations

Cryptography operations	Time (ms)
T_{AG}	0.07610
T_{MG}	15.82090
T_P	17.26060
$T_{AES-Enc}$	0.00794
$T_{AES-Dec}$	0.00498
T_m	0.00030
T_{HE}	0.7400
T_{PUF}	0.12
T_{H_1}	0.007380
T_{H_2}	23.61184

We first calculate the computational cost during the authentication process. In our proposed scheme, the user performs an AES encryption operation and an AES decryption operation and calculates a hash value. The smart meter performs a PUF operation to get $R = PUF(C)$, a hash value verification, an AES encryption operation, and an AES decryption operation. As shown in Table 4, the total computation cost during the authentication phase can be expressed as $T_{PUF} + 2\ T_{AES-Enc} + 2\ T_{AES-Dec} + 2\ T_{H1} = 11.805$ms. And we find that the computation cost in [10, 22, 24, 34] is 11.7096ms, 17.2615ms, 67.219ms, 82.0086ms, respectively.

Then we analyze the computational overhead of the proposed scheme in the message verification phase. First, we need to perform an addition operation of the elements on the group and three point-multiplication operations in the signature generation phase. Then we need to perform an addition operation of the elements on the group and three bilinear pairing operations in the signature verification phase. As shown in Table 4, the total computation cost during the signature generation, and verification phase can be expressed as $T_{AG} + 3T_{MG}$ and $T_{AG} + 3T_P$.

The cost of our scheme is lower than that of other schemes during the authentication phase, signature generation phase and signature verification phase, because we adopt some lightweight cryptographic operations. For example, during the authentication phase, we use the hash function to generate the key. However, bilinear pairing operations are used in [10] and [34], and it leads to more execution time. And in [24], the homomorphic encryption and decryption operations are performed when the key is generated. In the signature generation and verification phase, we take the advantage of the Chinese remainder theorem, and the control center only needs to perform one modular operation to support smart meters' dynamic operations. However, other schemes [10, 23-24, 34] all need to perform more scale multiplication operations or bilinear pairing operations to verify the legitimacy of the user, which leads to more execution time.

According to Figure 3, we can find that the cost of the authentication process of our proposed scheme is only higher than that of the scheme [24], but [24] cannot resist physical attacks. In Figure 4, we can find that in the signature generation and verification phase, the computational cost of our proposed scheme is lower than other schemes, and our scheme meets all essential security requirements. Therefore, our scheme is suitable for secure communication and group key management in the smart grid.

Table 4. Comparison of computational cost

Scheme	Auth	Sign	Verify
Ours	$T_{PUF}+2T_{AES-Enc}+2T_{AES-Dec}+2T_{H_1}$	$T_{AG}+3T_{MG}$	$T_{AG}+3T_{P}$
[24]	$T_{HE}+2T_{AES-Enc}+2T_{AES-Dec}$	$2T_{MG}+T_{H_1}+T_{AG}$	$3T_P+2T_{H_1}$
[34]	$3T_m+T_p$	$6T_{MG}+T_{H_1}+4T_{AG}+T_m$	$6T_P+3T_{MG}+T_{H_1}$
[23]	$2T_{H_2}$	$T_{H_1}+T_{H_2}+T_m+4T_{MG}$	$T_{H_1}+2T_{AG}+4T_{MG}$
[10]	$3T_{MG}+2T_P+T_{H_1}$	$8T_{MG}+5T_{AG}+T_{H_1}$	$T_{H_1}+2T_{AG}+4T_{MG}$

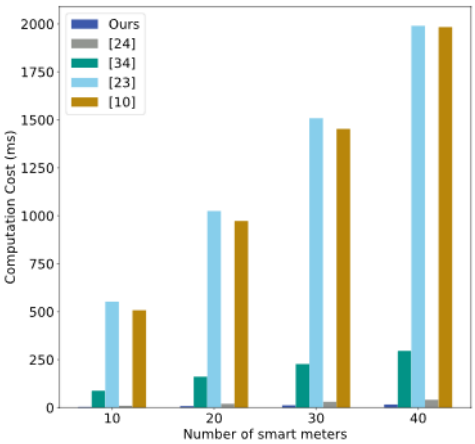


Figure 3. Computation cost during authentication phase

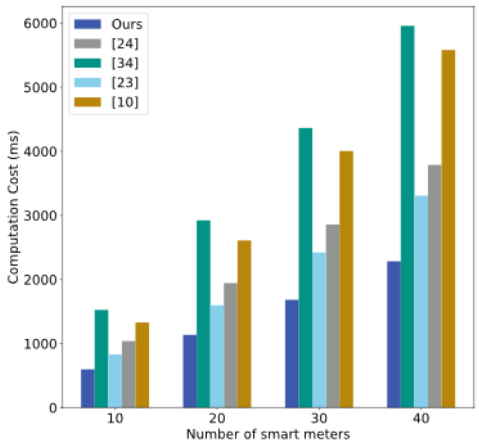


Figure 4. Computation cost sign and verify electricity data

7 Conclusion

This paper proposes a user-smart meter authentication and group key management scheme to realize secure data communication in the smart grid. In our proposed scheme, the Chinese remainder theorem technology is used to calculate and update group keys. Through this technology, our scheme can guarantee both forward and backward security. Moreover, compared with several other schemes, only our proposed scheme can resist physical attacks because of the use of PUF. And in our scheme, only some simple cryptographic primitives are used under the random oracle model and formal security analysis to prove that our solution can achieve many security requirements. Finally, performance comparisons with other schemes show that our proposal is well suited to the smart grid.

Acknowledgment

This work is supported by the National Science Foundation of China under Grants No. 62102169, the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 21KJB520033, the Key Research and Development Program (Social Development) of Lianyungang under Grant SF2102, the Excellent Teaching Team of "Qinglan Project" in Jiangsu Province under Grant No.2022-29, and the Postgraduate Research and Practice Innovation Program of Jiangsu Province SJCX22_0342.

References

[1] D. Liu, Y. Zhang, D. Jia, Q. Zhang, X. Zhao, H. Rong, Toward Secure Distributed Data Storage with Error Locating in Blockchain Enabled Edge Computing, *Computer Standards & Interfaces*, Vol. 79, Article No. 103560, January, 2022.

[2] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolammi, C. Su, Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks, *IEEE Internet of Things Journal*, Vol. 9, No. 11, pp. 8883-8891, June, 2022.

[3] W. Wang, H. Huang, L. Zhang, C. Su, Secure and Efficient Mutual Authentication Protocol for Smart Grid under Blockchain, *Peer-to-Peer Networking and Applications*, Vol. 14, pp. 2681-2693, September, 2021.

[4] W. Wang, Y. Yang, Z. Yin, K. Dev, X. Zhou, X. Li, N. M. F. Qureshi, C. Su, BSIF: Blockchain-based Secure, Interactive, and Fair Mobile Crowdsensing, *IEEE Journal on Selected Areas in Communications*, Vol. 40, No. 12, pp. 3452-3469, December, 2022.

[5] H. Yang, J. Shen, J. Lu, T. Zhou, X. Xia, S. Ji, A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in The Smart Healthcare, *Security and Communication Networks*, Vol. 2021, Article No. 5781354, September, 2021.

[6] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, An Adaptive Physical Layer Key Extraction Scheme for Smart Homes, *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 499-506.

[7] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, C. Su, A Physical-Layer Key Generation Approach Based on Received Signal Strength in Smart Homes, *IEEE Internet of Things Journal*, Vol. 9, No. 7, pp. 4917-4927, April, 2022.

[8] X. Xia, W. Qi, C. Mei, H. Wang, A Novel Protection Mechanism for Critical Mission IoT in Smart Grid, *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, Foshan, China, 2022, pp. 331-336.

[9] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, V. Chang, A Practical Group Blind Signature Scheme for Privacy Protection in Smart Grid, *Journal of Parallel and Distributed Computing*, Vol. 136, pp. 29-39, February, 2020.

[10] Z. Sui, M. Niedermeier, H. D. meer, Tai: A Threshold-based Anonymous Identification Scheme for Demand-Response In Smart Grids, *IEEE Transactions on Smart Grid*, Vol. 9, No. 4, pp. 3496-3506, July, 2018.

[11] J. L. Tsai, N. W. Lo, Secure Anonymous Key Distribution Scheme for Smart Grid, *IEEE transactions on smart grid*, Vol. 7, No. 2, pp. 906-914, March, 2016.

[12] V. Odelu, A. K. Das, M. Wazid, M. Conti, Provably Secure Authenticated Key Agreement Scheme for Smart Grid, *IEEE Transactions on Smart Grid*, Vol. 9, No. 3, pp. 1900-1910, May, 2018.

[13] R. Canetti, H. Krawczyk, Analysis of Key-Exchange Protocols and Their Use For Building Secure Channels, *international conference on the theory and applications of cryptographic techniques*, Austria, 2001, pp. 453-474.

[14] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, N. Kumar, An Identity based Authentication Protocol for Smart Grid Environment Using Physical Uncloneable Function, *IEEE Transactions on Smart Grid*, Vol. 12, No. 5, pp. 4426-4434, September, 2021.

[15] D. Sadhukhan, S. Ray, M. S. Obaidat, M. Dasgupta, A Secure and Privacy Preserving Lightweight Authentication Scheme for Smart-Grid Communication Using Elliptic Curve Cryptography, *Journal of Systems Architecture,* Vol. 114, Article No. 101938, March, 2021.

[16] A. Kumar, K. Abhishek, K. Shah, S. Namasudra, S. Kadry, A Novel Elliptic Curve Cryptography-based System for Smart Grid Communication, *International Journal of Web and Grid Services*, Vol. 17, No. 4, pp. 321–342, September, 2021.

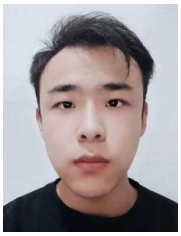
[17] A. Agarkar, H. Agrawal, J-Pake and ECC based Authentication Protocol for Smart Grid Network, *International Conference on Advances in Computing and Data Sciences*, Dehradun, India, 2018, pp. 507-522.

[18] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, Y. Xiang, Block Design-based Key Agreement for Group Data Sharing in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 16, No. 6, pp.

996-1010, November-December, 2019.
[19] C. Gentry, Z. Ramzan, Identity-based aggregate signatures, International workshop on public key cryptography, *2006 International Workshop on Public Key Cryptography*, New York, USA, 2006, pp. 257-273.
[20] A. Boldyreva, C. Gentry, A. O'Neill, D. H. Yum, Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing, *14th ACM conference on Computer and communications security*, Alexandria, VA, USA, 2007, pp. 276-285.
[21] D.-J. Lu, Y. Wang, An Identity-Based Aggregate Signature Scheme for Wireless Sensor Network Environmental Monitoring, *2019 6th International Conference on Systems and Informatics (ICSAI)*, Shanghai, China, 2019, pp. 1559-1564.
[22] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, Anonymous and Traceable Group Data Sharing in Cloud Computing, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 4, pp. 912-925, April, 2018.
[23] Z. Guan, Y. Zhang, L. Zhu, L. Wu, S. Yu, Effect: An Efficient Flexible Privacy-Preserving Data Aggregation Scheme with Authentication in Smart Grid, *Science China Information Sciences*, Vol. 62, No. 3, Article No. 32103, January, 2019.
[24] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, X. Shen, Eppdr: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 8, pp. 2053-2064, August, 2014.
[25] K. Lim, K. M. Tuladhar, X. Wang, W. Liu, A Scalable and Secure Key Distribution Scheme for Group Signature based Authentication in VANET, *2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON)*, New York, USA, 2017, pp. 478-483.
[26] A. Mansour, K. M. Malik, A. Alkaff, H. Kanaan, Alms: Asymmetric Lightweight Centralized Group Key Management Protocol for Vanets, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 3, pp. 1663-1678, March, 2021.
[27] L. E. Funderburg, I. Y. Lee, A Privacy-Preserving Key Management Scheme with Support for Sybil Attack Detection in VANETS, *Sensors*, Vol. 21, No. 4, Article No. 1063, February, 2021.
[28] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical One-Way Functions, *Science*, Vol. 297, No. 5589, pp. 2026-2030, September, 2002.
[29] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, *International conference on the theory and applications of cryptographic techniques*, Warsaw, Poland, 2003, pp. 416-432.
[30] D. Dolev, A. Yao, On the Security of Public Key Protocols, *IEEE Transactions on information theory*, Vol. 29, No. 2, pp. 198-208, March,1983.
[31] D. Liu, Z. Li, C. Wang, Y. Ren, Enabling Secure Mutual Authentication and Storage Checking in Cloud-assisted Iot, *Mathematical Biosciences and Engineering*, Vol. 19, No. 11, pp. 11034-11046, August, 2022.
[32] L. Law, B. J. Matt, Finding Invalid Signatures in Pairing-based Batches, *IMA International Conference on Cryptography and Coding*, Cirencester, UK, 2007, pp. 34-53.
[33] C. Wang, J. Shen, P. Vijayakumar, B. B. Gupta, Attribute-based Secure Data Aggregation for Isolated IoT-enabled Maritime Transportation SystemsAttribute-based Secure Data Aggregation for Isolated IoT-enabled Maritime Transportation Systems, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24 No. 2, pp. 2608-2617, February, 2023.
[34] T. Jeske, Privacy-Preserving Smart Metering without a Trusted-Third-Party, *Proceedings of the International Conference on Security and Cryptography*, Seville, Spain, 2011, pp. 114-123.
[35] D. Liu, Y. Zhang, W. Wang, K. Dev, S. A. Khowaja, Flexible Data Integrity Checking with Original Data Recovery in IoT-enabled Maritime Transportation Systems, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 2, pp. 2618-2629, February, 2023.
[36] P. Gope, B. Sikdar, Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication, *IEEE Transactions on Smart Grid*, Vol. 10, No. 4, pp. 3953-3962, July, 2019.

Biographies

Yang Zhou received the B.E. degree in 2020 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include cryptography, authentication, smart grid.



Bing Yang received the B.E. degree in 2021 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology Nanjing, China. His research interests include cryptography, cloud auditing, cloud storage.

Dengzhi Liu received the M.E. degree and Ph.D. degree from the School of Computer and Software, Nanjing University of Information Science and Technology, in 2017 and 2020, respectively. He is currently an Assistant Professor with the School of Computer Engineering, Jiangsu Ocean University, China. He mainly focuses on the security and privacy issues in data storage and transmission. He has authored more than 50 research papers and published in international conferences and journals. His current research interests include cloud computing security, edge computing security, cyber security, electronic forensics, and data security.