frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 09 January 2024
DOI 10.3389/fenrg.2023.1298837

OPEN ACCESS

EDITED BY
Haris M. Khalid,
University of Dubai, United Arab Emirates

REVIEWED BY
Aravind C. K.,
Mepco Schlenk Engineering College, India
Md. Rasel Sarkar,
University of New South Wales, Australia

*CORRESPONDENCE
Lei Zhang,
zhanglei@gpnu.edu.cn

RECEIVED 22 September 2023
ACCEPTED 20 December 2023
PUBLISHED 09 January 2024

CITATION
Wang M and Zhang L (2024), Efficient privacy protection scheme with batch verification in smart grid.
Front. Energy Res. 11:1298837.
doi: 10.3389/fenrg.2023.1298837

Efficient privacy protection scheme with batch verification in smart grid

Mingxiang Wang[1] and Lei Zhang[1,2]*

[1]School of Computer Science, Guangdong Polytechnic Normal University, Guangzhou, China, [2]School of Information Engineering, East University of Heilongjiang, Harbin, China

Smart grids can establish two-way communication with users, collect their electricity consumption data and provide reasonable pricing, but fine-grained electricity consumption data leads to the leakage of user privacy. In order to protect the privacy of user data and the security of data transmission process, this article proposes an efficient and batch validated privacy protection scheme. In this scheme, legitimate entities transmit encrypted electricity data after mutual authentication. To ensure the correct data is received, we propose a new batch signature verification algorithm. Security analysis shows that our solution achieves user privacy and data security. The simulation experiments provided demonstrate that the efficiency of the proposed scheme can satisfy the requirements of real-time communication.

KEYWORDS

high efficiency, batch validation, privacy protection, mutual authentication, homomorphic aggregation

1 Introduction

Smart grid is a replacement for traditional power grid. Smart grid combines advanced network communication technology, smart sensor equipment and big data analysis capability to provide efficient, stable and economical power distribution for the power grid. Build two-way communication between smart grid and users, collect fine-grained power consumption data on the user side through smart sensor devices, use big data analysis capabilities to analyze users' power consumption habits, grasp the fluctuations of power consumption, achieve stable power supply by regulating power generation, and reduce power loss. Because power is not convenient to store, it is essential to generate power according to supply and demand. However, collecting user electricity consumption data poses a serious problem, which is that the privacy of user electricity consumption may be obtained by malicious attackers to disrupt the stable operation of the power grid. Several proposals have been put forward regarding the protection of user privacy. However, there are pros and cons, and the existing issues have not been completely resolved. Therefore, solving the leakage of user privacy is an urgent issue for smart grids.

In order to address user privacy breaches, data aggregation is used to aggregate all user data together, making it impossible for anyone except the user to obtain detailed electricity consumption data. Legitimate data users can only obtain the aggregated data for analysis. Specifically, the user's data is not directly sent to the data user, but is first aggregated through a legitimate third party and then forwarded to the data user; During the transmission of user data, in order to prevent malicious attackers from directly obtaining power data, data encryption is required. Therefore, we need a scheme that supports homomorphic encryption to achieve data privacy and security.

Homomorphic encryption includes homomorphic addition and homomorphic multiplication. At present, many homomorphic encryption technologies have been implemented, including semi-homomorphic encryption and full homomorphic encryption. Semi-homomorphic encryption can achieve additive homomorphisms or multiplicative homomorphisms, and full homomorphic encryption can achieve additive homomorphisms and multiplicative homomorphisms. For example, paillier homomorphic encryption can realize additive homomorphism. But relatively speaking, the computational complexity of homomorphic encryption of paillier is relatively high, which has a great burden on smart meters in practical applications. All homomorphic encryption can achieve aggregation in the ciphertext domain, but the current technology is difficult to achieve efficient all homomorphic technology. For our solution, implementing additive homomorphism can meet the aggregation requirements of data, therefore, an efficient additive homomorphism technique is needed.

In this article, we propose an efficient smart grid privacy protection scheme that can achieve efficient identity authentication and effective data aggregation. In order to achieve effective data transmission, we need to authenticate the entities participating in the power grid. During the data transmission process, only the data of the authenticated entities will be accepted. We have designed an identity verification algorithm between participating entities to ensure the effectiveness of data transmission. To improve efficiency, our identity verification can achieve batch verification. In order to aggregate user electricity data, we used an encryption technology that supports additive homomorphism to achieve efficient data aggregation. Specifically, in our scheme, before data upload, we need to verify the identity of the control center and the intermediate aggregator. After the verification is successful, the user uses homomorphic encryption technology to encrypt the power data. At the same time, the user needs to sign the data to ensure correct user data upload. The intermediate aggregator aggregates user data after receiving the user's encrypted data and verifying the user's identity, After being signed, it will be forwarded to the control center, which will decrypt the aggregated data after verifying the identity of the aggregator, and provide appropriate power consumption strategy through analyzing the aggregated data.

Overall, the specific contributions of our proposed solution are as follows:

(1) We have designed an efficient privacy protection scheme based on the requirements of the smart grid, which can achieve effective data aggregation and protect user privacy.
(2) In order to protect the security of the data upload process, we have designed an identity signature verification algorithm that allows legitimate users to upload power consumption data. To improve efficiency, the identity verification algorithm can achieve batch verification operations.
(3) Our solution can resist attacks from malicious attackers, including internal attacks, external attacks, collusion attacks, and ensure the integrity and confidentiality of data.

The remaining organization of this article is as follows. In the second part, we reviewed previous work in this field and explored the advantages and disadvantages of relevant literature. In the third part, we give the related Cryptography knowledge and symbol explanation involved in this paper. In the fourth part, we provide the system model and security requirements. In the fifth section, a detailed solution process is provided to explain the establishment of the system model. In the sixth section, we analyzed and compared the security of the schemes. In Section 7, a performance evaluation was conducted to demonstrate that the stable operation of the system can be achieved. Finally, we provide the conclusion in Section 8.

2 Related work

In this section, we summarized and explored privacy protection schemes in smart grids.

Privacy protection is an important issue that needs to be addressed in smart grids. Many solutions have been proposed for privacy protection (Fan et al., 2013; Abdallah and Shen, 2014; Li et al., 2014; Li et al., 2015; Abdallah and Shen, 2018; Gong et al., 2018; Guo et al., 2018; Vincent et al., 2018; Fan et al., 2020; Hua et al., 2020; Song et al., 2020; Wei et al., 2020; Qian et al., 2021; Roozbeh et al., 2021; Zhang et al., 2022a; Baghestani et al., 2022; Zhang et al., 2022b; Mall et al., 2022; Nyangaresi, 2022; Sadhukhan et al., 2022; Sani et al., 2022; Zhao et al., 2022; Cao et al., 2023; Deng et al., 2023; Hu et al., 2023; Verma et al., 2023; Zhang and Dong, 2023), mainly focusing on data aggregation. Compared to other methods, data aggregation performs the best. For example, the method based on masking value can insert random values used to mask data into user data to achieve the purpose of confusing data. Malicious attackers cannot get effective data, but will lead to data loss and deviation of the final data. There is also a scheme based on secret sharing to build a secret shared between the two communication parties to achieve secure data transmission, but for internal attackers, the security of data cannot be guaranteed.

Data aggregation is realized by homomorphic encryption. Li et al. (2015) proposed a new privacy protection dual function aggregation scheme (PDA) for smart grid communication. This scheme uses the ring learning problem with errors to construct a homomorphic encryption scheme. When users report power data, they can calculate multiple statistical values in the encrypted case, improving the use value of the data, but the computational cost is high. Abdallah and Shen (2018) first proposed a lightweight privacy protection aggregation scheme based on lattice, which uses hard noise matrix and soft noise matrix to construct encryption, allowing smart appliances to aggregate data without involving smart meters. Smart meters serve as relay nodes, only transmitting data, and are suitable for small networks in single households. Abdallah and Shen (2014) used the homomorphic encryption technology based on NTRU lattice. NTRU lattice has a lower computing cost and also reduces the communication cost, because NTRU lattice encryption only requires simple multiplication and addition, making the system more lightweight. This scheme distributes electricity consumption data to users in the predicted area, in order to better protect user privacy and isolate the control center and users, and communicate separately with relay nodes. The

only drawback is that the literature indicates that this scheme is applied to small networks. Qian et al. (2021) first proposed a lightweight t-times homomorphic encryption scheme, which can further reduce the computing cost of intelligent devices. The scheme uses lattice based homomorphic encryption technology, which can resist quantum attacks. On this basis, two effective data aggregation schemes were proposed for application scenarios. The first solution is suitable for small networks, such as home networks and small office networks. The second solution is suitable for medium-sized networks, such as part of smart cities. Song et al. (2020) proposed a dynamic member data aggregation (DMDA) scheme using homomorphic encryption and identity based signature, which reduces the complexity of new users joining and old users exiting. In addition, the Action Center obtains the total data in the virtual aggregation area, and knows nothing about the data of a single user. However, communication is also required between meters, which increases the communication burden of edge device to a certain extent. Hua et al. (2020) first proposed a new type of attack called malicious data mining attack, through which opponents can infer the target user's electricity consumption data. Then aiming at this attack, a new data aggregation scheme is proposed. This scheme uses Paillier homomorphic encryption technology to encrypt data, and uses bilinear map to sign, which can not only resist malicious data mining attacks, but also output accurate aggregation results. Li et al. (2014) proposed an effective privacy protection demand response (EPPDR) scheme, which uses homomorphic encryption and bilinear pairing to achieve privacy protection demand aggregation and effective response. We also studied an adaptive key evolution technique that can adaptively control key evolution to ensure that the user's session key is forward secure. Unfortunately, neither of these schemes is lightweight and cannot resist quantum attacks.

In order to ensure the legality of identity and data security during the aggregation process, many authentication schemes have been proposed (Guo et al., 2020; Sui and Meer, 2020; Sanaullah Badar et al., 2022). Hafiz et al. (Sanaullah Badar et al., 2022) provide a secure authentication protocol for home domain networks. The article uses the physical non-destructive architecture of ECC and smart meters to ensure identity security. Sui and Meer (2020) proposed a batch and auditable privacy protection scheme for smart grid demand response, which can achieve batch identity verification and reward users who participate in demand response. Guo et al. (2020) proposed a lightweight batch verification privacy protection data aggregation scheme, which uses symmetric encryption algorithms to encrypt data after establishing session keys. However, symmetric encryption may lead to data leakage. In summary, current methodologies are incapable of ensuring all the benefits, such as being lightweight, resilient against all threats, and widely applicable. As a result, it is imperative to put forth novel approaches for privacy protection. Within our proposed privacy protection scheme, our primary objective is to attain data privacy security while simultaneously addressing prerequisites like being lightweight and resistant to malicious attacks.

3 Preliminaries

In this scheme, we use the NTRU scheme, which implements ECC and RSA on a lattice. The security of the scheme is based on the shortest vector problem.

3.1 NTRU lattice scheme

Let n be a power of 2, $\Phi = xn + 1, \mathcal{R} = \frac{\mathbb{Z}[x]}{\Phi}, \sigma \in \mathbb{R}$, q is a prime number such that Φ There are n linear factors $mod\, q (q = 1\, mod\, 2n)$: $\Phi = \prod_{i \le n} \phi_i = \prod_{i \le n} (x - \varphi_i) mod\, q, \mathcal{R}_q = \frac{\mathcal{R}}{q\mathcal{R}} = \frac{\mathbb{Z}_q[x]}{\Phi}, \mathcal{R}_q^*$ is the set of inverse elements of $\mathcal{R}_q$.

1) Key generation: Given $n, q \in \mathbb{Z}, p \in \mathcal{R}_q^*$, sampling the f', g' from the discrete Gaussian $\mathcal{D}_{\mathbb{Z}^n,\sigma}$.We can calculate the:

$$f = p \cdot f' + 1 \tag{1}$$

Here $(f mod\, q) \in \mathcal{R}_q^*, f = 1\, mod\, p$, we calculate the public key value h using the private key f, as follows:

$$h = \frac{pg'}{f} \in \mathcal{R}_q^* \tag{2}$$

Therefore, we obtain the public-private key pair $(h, f) \in \mathcal{R}_q^* \times \mathcal{R}$.

2) Encryption: For the message m that needs to be encrypted, the sender randomly generates two random numbers $s, e \leftarrow \bar{\gamma}_\alpha$, Use a public key for encryption as follows:

$$C = hs + pe + m \in \mathcal{R}_q \tag{3}$$

3) Decryption: When decrypting, the private key f can be used for decryption, as follows:

$$C' = f \cdot C \in \mathcal{R}_q \tag{4}$$

$$m = C'\, mod\, p \tag{5}$$

4) Homomorphic property: Assuming there are two users, each generating message m_1, m_2. Randomly select random numbers $(s_1, e_1), (s_2, e_2)$, and use public key encryption to obtain: $C_1 = hs_1 + pe_1 + m_1, C_2 = hs_2 + pe_2 + m_2$. Assuming $C = C_1 + C_2$, the homomorphic properties are as follows:

$$\begin{aligned} C &= hs_1 + pe_1 + m_1 + hs_2 + pe_2 + m_2 \\ &= h(s_1 + s_2) + p(e_1 + e_2) + (m_1 + m_2) \end{aligned} \tag{6}$$

3.2 Bilinear map

Assuming $\mathbb{G}, \mathbb{G}_T$ is two multiplicative cyclic group, which have the same order prime number q, and define Bilinear map e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Meet the following characteristics:

1) Bilinear: For all $u, v \in \mathbb{G}, a, b \in \mathbb{Z}_q$, satisfy $e(u^a, v^b) = e(u, v)^{ab}$.
2) Non-degeneracy: Assuming $\mathbb{G}$ randomly generates g, then $e(g, g) \neq 1$.

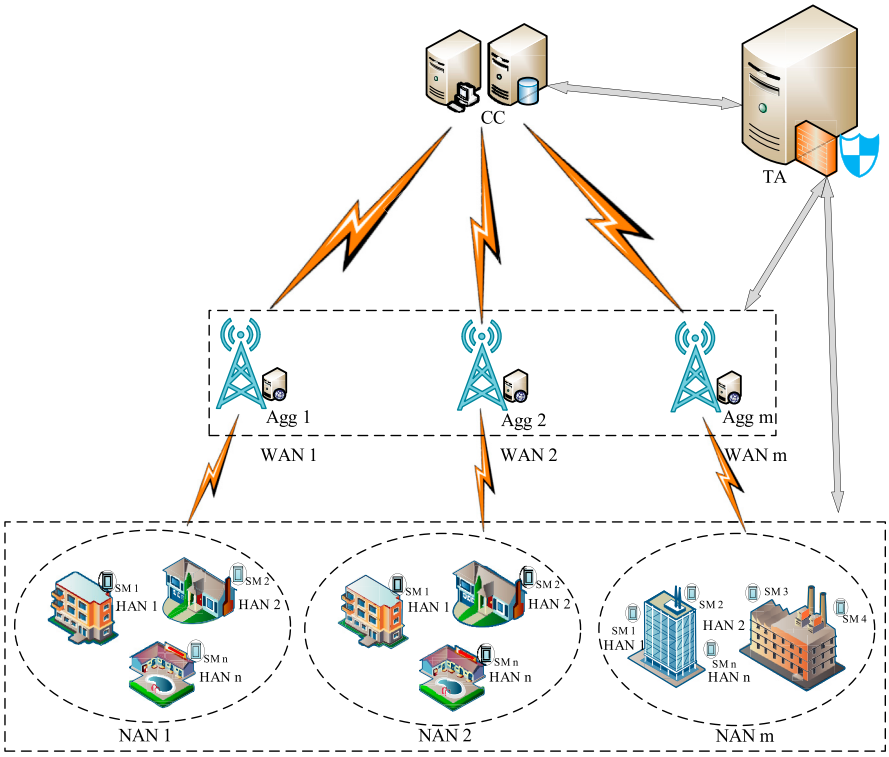


FIGURE 1
System model.

3) Computability: For every $u, v \in \mathbb{G}$, there must be an effective algorithm to calculate $e(u, v)$.

4 System model and design objectives

4.1 System model

In our proposed scheme, there are four entities: trusted third party (TA) for key distribution, control center (CC) for data collection, and m intermediate aggregator Agg_i for data aggregation, $(i \in [1, m])$. N smart meters SM_{ij} under Agg_i, $(j \in [1, n])$. Figure 1 specifically describes the system model of the proposed scheme, as well as explanations of the corresponding symbols. Below is an introduction to the role of each entity.

In an intelligent grid environment, the communication network is represented by a layered architecture. The communication network layer can be divided into three main network transmission layers: 1) Wide Area Network (Wide Area Network, WAN), 2) Neighborhood Area Network (Neighborhood Area Network, NAN), and 3) Home Area Network (Home Area Network, HAN).

Wide Area Network (WAN): It provides communication between the power company and all distribution substations. WAN has distributed generation and storage capabilities and is a high-bandwidth bidirectional communication network. It employs advanced monitoring and control techniques to handle long-distance information transmission and achieve real-time responsiveness. Fiber optics and microwave communications are suitable for WAN due to their high bandwidth, low latency, and reliable communication requirements.

Neighborhood Area Network (NAN): It covers the communication framework of distribution substations' network, enabling automatic distribution and control of communication between all nodes within the network. NAN acts as a bridge between HAN and WAN, processing the information sent by HAN through NAN and sending it to WAN via data concentrators. Fiber optics, WiMAX, cellular, and RF grid technologies are preferred transmission technologies for NAN.

Home Area Network (HAN): It is the communication framework for the user end of distribution substations, providing a communication network for the user area and located at the furthest end of the network architecture. It collects electricity usage information through smart meters, manages and provides feedback on users' electricity consumption behaviors. HAN has the characteristics of low bandwidth, low speed, and low cost communication. ZigBee, Wi-Fi, and other technologies are candidates for HAN communication.

TA: A trusted third party is a fully trusted institution that stores the identities of all legitimate entities. TA generates system parameters for other entities for authentication between different entities.

CC: The control center is an honest and curious entity, mainly used for the collection and analysis of power data. By collecting regular power consumption data of users, CC can predict the next power consumption of users through big data analysis, adjust the generation capacity and formulate reasonable electricity prices, and users can receive electricity price information and decide on their own electricity use.

Agg: The intermediate News aggregator is an honest and curious entity. Agg is the relay node between CC and SM. It aggregates power data from all SM in the region and forwards it to CC.

SM: Smart electricity meter is an honest and curious entity. SM is a edge device deployed on the user side. It records the power consumption data of users and transmits it to Agg encrypted.

For system modeling, we first use TA to generate the required system parameters for distribution to other entities. Secondly, other entities need to mutually authenticate each other to ensure the legitimacy of the participating entities before uploading data. Finally, SM uploads encrypted data, which is aggregated and forwarded to CC by Agg. CC can decrypt the aggregated data. Throughout this process, all entities except the user are unable to access the corresponding personal private data.

4.2 Attack model

In our proposed solution, we specifically consider the following attack models:

1) External attacks: external attacks refer to attackers from outside the system, such as malicious smart meters, aggregator and other attackers. They attempt to forge legal identities to steal power data, forge false power data to disrupt the stable operation of the power system, and may also launch denial of service attacks (DoS attacks).
2) Internal attack: In our proposed solution, CC and Agg are both honest and curious entities that faithfully complete system tasks. Agg may learn plaintext message content from the received SM data, and CC may learn user personal power data from the received aggregated data.
3) Collusive attack: CC and Agg may launch a collusive attack to obtain data from a single user.

4.3 Design objectives

Our solution should meet the following design goals for the defined attack model:

1) Authentication of legitimate users: Before uploading user data, the scheme can verify the identity of each participant in the system and detect the false identity of malicious attackers, ensuring that the data is forwarded by legitimate entities.
2) Integrity and confidentiality of power data: In the proposed solution, we should ensure the security of encrypted power data, that is, integrity and confidentiality. In the process of power data transmission, even if a malicious attacker obtains encrypted data, he/she cannot decrypt the data, and internal attackers cannot obtain detailed personal data. Even if a collusive attack is launched, only aggregated data can be obtained.
3) Batch verification: The solution should enable batch processing of identity verification during the message upload process, improve verification efficiency, and reduce system operation consumption.
4) Privacy of user: In the scheme, we should ensure the privacy of user, while CC can only obtain aggregated power data, Agg can only obtain encrypted data, and they cannot infer any information about the user.

TABLE 1 Symbols and interpretation.

Symbols	Interpretation
CC	Control center, responsible for collecting and analyzing power data
TA	Trust Center, responsible for generating system parameters
Agg_i	The i-th aggregator
SM_{ij}	The j-th smart meter under the i-th aggregator
m	Maximum number of aggregator
n	Maximum number of smart meters in each aggregator
ID_C	CC's ID
ID_i	ID of the i-th aggregator
ID_{ij}	Identity ID of the j-th smart meter under the i-th aggregator
h	CC generated encrypted public key
f	CC generated encrypted private key
m_{ij}	Power data plaintext generated by SM_{ij}
C_{ij}	Power data ciphertext generated by SM_{ij}
s_{ij}, e_{ij}	SM_{ij} Randomly selected random number, $s_{ij}, e_{ij} \leftarrow \bar{y}_\alpha$
(X_C, x_C)	CC's Public private key pairs generated by system parameters, $x_C \in \mathbb{Z}_q, X_C \in \mathbb{G}$
(X_i, x_i)	Agg_i's public and private key pairs generated by system parameters, $x_i \in \mathbb{Z}_q, X_i \in \mathbb{G}$
(X_{ij}, x_{ij})	SM_{ij}'s public private key pair generated by system parameters, $x_{ij} \in \mathbb{Z}_q, X_{ij} \in \mathbb{G}$
y_{ij}	TA distributes Random number to SM_{ij}, $y_{ij} \in \mathbb{R}$
H: $\{0,1\}^* \rightarrow \mathbb{G}$	Global hash function, mapped from $\{0,1\}^*$ to $\mathbb{G}$
H_1: $\{0,1\}^* \rightarrow \{0,1\}^\lambda$	Hash function, mapping from $\{0,1\}^*$ to $\{0,1\}^\lambda$

5 Proposed solution

In this section, we will provide a detailed design process, which is divided into five stages: A. System initialization stage; B. Certification stage; C. Data reporting stage; D. Decrypting data stage; E. Analysis and feedback stage and Table 1 provides some symbols used in the proposed scheme.

5.1 System initialization phase

1) Generating system parameters: TA defines two multiplicative cyclic group $\mathbb{G}, \mathbb{G}_T$ with prime q. $\mathbb{G}$ randomly generates g and defines a Bilinear map e: e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Hash function

H: $\{0,1\}^* \to \mathbb{G}$, H_1: $\{0,1\}^* \to \{0,1\}^\lambda$, For SM_{ij} randomly generates random numbers $y_{ij} \in \mathbb{R}$, satisfies $\sum_{i=1}^{n} y_{ij} = 0$. TA broadcasting system parameters $\{\mathbb{G}, \mathbb{G}_T, g, e, H, H_1\}$ are given to all participating entities, and CC generates encrypted public and private key pairs $(h, f) \in \mathcal{R}_q^* \times \mathcal{R}$ through the NTRU algorithm.

2) Registered identity: CC randomly selects a random number $x_C \in$ $_q$. Calculate $X_C = g^{x_C}$, send $\{H_1(\mathrm{ID}_C) \parallel X_C\}$ to TA, and TA calculates $H_1(\mathrm{ID}_C)$ based on the stored identity ID_C, if CC's authentication passes, TA broadcasts X_C; Agg_i randomly select a random number $x_i \in$ $_q$, calculate $X_i = g^{x_i}$, send $\{H_1(\mathrm{ID}_i) \parallel X_i\}$ to TA, and TA calculates $H_1(\mathrm{ID}_i)$ based on the stored ID_i, if the identity of Agg_i verification passed, TA broadcast X_i; SM_{ij} randomly select a random number $x_{ij} \in$ $_q$, calculate $X_{ij} = g^{x_{ij}}$, send $\{H_1(\mathrm{ID}_{ij}) \parallel X_{ij}\}$ to TA, and TA calculates $H_1(\mathrm{ID}_{ij})$ based on the stored ID_{ij}, if the identity of SM_{ij} verification passed, TA broadcast X_{ij}; Distribute y_{ij} through secure channels to SM_{ij}.

5.2 Certification stage

1) CC → Agg_i: CC wants to collect user data, first of all, it needs to report to Agg_i prove its identity, use own identity private key to encrypted the collect data request $\mathcal{Q}$, generate a signature and send it to Agg_i. Namely, $\sigma_c = H(\mathcal{Q}, T_v)^{x_c}$, T_v is a timestamp, which can resist Replay attack. Send $\{\mathcal{Q}, \sigma_c, h, T_v\}$ To Agg_i. Agg_i receive the request and signature sent by CC, first verify the timestamp, and then calculate $e(H(\mathcal{Q}, T_v), X_C) = e(\sigma_c, g)$ to verify the identity of CC.
2) $\mathrm{Agg}_i \to SM_{ij}$: After Agg_i verifying the identity of CC, it need to forward the data collection request to SM_{ij}. Agg_i first need to report to SM_{ij} proves identity, encrypts data collection request $\mathcal{Q}$ using its own identity private key, generates a signature, and sends it to SM_{ij}, i.e., $\sigma_i = H(\mathcal{Q}, T_v)^{x_i}$, T_v is the timestamp, sending $\{\mathcal{Q}, \sigma_i, h, T_v\}$ To SM_{ij}, SM_{ij} received the request and signature sent by Agg_i first verify the timestamp, and then calculate $e(H(\mathcal{Q}, T_v), X_i) = e(\sigma_i, g)$ Verify the identity of Agg_i. If the identity of Agg_i is correct, then SM_{ij} executes data collection requests.

```
Input:
  Q, x ∈ _q, g, H.
Output:
  {Q, σ, T_v}
A randomly select x ∈ _q
Let X = g^x
Let σ = H(Q, T_v)^x
Send {Q, σ, T_v} to B
B check T_v, then
If e(H(Q, T_v), X_C) = e(σ, g) then
  Verification passed
  Else
  reject
End
```

Algorithm 1. Authentication Algorithm.

5.3 Data reporting phase

1) $SM_{ij} \to \mathrm{Agg}_i$: After SM_{ij} verified the identity of Agg_i, execute the request to collect data and generate electricity data m_{ij}, encrypting power data using the public key h sent by CC, SM_{ij} select random number $s_{ij}, e_{ij} \leftarrow \bar{\gamma}_\alpha$, TA generated y_{ij} for SM_{ij}, use Formula 3 to calculate the encrypted ciphertext: $C_{ij} = hs_{ij} + pe_{ij} + m_{ij} + y_{ij}$, generate a signature using the identity private key before forwarding the ciphertext: $\sigma_{ij} = H(C_{ij}, T_v)^{x_{ij}}$, forwarding $\{\{C_{ij}, \sigma_{ij}, T_v\}$ To Agg_i.
2) $\mathrm{Agg}_i \to$ CC: After Agg_i have received all the data is forwarded by SM_{ij}, the timestamp T_v needs to be verified first. Then calculate $\sum_{j=1}^{n} e(H(C_{ij}, T_v), X_{ij}) = \sum_{j=1}^{n} e(\sigma_{ij}, g)$, if the equation holds, then Agg_i aggregate all received power data form SM_{ij}, $C_i = \sum_{j=1}^{n} C_{ij}$, otherwise, discard the data. Illegal users can be found by verifying a single identity signature. After aggregating all data, Agg_i calculate $\sigma_i = H(C_i, T_v)^{x_i}$, generate its signature, forward $\{C_i, \sigma_i, T_v\}$ To CC. The specific identity authentication and encryption algorithms are described in Algorithm 1 and Algorithm 2.

```
Input:
  n, q ∈ ℤ, p ∈ R_q^*, σ ∈ ℝ, s_ij, e_ij ← γ̄_α, y_ij ∈ ℝ, m_ij .
Output:
  C_ij
Sample f' from D_{ℤ^n,σ}, let f = p · f' + 1
If (f mod q) ∉ R_q^*,
  resample.
Sample g' from D_{ℤ^n,σ},
If (g' mod q) ∉ R_q^*,
  resample
Return secret key sk = f and public key pk = pg'/f ∈ R_q^*.
Set s_ij, e_ij ← γ̄_α, y_ij ∈ ℝ
Let C_ij = hs_ij + pe_ij + m_ij + y_ij
Return C_ij
```

Algorithm 2. Encryption Algorithm.

5.4 Decrypting data stage

CC decrypts data: After CC received data form Agg_i aggregated SM_{ij}, first verify the timestamp, and then calculate $\sum_{i=1}^{m} e(H(C_i, T_v), X_i) = \sum_{i=1}^{m} e(\sigma_i, g)$. If the equation holds, CC receives the correct aggregated data, and *vice versa*, discards the data. CC decrypts the received aggregated data through its own encrypted private key f. CC is calculated using Formula 4:

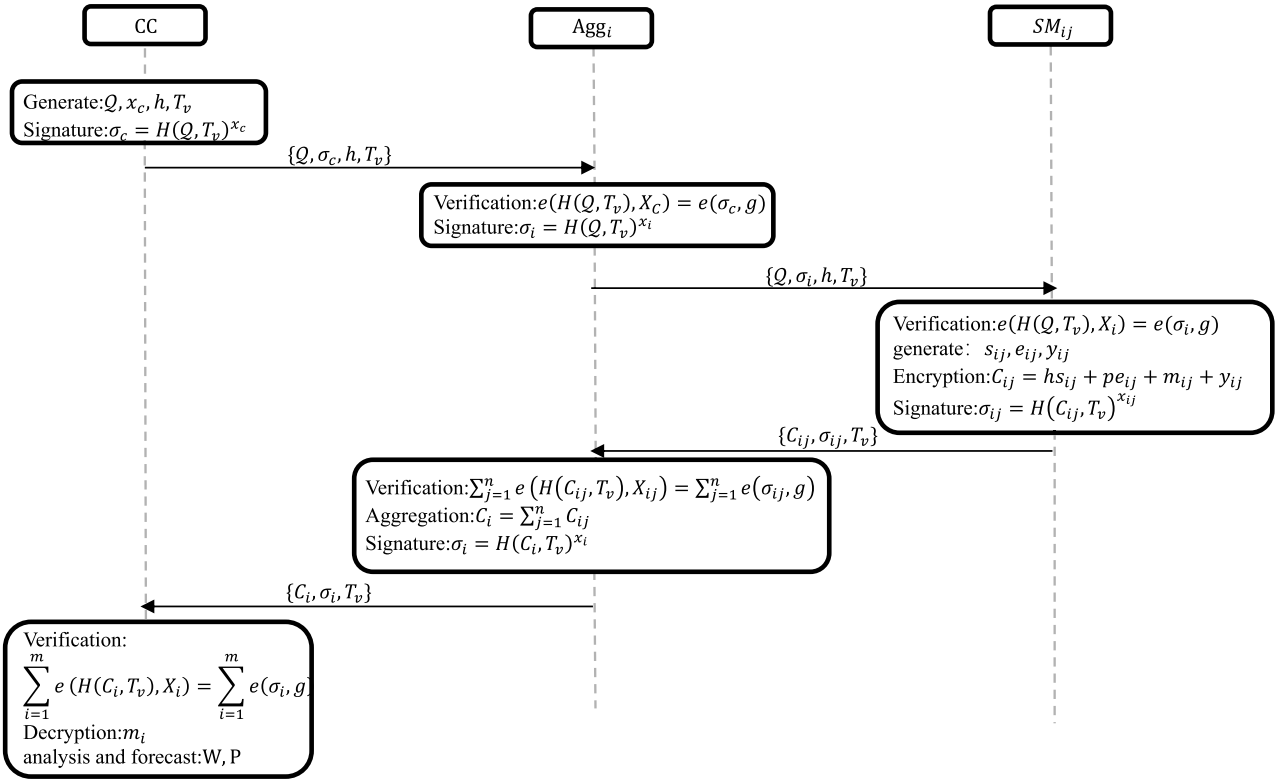
$$C' = f \cdot C_i = f \cdot \sum_{j=1}^{n} \left(hs_{ij} + pe_{ij} + m_{ij} + y_{ij}\right) \tag{7}$$

use Formula 5 to calculate:

$$m_i = C' \bmod p = \sum_{j=1}^{m} m_{ij} \tag{8}$$

m_i is the decrypted aggregated data. Algorithm 3 describes the decryption algorithm Formula 9 proves the correctness of decryption.

TABLE 2 Flow chart of the proposed solution.




```
Input:
  C_ij, f.
Output:
  m_i
Let C_i = ∑_{j=1}^{n} C_ij
Let C' = f · C_i = f · ∑_{j=1}^{n} (hs_ij + pe_ij + m_ij + y_ij)
Let m_i = C' mod p = ∑_{j=1}^{m} m_ij
Return m_i
```

Algorithm 3. Decryption Algorithm.

5.5 Analysis and feedback stage

After CC decrypts the aggregated data, it analyzes the data and predicts the power generation W and time of use electricity price P for the next period of time. The time of use electricity price P is sent to users for adjusting their electricity consumption (Table 2).

6 Safety analysis

In this section, we provide a security proof of the scheme based on the design objectives, which mainly includes four aspects: secure identity authentication, integrity of power data, confidentiality of power data, and privacy of user identity. At the same time, we also made comparisons with other solutions.

6.1 Secure identity authentication

We have described the security verification of the proposed scheme. Specifically, the signature verification of the scheme is based on the CDH assumption of hardness, and only the verified ID can perform correct signature verification. Without the help of the trust center, attackers cannot forge a valid signature because the collision resistance and unidirectionality of the hash function cannot find two different IDs with the same output, nor can input values be found through hash values. Therefore, we have achieved resistance to external attacks.

Theorem 1. Assuming a hash function H_1 is a random oracle. If the CDH problem is difficult to solve, then our identity authentication algorithm has the ability to reduce losses $L = q_H$'s EU-CMA security model is provably secure, where q_H is the number of hash requests queried from the random oracle (Wei et al., 2020).

Proof: Assuming the existence of an adversary $\mathcal{A}$, it is possible to use advantage of (t, q_s, ε) breaking the signature scheme. We can construct a simulator $\mathcal{B}$ to call adversary $\mathcal{A}$ to solve the CDH problem, given $g, g^a, g^b \in \mathbb{G}$, and calculate g^{ab}. Simulator $\mathcal{B}$ controls the random oracle and calls $\mathcal{A}$ to perform the following steps.

1) Setup: B sets the public key $X = g^x$. The public key is obtained from the given $\mathbb{G}$, and the simulator does not know the private key x.
2) H-Query: $\mathcal{A}$ performs a hash query at this stage. $\mathcal{B}$ randomly selects an integer $i^* \in [1, q_H]$ before receiving $\mathcal{A}$'s query. Then

$\mathcal{B}$ prepares a Hash table (initially empty) to store all hash queries and results. Assuming the i-th hash query is m_i. The timestamp is T_v. If m_i is already in the Hash table, and $\mathcal{B}$ responds to the corresponding information in the table. Otherwise, $\mathcal{B}$ randomly selects a $w_i \in$ $_q$. Respond to the following information:

$$H(m_i, T_v) = \begin{cases} g^{b+w_i}, \text{if } i = i^* \\ g^{w_i}, \text{otherwise} \end{cases}$$

$\mathcal{B}$ responds to the query corresponding to $H(m_i, T_v)$ and adds $(i, m_i, w_i, H(m_i))$ to the Hash table.

3) Query: $\mathcal{A}$ performs signature query at this stage. For signature query on m_i, if m_i is the i^*-th query message in the Hash table, it will be aborted. Otherwise, obtain $H(m_i, T_v) = g^{w_i}$, and $\mathcal{B}$ calculates the signature: $\sigma_{m_i} = (g^a)^{w_i}$, σ_i is the correct signature of m_i.
4) Forgery: $\mathcal{A}$ returns a forged signature σ_{m^*} for a message m^*. If m^* has't been queried the i^*-th query message in the Hash table, terminate; otherwise, $H(m^*, T_v) = g^{b+w_{i^*}}$ is obtained. Through the definition of signature, we obtain: $\sigma_{m^*} = (g^{b+w_{i^*}})^a = g^{ab+aw_{i^*}}$, $\mathcal{B}$ calculation:

$$\frac{\sigma_{m^*}}{(g^a)^{w_{i^*}}} = \frac{g^{ab+aw_{i^*}}}{(g^a)^{w_{i^*}}} = g^{ab}$$

g^{ab} is the solution to the CDH problem.

6.2 Integrity of power data

In this section, we explain that the proposed scheme can ensure the integrity of power data.

1) Security of signature algorithms

We use signature algorithms to ensure legal identity while transmitting data, and also verify whether the encrypted ciphertext has been tampered and forged. In SM_{ij} forwarded the message to Agg_i, we perform a hash operation on the ciphertext and timestamp. If the ciphertext is tampered with and forged during transmission, the equation: $\sum_{j=1}^{n} e(H(C_{ij}, T_v), X_{ij}) = \sum_{j=1}^{n} e(\sigma_{ij}, g)$ is not hold, ensures the integrity of our ciphertext.

2) The correctness of encryption algorithm decryption

Lemma 1. If $\omega(n^{1.5}\log n)\alpha \deg(p)\| p \|^2\sigma < 1 (resp.\omega(n^{0.5}\log n)\alpha\| p \|^2\sigma < 1) if \deg p \le 1$, then when the NTRU decryption algorithm selects s, e, f, g with a probability of $1 - n^{-\omega(1)}$ Restore m_i (Zhao et al., 2022).

Proof: In the decryption algorithm, we have $C' = f \cdot \sum_{j=1}^{n} (hs_{ij} + pe_{ij} + m_{ij} + y_{ij}) mod\, q$, on $\mathbb{R}$, we calculate $C'' = f \cdot \sum_{j=1}^{n} (hs_{ij} + pe_{ij} + m_{ij} + y_{ij})$. If $\| C'' \|_\infty < \frac{q}{2}$, then $C' = C''$ on $\mathbb{R}$, therefore, when $f = 1 \, mod\, p$, $C' \, mod\, p = C'' \, mod\, p = m_i \, mod\, p$, which means our decrypted plaintext ensures the integrity of the data. The specific decryption accuracy is as follows Formulas 1, 2, 6, 7, and 8 can verify Formula 9:

$$\begin{aligned} m_i &= C' \, mod\, p \\ &= f \cdot \sum_{j=1}^{n} \left(hs_{ij} + pe_{ij} + m_{ij} + y_{ij}\right) mod\, p \\ &= \sum_{j=1}^{n} \left(f \cdot \frac{pg'}{f} s_{ij} + f \cdot pe_{ij} + f \cdot m_{ij} + y_{ij} \right) mod\, p \\ &= \sum_{j=1}^{m} m_{ij} \end{aligned} \tag{9}$$

6.3 Confidentiality of power data

In this section, we provide a solution that ensures the confidentiality of power data.

1) Lemma 2 Assuming n is a power of 2, such that $\Phi = x^n + 1$ is decomposed into n linear factor modulo prime numbers $q = \omega(1)$. set up $\varepsilon, \delta > 0, p \in \mathcal{R}_q^*, \sigma \ge 2n\sqrt{\ln(8nq)} \cdot q^{1/2+\varepsilon}$. If there is an IND-CPA attack against the NTRU encryption algorithm, it runs within time T and has a success probability of $1/2 + \delta$. Then there exists a solution with parameters q and α $R - LWE_{HNF}^*$ algorithm, which runs within time $T' = T + O(n)$ and has a success probability of $\delta' = \delta - q^{-\Omega(n)}$ (Zhao et al., 2022).

Proof: Assuming $\mathcal{A}'$ defines an IND-CPA attack algorithm. We constructed a $\mathcal{B}'$ for algorithm $R - LWE_{HNF}^*$ It runs as follows, given from $U(\mathcal{R}_q^* \times \mathcal{R})$ or $A_{s,\psi}^*$ for some previously selected $s \leftarrow \psi, \psi \leftarrow \bar{\gamma}_\alpha$ to sampling of oracle machine $\mathcal{O}$. Algorithm $\mathcal{B}'$ first calls $\mathcal{O}$ from $\mathcal{R}_q^* \times \mathcal{R}$ obtains a sample (h', C'). Then, algorithm $\mathcal{B}'$ uses the public key $h = p \cdot h' \in \mathbb{R}_q$ runs $\mathcal{A}'$. When $\mathcal{A}'$ outputs a challenge message M_0, M_1, algorithm $\mathcal{B}'$ selects $b \leftarrow U(\{0, 1\})$ and calculates the challenge ciphertext $C = p \cdot C' + \text{M}_b \in \mathbb{R}_q$. And return C to $\mathcal{A}'$. Finally, when $\mathcal{A}'$ outputs its guess of b', if $b' = b$, then algorithm $\mathcal{B}'$ outputs 1, otherwise it outputs 0.

Due to the reversibility of $p \, mod\, q$, the h' used by $\mathcal{B}'$ in $\mathcal{R}_q^*$ is uniformly random, so the public key h given to $\mathcal{A}'$ is also uniformly random. Therefore, according to Theorem 3 (Wei et al., 2020), the private key given to $\mathcal{A}'$ is within the Statistical distance $q^{-\Omega(n)}$ of the public key distribution in the real attack. In addition, the ciphertext C given to $\mathcal{A}'$ by $C = h \cdot s + e$ has the same correct distribution as in IND-CPA attacks. Overall, if $\mathcal{O}$ output the sample from $A_{s,\psi}^*$, the probability of $\mathcal{A}'$ succeeding and $\mathcal{B}'$ returning 1 is greater than or equal the $1/2 + \delta - q^{-\Omega(n)}$.

2) Resist internal attacks: In our solution, we can resist internal attacks. Assuming Agg_i want to obtain electricity data for individual users, Agg_i need to decrypt the private key of the ciphertext because the message power data is encrypted through the public key, and the private key is only known by CC, so Agg_i cannot obtain clear text of power data. Assuming CC wants to obtain user personal data, this cannot be achieved because encrypted data is stored in Agg_i after aggregation, CC can only obtain multiple user data after aggregation, and cannot obtain detailed personal data from the aggregated data.
3) Resisting Collusion Attacks: Assuming Agg_i colluded with CC to launch a collusive attack, which cannot be achieved because we added y_{ij} only known for SM_{ij} when encrypting ciphertext,

TABLE 3 Safety and function comparison.

Schemes	A	C	I	B	P
Abdallah's scheme (Hu et al., 2023)	N	Y	Y	N	Y
Hafiz's scheme (Verma et al., 2023)	Y	Y	N	N	Y
Sui's scheme (Li et al., 2015)	Y	Y	Y	Y	Y
Ours scheme	Y	Y	Y	Y	Y

if CC gives the decryption private key to Agg_i is used to decrypt individual data, because of the random number y_{ij}, Agg_i unable to decrypt individual data; If Agg_i sends individual user data to CC, CC is also unable to decrypt individual data, as cannot be known y_{ij}. Because $\sum_{i=1}^{n} y_{ij} = 0$, so only after aggregating all ciphertext can decryption be performed.

6.4 Privacy protection of user identity

Our scheme can protect the identity privacy of users. During the initialization phase, we used TA to authenticate the participating entities. Only authenticated entities can broadcast public keys, and only those that sign with private keys can be verified. Our solution does not involve user identity information during data transmission, thus ensuring the privacy of user identity.

6.5 Comparisons

We conducted a comparison of security and functionality with other relevant schemes. Certification is used to ensure that all participating entities are legal, represented by A. Confidentiality represents that data transmission is not accessible to other unauthorized participants, represented by C. Integrity refers to ensuring that information or data is not unauthorized tampered with during transmission or storage, or can be promptly detected after tampering, represented by I. Batch verification is represented by B and can improve the efficiency in identity verification process and reduce computational costs. Privacy protection is represented by P, indicating whether the proposed scheme implements data privacy protection. Y and N represent implementation and non-implementation, respectively. Details are shown in Table 3.

7 Performance analysis

In this section, we analyzed the performance of the proposed scheme, mainly including computational cost and communication overhead. We compared it with recent privacy protection schemes to highlight the efficiency of our scheme. The experiment was conducted on an Intel (R) Core (TM) i5-10210U CPU @ 2.10 GHz 8.00 GB RAM laptop.

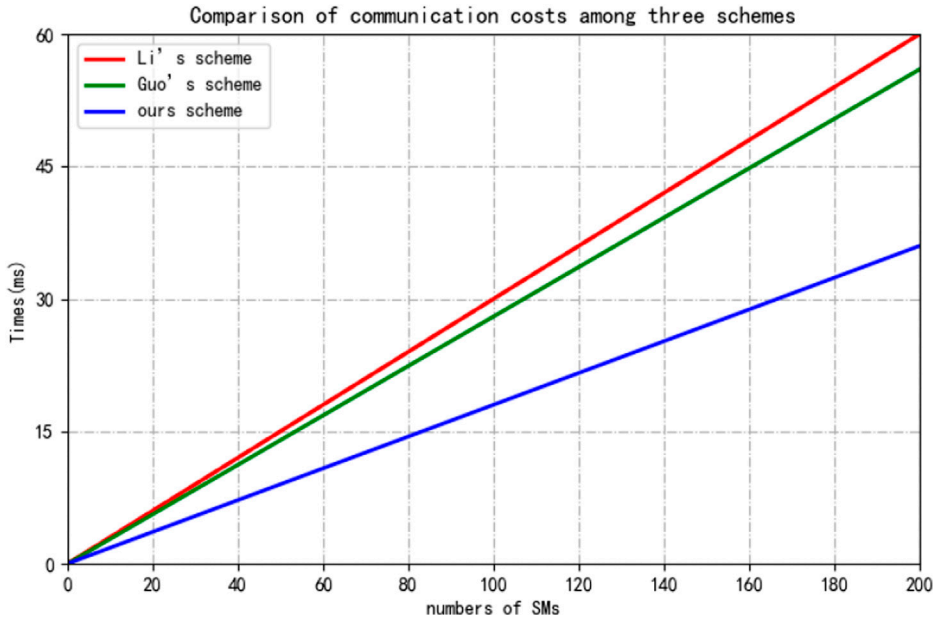


FIGURE 2
Comparison of communication costs with other solutions.

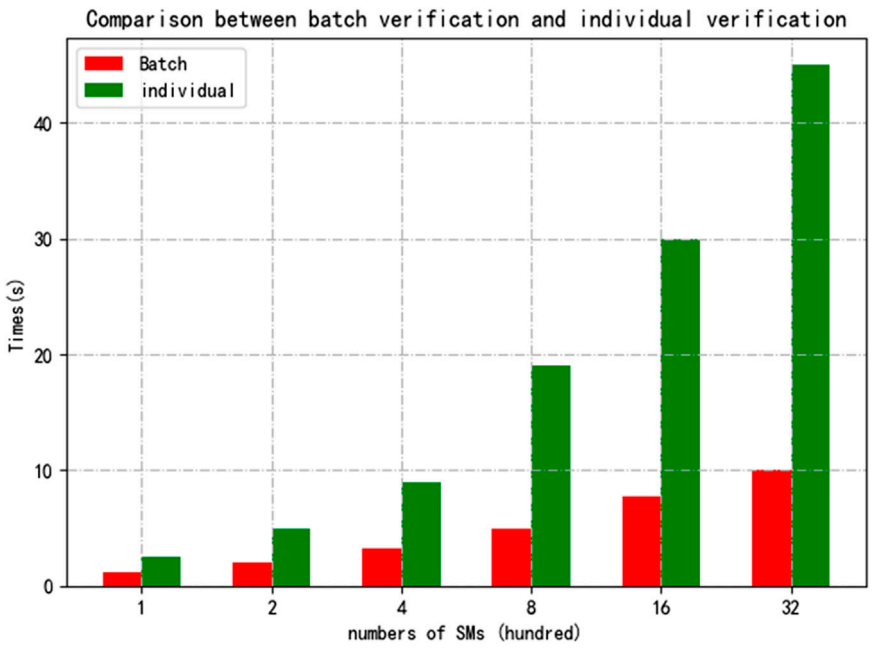


FIGURE 3
Comparison between batch validation and individual validation.

TABLE 4 Calculated costs for our plan and other plans.

Schemes	Computation cost
Li's scheme (Nyangaresi, 2022)	$2G_m + 2c_e + G_p + 3c_s$
Guo's scheme (Abdallah and Shen, 2018)	$3G_m + 9c_e + c_x + 3c_s$
Ours	$3c_m + 2c_e + 2G_p + 2c_s$

7.1 Communication overhead

We conducted a study on the performance of communication overhead in this section. In Li's scheme, $\mathbb{G}$ with a 160-bit order is selected and the point compression technique is used. The elements in $\mathbb{G}$ are approximate 161 bits. AES ciphertext with a 256-bit is chosen, and C_{ij} should be generated based on the 256-bit block encryption. Therefore, the total communication overhead can be calculated as (161* min (l_{ij} m_{ij})+80)/256 * 256 + 80 + 336) bits. In Guo's scheme, when a smart meter sends a usage report to both the demand response management unit and the consumer, it analyzes the consumer's desire to follow the instructions of the demand response management unit and provides proof of confirmation. The size of the report is 8| $\mathbb{G}$ |+3| Z_q^* |+|ID|+|t|, with a length of 1768 bits, excluding identity and timestamp. In comparison, In our scheme, the authentication phase does not need to occur every time data is reported. Only when new entities join or exit, the added entities are authenticated. Therefore, we do not consider the cost of the authentication phase, but only consider the communication and sales during the data reporting and decryption phases. Specifically, SM_{ij} Send $\{C_{ij}, \sigma_{ij}, T_v\}$ To Agg_i. Agg_i Send $\{C_i, \sigma_i, T_v\}$ to CC, the size of the ciphertext and signature are consistent with the timestamp size. We set the ciphertext length to 530bit, the signature size to 1024bit, and the timestamp size can be ignored, Therefore, the total size is 1554bit. We compared it with other schemes, as shown in Figure 2. Compared with the other two schemes, our scheme has lower communication overhead and can achieve efficient information transmission with the same number of electricity meters.

7.2 Calculate costs

In our scheme, the NTRU lattice scheme is used to encrypt plaintext. The encryption operation involves addition and multiplication, and the computational cost is relatively small compared to other encryption schemes. In terms of signature verification, we have implemented batch signature verification operations, which can reduce the computational cost. In Figure 3, we compared the computational cost of batch verification with that of individual verification. The results show that under the same number of signatures, The computational cost of batch validation is approximately half that of individual validation. We provide the calculation costs of our scheme and other schemes in Table 4, and conduct experimental comparisons in Figure 4. We use c_s represents the calculation cost of the hash function, using c_x represents XOR calculation cost, c_e represents the computational cost of the power operation, c_m represents the computational cost of multiplication, G_p and G_m represents the computational cost of pairing operations and multiplication operations in G. The calculation cost of our plan is $3c_m + 2c_e + 2G_p + 2c_s$. Li et al. calculated the cost as $2G_m + 2c_e + G_p + 3c_s$. The computational cost of Guo et al.'s (Abdallah and Shen, 2018) scheme is $3G_m + 9c_e + c_x + 3c_s$. Since Li (Nyangaresi, 2022) and others use homomorphic

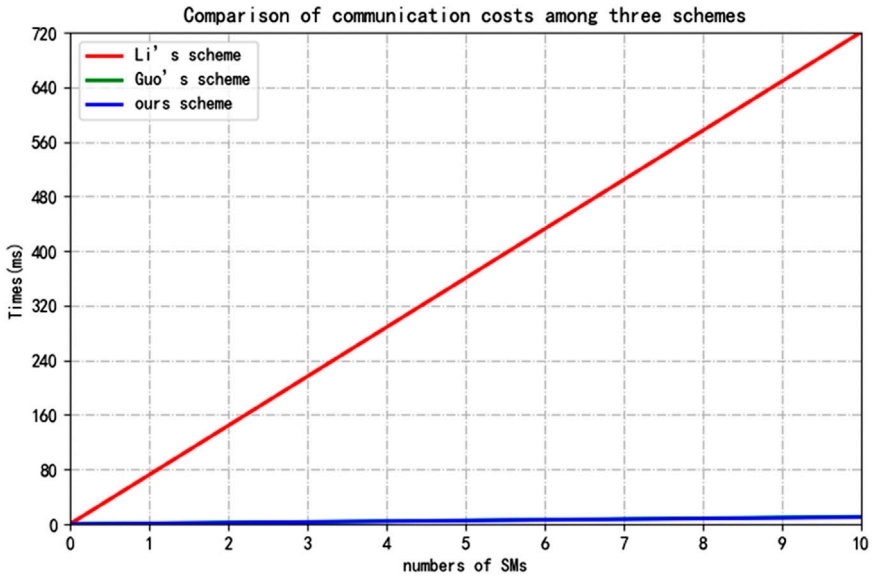


FIGURE 4
Comparison of calculated costs between our scheme and other schemes.

encryption based on Paillier, which relatively increases the computing cost, the experimental results show that our scheme has low computing cost and can achieve efficient operation.

In the proposed solution, a trusted center is included, assuming that it is a trusted third party. However, in real life, it is difficult to find an absolutely trustworthy third party to implement our solution, which is one of the limitations of the proposed solution. Other solutions that involve a third-party trust agency also face similar problems. At the same time, although our solution is lightweight, there must be a more efficient solution available. Therefore, establishing a solution without a trusted third party and improving efficiency is the direction of our next research.

8 Conclusion

Privacy protection is one of the obstacles to the rapid development of smart grids. Only by solving the privacy issues of the participating entities involved in smart grids can the collected granular data be efficiently used to make the grid intelligent. Considering the massive information collection in smart grids and the limitations of edge devices, an efficient privacy protection solution is needed. In this paper, we propose an efficient and batch-verified privacy protection scheme for smart grids. This scheme uses homomorphic encryption technology to achieve effective aggregation of user power data. During the transmission of power data, legitimate users sign the messages, ensuring confidentiality, integrity, and availability of the data. To improve efficiency, we have proposed a method for batch verification, reducing computational cost and communication overhead, in order to protect user privacy. Security analysis shows that our scheme is resistant to external attacks, internal attacks, and collusion attacks. Performance analysis shows that our scheme enables efficient data aggregation and is applicable to edge devices in smart grids. In summary, the proposed new privacy protection scheme enhances efficiency and can withstand malicious attacks such as tampering, forgery, and theft, thereby improving the privacy security of smart grids.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Materials, further inquiries can be directed to the corresponding author.

Author contributions

MW: Methodology, Validation, Writing–original draft. LZ: Funding acquisition, Writing–review and editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. The work of LZ was supported by Natural Science Foundation of Heilongjiang Province of China (LH2020F041), and the research start-up funds of Guangdong Polytechnic Normal University (Grant No. 991682313).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abdallah, A., and Shen, X. S. (2018). A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. *IEEE Trans. Smart Grid* 9 (1), 396–405. doi:10.1109/tsg.2016.2553647

Abdallah, A. R., and Shen, X. S. (2014). "A lightweight lattice-based security and privacy-preserving scheme for smart grid," in Global Communications Conference, Austin, Texas, 8-12 December, 2014 (IEEE).

Baghestani, S. H., Moazami, F., and Tahavori, M. (2022). Lightweight authenticated key agreement for smart metering in smart grid. *IEEE Syst. J.* 16 (3), 4983–4991. doi:10.1109/jsyst.2022.3188759

Cao, Y.-N., Wang, Y., Ding, Y., Guo, Z., Wu, Q., and Liang, H. (2023). Blockchain-empowered security and privacy protection technologies for smart grid. *Comput. Stand. Interfaces* 85, 103708. doi:10.1016/j.csi.2022.103708

Deng, L., Wang, T., Feng, S., Qu, Y., and Li, S. (2023). Secure identity-based designated verifier anonymous aggregate signature scheme suitable for smart grids. *IEEE Internet Things J.* 10 (1), 57–65. doi:10.1109/jiot.2022.3199480

Fan, C. I., Huang, S. Y., and Lai, Y. L. (2013). Privacy-enhanced data aggregation scheme against internal attackers in smart grid. *IEEE Trans. Industrial Inf.* 10 (1), 666–675. doi:10.1109/tii.2013.2277938

Fan, W. A., Xiong, L., Lx, D., and Kumari, S. (2020). A privacy-preserving scheme with identity traceable property for smart grid. *Comput. Commun.* 157, 38–44. doi:10.1016/j.comcom.2020.03.047

Gong, X., Hua, Q. S., Qian, L., Yu, D., and Jin, H. (2018). "Communication-efficient and privacy-preserving data aggregation without trusted authority," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications, Honolulu, Hawaii, 16-19 April 2018 (IEEE).

Guo, C., Jiang, X., Choo, K. K. R., Tang, X., and Zhang, J. (2020). Lightweight privacy preserving data aggregation with batch verification for smart grid. *Future Gener. Comput. Syst.*, 112. doi:10.1016/j.future.2020.06.001

Guo, F., Susilo, W., and Mu, Yi (2018). *Introduction to security reduction*. Cham: Springer.

Hu, S., Chen, Y., Zheng, Y., Xing, B., Li, Y., Zhang, L., et al. (2023). Provably secure ECC-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid. *IEEE Trans. Industrial Inf.* 19 (4), 5985–5994. doi:10.1109/tii.2022.3191319

Hua, S. A., Yl, A., Zhe, X. D., and Zhang, M. (2020). An efficient aggregation scheme resisting on malicious data mining attacks for smart grid. *Inf. Sci.* 526, 289–300. doi:10.1016/j.ins.2020.03.107

Li, C., Lu, R., Li, H., Chen, L., and Chen, J. (2015). PDA: a privacy-preserving dual-functional aggregation scheme for smart grid communications. *Secur. Commun. Netw.* 8 (15), 2494–2506. doi:10.1002/sec.1191

Li, H., Lin, X., Yang, H., Liang, X., Lu, R., and Shen, X. (2014). EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. *IEEE Trans. Parallel & Distributed Syst.* 25 (8), 2053–2064. doi:10.1109/tpds.2013.124

Mall, P., Amin, R., Das, A. K., Leung, M. T., and Choo, K.-K. R. (2022). PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: a comprehensive survey. *IEEE Internet Things J.* 9 (11), 8205–8228. doi:10.1109/jiot.2022.3142084

Nyangaresi, V. O. (2022). Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *J. Syst. Archit.* 133, 102763. doi:10.1016/j.sysarc.2022.102763

Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., and Li, J. (2020). Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Comput. Secur.* 97, 101958. doi:10.1016/j.cose.2020.101958

Qian, J., Cao, Z., Dong, X., Shen, J., Liu, Z., and Ye, Y. (2021). Two secure and efficient lightweight data aggregation schemes for smart grid. *IEEE Trans. Smart Grid* 12 (3), 2625–2637. doi:10.1109/tsg.2020.3044916

Roozbeh, S., Mahmoud, S., Ameri, M. H., and Aref, M. R. (2021). A secure and privacy-preserving protocol for holding double auctions in smart grid. *Inf. Sci. Int. J.* 557 (1), 108–129. doi:10.1016/j.ins.2020.12.038

Sadhukhan, D., Ray, S., Obaidat, M., and Dasgupta, M. (2022). A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *J. Syst. Archit.* 114, 2021. doi:10.1016/j.sysarc.2020.101938

Sanaullah Badar, H. M., Mahmood, K., Akram, W., Ghaffar, Z., Umar, M., and Das, A. K. (2022). Secure authentication protocol for home area network in smart grid-based smart cities. *Comput. Electr. Eng.* 108, 108721. doi:10.1016/j.compeleceng.2023.108721

Sani, A. S., Bertino, E., Yuan, D., Meng, K., and Dong, Z. Y. (2022). SPrivAD: a secure and privacy-preserving mutually dependent authentication and data access scheme for smart communities. *Comput. Secur.* 115, 102610. doi:10.1016/j.cose.2022.102610

Song, J., Liu, Y., Shao, J., and Tang, C. (2020). A dynamic membership data aggregation (DMDA) protocol for smart grid. *IEEE Syst. J.* 14 (1), 900–908. doi:10.1109/jsyst.2019.2912415

Stehlé, D., and Steinfeld, R. (2011). *Making NTRU as secure as worst-case problems over ideal lattices*. Cham: Springer-Verlag.

Sui, Z. Y., and Meer, H. D. (2020). BAP: a batch and auditable privacy preservation scheme for demand response in smart grids. *IEEE Trans. Industrial Inf.* 16 (2), 842–853. doi:10.1109/tii.2019.2926325

Verma, G. K., Gope, P., Saxena, N., and Kumar, N. (2023). CB-DA: lightweight and escrow-free certificate-based data aggregation for smart grid. *IEEE Trans. Dependable Secure Comput.* 20 (3), 2011–2024. doi:10.1109/tdsc.2022.3169952

Vincent, H., Bhaskar, B., and Caroline, F. (2018). Design and implementation of low-depth pairing-based homomorphic encryption scheme. *J. Cryptogr. Eng.*, 1–17. doi:10.1007/s13389-018-0192-y

Wei, K., Jian, S., Pv, C., Cho, Y., and Chang, V. (2020). A practical group blind signature scheme for privacy protection in smart grid. *J. Parallel Distributed Comput.* 136, 29–39. doi:10.1016/j.jpdc.2019.09.016

Zhang, J., and Dong, C. (2023). Privacy-preserving data aggregation scheme against deletion and tampering attacks from aggregators. *J. King Saud Univ. - Comput. Inf. Sci.* 35 (4), 100–111. doi:10.1016/j.jksuci.2023.03.002

Zhang, W., Liu, S., Xia, Z., Han, J., and Gao, J. F. (2022b). Hydrophobic and porous carbon nanofiber membrane for high performance solar-driven interfacial evaporation with excellent salt resistance. *J. Inf. Secur. Appl.* 612, 66–75. May. doi:10.1016/j.jcis.2021.12.093

Zhang, W., Huang, C., Gu, D., Zhang, J., Xue, J., and Wang, H. (2022a). Privacy-preserving statistical analysis over multi-dimensional aggregated data in edge computing-based smart grid systems. *J. Syst. Archit.* 2022 (127), 127. doi:10.1016/j.sysarc.2022.102508

Zhao, P., Huang, Y., Gao, J., Xing, L., Wu, H., and Ma, H. (2022). Federated learning-based collaborative authentication protocol for shared data in social IoV. *IEEE Sensors J.* 22 (7), 7385–7398. doi:10.1109/jsen.2022.3153338