Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **7**, Number **4**, November **2022**

Smart Grid Aggregation Billing Scheme Based on Blockchain

Xiuqiang Chen

College of Computer Science and Mathematics
Fujian University of Technology
Fuzhou, Fujian, 350118, China
Hale_Chan@163.com

Feng Wang*

College of Computer Science and Mathematics
Fujian Provincial Key Laboratory of Big Data Mining and Applications
Fujian University of Technology
Fuzhou, Fujian, 350118, China
Fujian Provincial Key Laboratory of Network Security and Cryptology
Fujian Normal University
Fuzhou, Fujian, 350007, China
w.h.feng@163.com

Zhongming Huang

College of Computer Science and Mathematics
Fujian University of Technology
Fuzhou, Fujian, 350118, China
1875584288@qq.com

Yeh-Cheng Chen

Department of Computer Science
University of California
Davis, CA 001313, USA
ycch@ucdavis.edu

*Corresponding author: Feng Wang

Received July 13, 2022, revised August 21, 2022, accepted October 1, 2022.

Abstract. *With the large-scale deployment of smart meters, numerous real-time power consumption data should be interacted and calculated in smart grid. However, the data processing not only consume a large amount of computing resources, but also brings some security problems of interactive parties, such as users' privacy disclosure, etc. In order to solve these problems, we propose a smart grid aggregation billing scheme based on blockchain, which can perform aggregation billing without relying on trusted authority (TA). In our scheme, the smart meters use Paillier encryption algorithm to encrypt the power consumption data for privacy protecting, and use BLS short signature algorithm to sign the power consumption data for data integrity and non-repudiation, then sends them to the aggregation node (AN) selected through the blockchain's distributed consensus algorithm (i.e., Raft algorithm). AN aggregates the ciphertext data and calculates the electric charge, then sends them to electric service providers (ESP) and stores them in blockchain. The ESP obtains data, decrypts and obtains the total power consumption data of all users in a slot, the electricity charges of a user in a slot and the monthly electricity charges of a user. Especially, an electricity charges verification phase is introduced in our scheme to avoid malicious AN attack. Security analysis shows that our scheme not only achieves the characteristics of confidentiality, data integrity and non-repudiation, but also resist malicious AN attack. Performance evaluation shows that our scheme has better performance and lower computational overhead than existing schemes.*
Keywords: smart grid, blockchain, aggregation billing, encryption algorithm, Raft algorithm

1. **Introduction.** With the development of information technology and the increasingly complex power environment, the traditional power grid has been unable to meet the current social needs [1]. As a new power grid mechanism, smart grid integrates information technology, power grid infrastructure and control technology, which is the continuation and development of traditional power grid [2-3]. Although smart grid improves people's quality of life to some extent, it also brings many security risks. Generally, power companies usually calculate the electricity charge according to the amount of electricity consumed by the electrical equipment in the user's home. However, electricity modification may lead to changes in users charges [4]. Therefore, there must be no problem in the collection of electricity, which is related to the accuracy of electricity charge calculation, and it is also very important to protect the privacy and safety of users while collecting electricity.

In addition, electricity price [5] is also a major factor of determining how much electricity users charge. As we all know, electricity price is the most effective economic adjustment lever in the power market. The formulation of electricity price is the key to the reform and development of power industry. The rapid development of smart grid has brought great impact on the traditional fixed price mechanism. As one of the important means of power demand side management, time-of-use (TOU) electricity price is playing a more and more important role in the economic management of power industry all over the world. Using TOU electricity price can realize peak shaving and valley filling, peak shifting and valley leveling, slow down the power investment in the generation side, improve the reliability of power supplies, and reduce users' electricity charges [6]. At the same time, the time-of-use price also brings users the correct problem of electricity charges.

Blockchain, as a distributed public account, records transactions in chronological order and is maintained by many distributed nodes through consensus protocols [7]. Unlike existing centralized systems, all nodes in the blockchain are peering nodes, jointly responsible for maintaining the entire network and building a decentralized environment [8]. Therefore, the dispersion of blockchain can greatly improve the safety performance of the whole system. In addition, all transactions in the blockchain are public and distributed,

and each node stores all transactions in the blockchain. Blocks of blockchain are linked to sequence in list structure to ensure that users can track transactions in blockchain [9]. Since the block is linked by a list structure, the block header of each block contains the hash address of the previous block, and the hash address of each block is based on the block content. If the adversary tries to modify the content of the block, the attacker will pay a huge price. Therefore, blockchain has been widely used on the Internet of Things (IoT) [7,10], smart grid [20-21] and other fields in recent years.

Data aggregation technology [11] can save computing resources and allow power companies to collect aggregated data instead of single data. Therefore, this technology can well protect the privacy of users without affecting the analysis of data and the adjustment of power supplies. Although there have been many researches on the privacy protection for smart grid data aggregation, there are still some problems to be solved. In most smart grid data aggregation schemes, a trusted third party usually acts as the aggregator or gateway, and the encryption algorithm and signature algorithm are used together to process the power consumption data collected by smart meters. In order to prevent malicious aggregators or gateways, various privacy preserving data aggregation schemes is proposed. As the power consumption data involves the user's energy use patterns, which are closely related to the user's personal life, improper handling of these data may lead to users privacy disclosure.

Although some schemes [12-21] solved the corresponding problems of data aggregation in varying degrees, there are still some shortcomings. First, the PBFT algorithm of scheme [19-20] has the problems of high communication complexity and low scalability, so it is necessary to find a better consensus algorithm to solve the above problems. Second, although scheme [21] proposes an improved Paillier encryption algorithm, it still retains the additive homomorphism of the original algorithm. Therefore, we propose a smart grid aggregation billing scheme based on blockchain. Our contributions are mainly reflected on the following four aspects.

1. We propose a new attack method named malicious AN attack, the malicious AN can tamper with electricity without being detected. Then we propose a smart grid aggregation billing scheme based on blockchain, which can resist this attack.

2. We use a more efficient Raft algorithm [22] instead of PBFT algorithm, which reduces the computational overhead accordingly.

3. Our scheme supports secure aggregated billing based on blockchain and does not rely on trusted authority, ensuring the security of private data throughout the billing process, which is in line with the development trend of smart grid in the future.

4. Compared with existing schemes, our scheme has better security performance and computational overhead.

2. **Related work.** To solve the problems of user privacy protection and data validity verification in smart grid, most existing schemes often use the additive homomorphism of various encryption algorithms to aggregate user data, and only send the aggregation results in the power center, so as to hide the data of a single user [23].

Lu *et al.* [12] used a Paillier homomorphic encryption algorithm [24] to protect the privacy of multidimensional data, and adopted batch verification technology to reduce the authentication cost. Chen *et al.* [13] proposed a power data aggregation scheme based on Paillier encryption algorithm. The scheme uses a trusted authority to generate a key for the smart meter, and solves the problem of meter failure to a certain extent, but it can not completely solve the problem of privacy protection. Li *et al.* [14] proposed a privacy preserving multi subset data aggregation scheme based on Paillier, which not only meets the requirements of smart grid control center for data granularity, but also protects

users' privacy. Karampour *et al.* [15] used the Paillier encryption system and AV network mask in the smart grid to realize the aggregation of privacy protection data, which can effectively protect the privacy of user data without any secure channel. Chen *et al.* [16] proposed a data aggregation scheme for smart meters based on Paillier homomorphic cryptosystem. In their scheme, the smart meter can use one message to report various types of power consumption data, which is convenient for suppliers to perform variance analysis and one-way variance analysis on the data.

The above schemes are basically centralized, and there are safety risks such as single point of failure. Blockchain is the underlying technology of the digital cryptocurrency system represented by bitcoin [25]. It can implement trusted transactions in untrusted distributed systems through encryption algorithm, timestamp and distributed consensus. The coordination between nodes in the blockchain solves the common problems of high cost, low efficiency and unsafe data storage in centralized organizations [26]. At present, relevant studies[17-21] had applied blockchain technology to smart grid to meet the above challenges.

Chen *et al.* [17] integrated fog computing and blockchain, and developed a secure data aggregation scheme with low computing overhead by combining Paillier encryption, batch processing aggregation signature and anonymous authentication. However, their method does not give the method to select aggregation nodes. Fan *et al.* [18] proposed a distributed smart grid privacy protection data aggregation scheme based on blockchain. The scheme selects a mining node through the leader election algorithm and records the data of smart meters into the blockchain. BLS [27] signature and Paillier encryption are based on bilinear pairings to ensure the security and integrity of messages during transmission. Wang *et al.* [19] proposed a distributed electricity meter data aggregation framework based on blockchain and homomorphic encryption, in which the consensus mechanism is supported by the practical Byzantine fault tolerance (PBFT) algorithm. Luo *et al.* [20] using Paillier homomorphic encryption and PBFT algorithm, proposed a decentralized microgrid data aggregation scheme without any authorization center and anti-malicious aggregator, which realized user privacy protection, data integrity protection, public storage and sharing. Xue *et al.* [21] proposed a privacy protection service outsourcing scheme for smart grid real-time pricing demand response. In order to prevent the privacy disclosure of users, this scheme modifies the Paillier encryption algorithm to have two different decryption keys.

3. **Preliminaries.**

3.1. **Bilinear Pairing.**

Given two q-order prime cyclic groups G and G_T. $e : G \times G \to G_T$ is a bilinear mapping, if it has the following properties.

Bilinear. For all $u, v \in G$, $a, b \in Z_q^*$, there are $e(u^a, v^b) = e(u, v)^{ab}$.

Non-degeneracy. For all $u, v \in G$, $e(u, v) \neq 1$.

Computability. For all $u, v \in G$, there is an effective algorithm to calculate $e(u, v)$.

3.2. **Paillier Homomorphic Encryption.**

Homomorphic encryption is a classical cryptographic algorithm, which is constructed based on complex mathematical problems [20]. Using homomorphic encryption, we can obtain the aggregation results from the computation operations in the ciphertext domain without knowing the specific plaintext data. The specific steps of Paillier homomorphic encryption algorithm [24] is as follows.

Key generation. Select two random large primes p and q, where $\gcd(pq, (p-1)(q-1)) = 1$. Then calculate $N = pq$ and λ=lcm$(p-1, q-1)$. Next, select a generator $g \in Z_{N^2}^*$ to calculate $\mu = (L(g^\lambda \bmod N^2))^{-1}$, where $L(u) = \frac{u-1}{N}$. We can get public key $PK = (N, g)$ and private key $SK = (\lambda, \mu)$.

Encryption. Encrypt the message $d \in Z_N$, select a random number $r \in Z_N^*$, and then calculate the ciphertext $C = E(d) = g^d r^N \bmod N^2$.

Decryption. Decrypt ciphertext $C \in Z_{N^2}^*$ and calculate $m = D(C) = L(C^{\lambda \bmod N^2}) \cdot \mu \bmod N$.

Additive homomorphism. For any d_1,d_2, the following formula(1),(2),(3) holds.

$$D(E(d_1)E(d_2) \bmod N^2) \equiv d_1 + d_2 \bmod N \tag{1}$$

$$D(E(d_1)^{d_2}) \bmod N^2) \equiv d_1 \cdot d_2 \bmod N \tag{2}$$

$$D(E(d_1)g^{d_2}) \bmod N^2) \equiv d_1 + d_2 \bmod N \tag{3}$$

3.3. **Boneh-Lynn-Shacham Short Signature.** Boneh-Lynn-Shacham (BLS) [27] is a short signature scheme based on bilinear pairing. It selects a hash function H_1: $\{0,1\}^* \to G$, a bilinear pair $e : G \times G \to G_T$, and g is a random generator of G. The BLS signature scheme includes three stages : key generation, signature and verification.

Key generation. The secret key $x \in Z_q^*$, and compute the public key $pk = x \cdot g$.

Signature. The plaintext $d \in G$, compute the signature $\sigma = x \cdot H(d)$.

Verification. If $e(\sigma, g) = e(H(d), pk)$, then the signature is valid. Otherwise invalid.

4. **Malicious AN attack on Xue *et al.*'s Scheme.** Xue *et al.* proposed a privacy protection serviced outsourcing scheme for smart grid real-time pricing (RTP) demanded response (DR) [21]. The scheme divides customers into two types: traditional customers and DR customers. Traditional customers participate in traditional data aggregation. DR customers participate in RTP DR program and are responsible for dynamic pricing strategy. In addition, the DR program has time slots and assumes that a billing period contains T time slots. The price at each time slot is fixed, but the price at different times is usually different [21]. In order to peak-cutting and valley-filling, the TOU price strategy is proposed, which makes the malicious gateway or aggregator have an opportunity. In order to reduce their own electricity charges, dishonest users will lure the gateway or aggregator, making the gateway or aggregator used the time-of-use price strategy and the homomorphism of Paillier encryption algorithm to modify the power consumption data.

For Paillier encryption algorithm, there are many related researches [12,14,20] proposed using its additive homomorphism (i.e., formula (1)) for data aggregation. In addition, some related studies [21] proposed to use its additive homomorphism (i.e., formula (2)) to aggregate billing. But we haven't found any researchers suggesting that gateways or aggregators might exploit their additive homomorphism (i.e., formula (3)) for the following attack.

In Xue *et al.*'s [21] scheme, we assume that there are two DR customers U_α and U_β in RTP DR program. During peak periods (i.e., time slot t), the gateway may reduce electricity consumption b for U_α by formula (4) and increase electricity b for U_β by formula (5). Similarly, during trough periods (i.e., time slot t'), the gateway increases electricity b for U_α through formula (6), and reduces electricity a for U_β through formula (7).

$$D(E(d_{\alpha,t}) \cdot g^{-b}) \bmod N^2) \equiv d_{\alpha,t} - b \bmod N \tag{4}$$

$$D(E(d_{\beta,t}) \cdot g^{b}) \bmod N^2) \equiv d_{\beta,t} + b \bmod N \tag{5}$$

$$D(E(d_{\alpha,t'}) \cdot g^{b}) \bmod N^2) \equiv d_{\alpha,t'} + b \bmod N \tag{6}$$

$$D(E(d_{\beta,t'}) \cdot g^{-a}) \bmod N^2) \equiv d_{\beta,t'} - b \bmod N \tag{7}$$

Based on the above operation, we can know that customer U_α in the peak periods of electricity reduced b, and the trough periods of electricity increased b, and customer U_β is the opposite. Especially, due to time-of-use electricity prices, this means that total monthly electricity of U_α and U_β is constant, and their monthly electricity charges have changed. We call this attack as malicious AN attack. In order to prevent the above problems, we propose a smart grid aggregation billing scheme based on blockchain. In our scheme, we introduce the electricity charge verification process, so that our scheme can resit malicious AN attack.

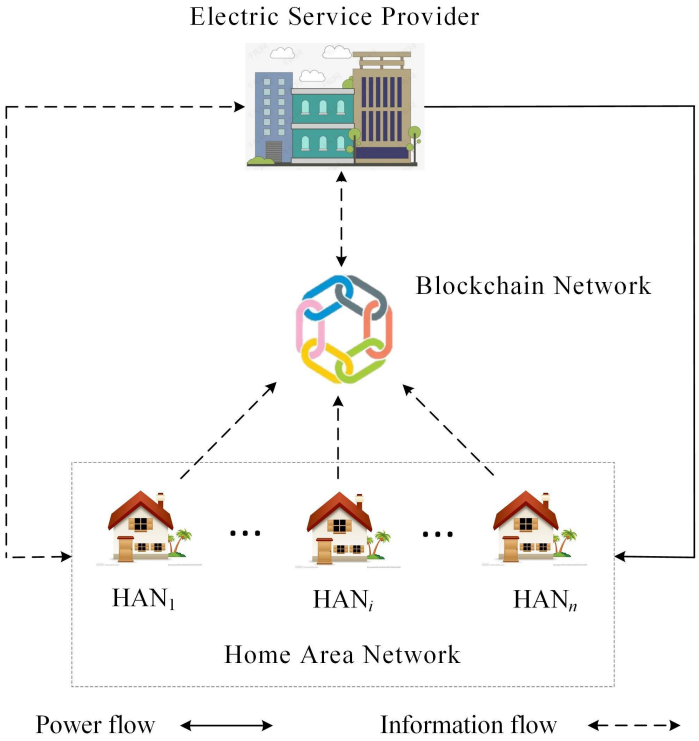

FIGURE 1. System model

5. Problem Formalization.

5.1. **System Model.** The system model of our scheme is shown in FIGURE 1. It mainly includes three entities: electric service provider (ESP), blockchain network and home area network (HAN). The specific description of each entity is as follows.

ESP. ESP is completely credible. It is responsible for starting the whole system, participating in the operation and key distribution of the system initialization phase, and providing registration services for other entities. It has certain data analysis and computing power. It can perform billing, power consumption trend analysis and dynamic pricing.

Blockchain Network. As shown in FIGURE 2, the blockchain network is mainly composed of m aggregators (AG). Each AG is equivalent to a blockchain node (BN). BN is responsible for collecting the power consumption data of n HAN in the community. Considering that a BN may be hijacked by an adversary, resulting in a single point of failure, security and other problems, the raft consensus algorithm elects AN from m BN

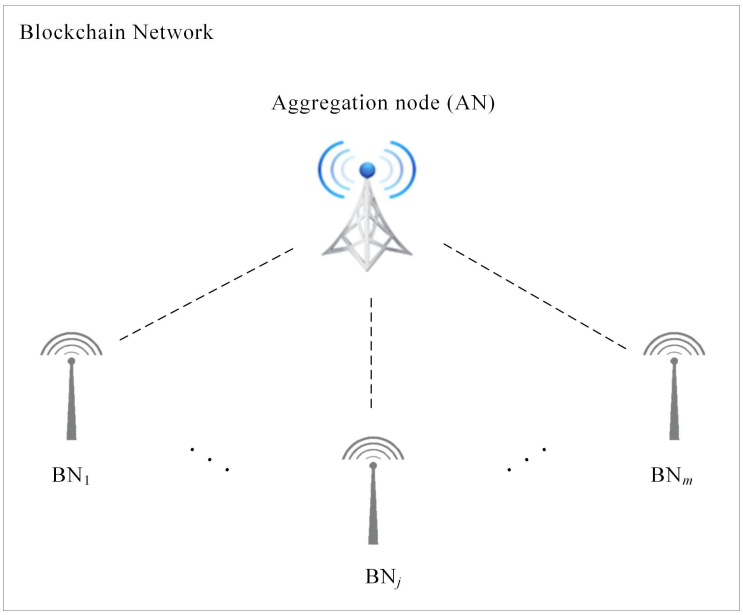

FIGURE 2. Blockchain network

to complete the block packaging work and periodically aggregate the encrypted power data uploaded by smart meters. However, AN elected by the Raft consensus algorithm is not entirely credible, so it may carry out some illegal operations for attractive interests. For example, AN may modify the power consumption data of HAN, making some or all HAN electricity charges change.

HAN. Each HAN is composed of a smart meter (SM) and a set of household appliances (HA). SM collects and uploads power consumption data of HA regularly. Most HAN is considered honest but curious. They operate according to the protocol and do not initiate active attacks.

5.2. **Design Goal.** Specifically, our scheme should meet the following security demands.

Confidentiality. Any untrusted and unauthorized entity cannot know the user's power consumption data and electricity charge information, i.e., if the external personnel or malicious participants obtain encrypted messages, they cannot recognize the original data.

Data integrity and non-repudiation. Our scheme adopts BLS signature and the blockchain technology to ensure data integrity and non-repudiation.

Resist malicious AN attack. Malicious AN attacked means that malicious AN uses the additive homomorphism of Paillier encryption algorithm to modify the power consumption data of HAN for some purpose. Our scheme can effectively resist this attack mentioned in Section 4.

6. **The Proposed Scheme.** In this part, we introduce the operation mechanism of the smart grid aggregation billing scheme based on blockchain in detail. The scheme consists of six phases, including system initialization, entity registration, user report generation, blockchain network data processing, ESP data analysis and electricity charge verification. The notations are listed in TABLE 1.

6.1. **System Initialization.** The system initialization process mainly includes the following four steps.

Step 1: ESP constructs bilinear mappin $e : G \times G \to G_T$, where G and G_T are two cyclic groups of order q, and g_1 is the generator of G.

TABLE 1. Symbols in the proposed scheme

Symbol	Description
g_1, g_2	A generator of G
n	Number of smart meters in a area
H_1	Hash functions: H_1:{0,1}$^* \rightarrow G$
HAN_i	The ith home area network in a area
SM_i	Smart meter in ith home area network
d_i	Power consumption data of smart meter SM_i
L	Any number of HAN in a area
x_i, pk_i, σ_i	Private key, public key, and signature of SM_i
x_j, pk_j, σ_j	Private key, public key, and signature of AG_j
$C_{i,\gamma}$	Ciphertext of SM_i in γ time slots
C_γ	Aggregated ciphertext in γ time slots
$Cha_{i,\gamma}$	Electricity charge ciphertext of HAN_i in γ time slots
Cha_i	Monthly electricity charge ciphertext of HAN_i
$\|\|$	Concatenation operation

Step 2: ESP generates Paillier cryptosystem public key (N, g_2) and private key (λ, μ), where $g_2 \in Z^*_{N^2}$.

Step 3: ESP selects a hash function H_1, where $H_1 : \{0,1\}^* \rightarrow G$.

Step 4: ESP publishes the system public parameters {q,g_1,g_2,G,G_T,e,N,H_1,}.

6.2. **Entity Registration.** Entity registration phase mainly includes HAN registration and aggregator (or blockchain node) registration.

HAN registration. $\text{HAN}_i(1 \leq i \leq n)$ selects a random number $x_i \in Z^*_q$ as its private key, and calculates the corresponding public key $pk_i = x_i \cdot g_1$. In addition, ESP generates smart meter SM_i with ID_i for HAN_i. After successful registration, ESP will install SM_i in HAN_i within the specified time to collect power consumption data of HA in HAN_i.

AG (or BN) registration. Similarly, $\text{AG}_j(1 \leq j \leq m)$ selects a random number $x_j \in Z^*_q$ as the private key and calculates the corresponding public key $pk_j = x_j \cdot g_1$.

6.3. **User Report Generation.** For simplicity, we let SM collect power consumption data every 60 minutes, so there are $z = 24\omega$ (where ω is the number of days, $\omega \in [28, 29, 30, 31]$) time slots in a billing period (for example, one month), such as, T_1,..., T_γ ,..., T_z. Specifically, SM_i in $\text{HAN}_i(1 \leq i \leq n)$ collects power consumption data $d_{i,\gamma}$ in T_γ and performs the following steps.

Step 1: SM_i selects a random number $r_i \in Z^*_N$ and calculates electricity ciphertext $C_{i,\gamma}$ of SM_i at T_γ according to formula (8).

$$C_{i,\gamma} = E(d_{i,\gamma}) = g_2^{d_{i,\gamma}} r_i^N \bmod N^2 \tag{8}$$

Step 2: SM_i calculates the signature $\sigma_i = x_i \cdot H_1(C_{i,\gamma} \parallel T_i \parallel ID_i)$, where T_i is the current timestamp, which is used to resist replay attacks. ID_i is the identity of SM_i, which is anonymous to entities other than SM_i.

Step 3: SM_i generates a packet $P_i = C_{i,\gamma} \parallel T_i \parallel ID_i \parallel \sigma_i$ and sends it to BN_j (i.e., aggregator AG_j).

6.4. **Blockchain Network Data Processing.** After receiving packet P_i from SM_i, BN_j checks the validity of timestamp T_i and identity ID of packet P_i. After validation, BN_j broadcasts P_i to the blockchain network and is stored in the local memory pool by other blockchain nodes. Finally, the blockchain network temporarily selects an aggregation node through the Raft consensus algorithm. On the one hand, AN verified the batch signature of the packet, encapsulates it into blocks, and broadcasts it to the blockchain network for other blockchain nodes to add it to the blockchain classification account of the region. On the other hand, AN aggregate data and aggregate billing. The specific process is as follows.

Batch signature verification. AN performs batch signature verification for packet P_i from SM_i via formula (9).

$$e(\textstyle\sum_{i=1}^{n}\sigma_i, g_1) = \prod_{i=1}^{n} e(H_1(C_{i,\gamma} \parallel T_i \parallel ID_i), pk_i) \tag{9}$$

In the following equation, the correctness of the signature scheme is proved.

$$\begin{aligned} e(\textstyle\sum_{i=1}^{n}\sigma_i, g_1) &= e(\textstyle\sum_{i=1}^{n} x_i \cdot H_1(C_{i,\gamma} \parallel T_i \parallel ID_i), g_1) \\ &= \textstyle\prod_{i=1}^{n} e(x_i \cdot H_1(C_{i,\gamma} \parallel T_i \parallel ID_i), g_1) \\ &= \textstyle\prod_{i=1}^{n} e(H_1(C_{i,\gamma} \parallel T_i \parallel ID_i), x_i \cdot g_1) \\ &= \textstyle\prod_{i=1}^{n} e(H_1(C_{i,\gamma} \parallel T_i \parallel ID_i), pk_i) \end{aligned} \tag{10}$$

Block generation. The data packet P_i with successful signature verification will be packaged into blocks, and then broadcast to the blockchain network. Finally, each blockchain node link the newly generated blocks of the local blockchain ledger to maintain a consistent ledger.

Because AN selected by Raft algorithm has high credibility, it can act as aggregator temporarily. AN can perform data aggregation and aggregation billing operations on data that have been verified by signature without decrypting power consumption data.

Data aggregation. After the signature verification is passed, according to the additive homomorphism of Paillier encryption algorithm, AN aggregates the encrypted electricity data $C_{i,\gamma}$ in the new block according to formula (11) for ESP to be used in power dispatching and price forecasting. Since this paper mainly considers the protection for user privacy and aggregation billing, if readers are interested in power dispatching and price forecasting, references [19-20] can be used.

$$C_\gamma = \textstyle\prod_{i=1}^{n} C_{i,\gamma} \bmod N^2 \tag{11}$$

Aggregate billing. According to the current electricity price standard, the electricity price of different time is different [28]. According to ESP requirements, AN carries out aggregate billing for ciphertext $C_{i,\gamma}$ of power consumption data, the specific steps are as follows.

Step 1: AN obtains TOU price $p_\gamma \in \{p_h, p_n, p_l\}$ according to Algorithm 1 after receiving $C_{i,\gamma}$. The electric charge ciphertext $Cha_{i,\gamma}$ of SM_i at time slot $T_\gamma (1 \le \gamma \le z)$ is calculated by formula (12).

$$Cha_{i,\gamma} = C_{i,\gamma}^{p_\gamma} \bmod N^2 \tag{12}$$

Step 2: After receiving $z = 24\omega$ $Cha_{i,\gamma}$ (i.e., the end of a month), AN calculates the monthly electricity charge ciphertext Cha_i of SM_i according to formula (13).

Algorithm 1

Input : γ
Output : $p_\gamma \in \{p_h, p_n, p_l\}$
1: **if** $(7+24(\omega-1)) \leq \gamma < (11+24(\omega-1)) \cup (19+24(\omega-1)) \leq \gamma < (23+24(\omega-1))$ **then**
2: $p_\gamma = p_h$;
3: **else if** $(11+24(\omega-1)) \leq \gamma < (19+24(\omega-1))$ **then**
4: $p_\gamma = p_n$;
5: **else if** $(23+24(\omega-1)) \leq \gamma \leq (24+24(\omega-1)) \cup (1+24(\omega-1)) \leq \gamma < (7+24(\omega-1))$ **then**
6: $p_\gamma = p_h$;
7: **end if**
8: **return** $p_\gamma \in \{p_h, p_n, p_l\}$

$$Cha_i = \prod_{\gamma=1}^{z} (Cha_{i,\gamma}) \bmod N^2 = (Cha_{i,1} \cdot Cha_{i,2} \cdot \cdots \cdot Cha_{i,\gamma} \cdot \cdots \cdot Cha_{i,z}) \bmod N^2 \tag{13}$$

Step 3: AN uses its own private key x_j to sign the data according to the formula (14).

$$\sigma_j = x_j \cdot H_1(C_{i,\gamma} \| C_\gamma \| Cha_{i,\gamma} \| Cha_i \| T_j \| ID_j) \tag{14}$$

Step 4: AN generates packet $P_j = C_{i,\gamma} \parallel C_\gamma \parallel Cha_{i,\gamma} \parallel Cha_i \parallel T_j \parallel ID_j \parallel \sigma_j$ and copies it twice. One is stored in blockchain and the other is sent to ESP.

6.5. **ESP Data Analysis.** ESP receives the packet P_j sent by AN, first verifies the signature σ_j, and then uses the private key SK to decrypt the aggregate ciphertext M_γ of n HANs in the community at T_γ, the electricity charge $MT_{i,\gamma}$ of SM_i (that is, HAN_i) at T_γ and the total monthly electricity charge MT_i of SM_i.

$$M_\gamma = D(C_\gamma) = \frac{L(C_\gamma^\lambda \bmod N^2)}{L(g_2^\lambda \bmod N^2)} \bmod N = \sum_{i=1}^{n} m_{i,\gamma} \tag{15}$$

$$MT_{i,\gamma} = D(Cha_{i,\gamma}) = \frac{L(Cha_{i,\gamma}^\lambda \bmod N^2)}{L(g_2^\lambda \bmod N^2)} \bmod N = m_{i,\gamma} \cdot p_\gamma \tag{16}$$

$$MT_i = D(Cha_i) = \frac{L(Cha_i^\lambda \bmod N^2)}{L(g_2^\lambda \bmod N^2)} \bmod N = \sum_{\gamma=1}^{z} (m_{i,\gamma} \cdot p_\gamma) \tag{17}$$

6.6. **Electricity Charge Verification.** Malicious AN may modify power consumption data according to the method proposed in section 4 before aggregation billing. Therefore, anyone (for example, HAN or ESP) can obtain data from the blockchain for electricity charge verification. The specific operation is as follows.

Step 1: When anyone doubts about electricity charges, they will obtain the ciphertext $C_{k,\gamma}$ of $\mathrm{SM}_k (k \in L \subseteq [1, n])$ from the blockchain, and recalculate the monthly electricity charges ciphertext Cha'_k of SM_k according to formula (18).

$$Cha'_k = \prod_{\gamma=1}^{z} (C_{k,\gamma})^{p_\gamma} \bmod N^2 \tag{18}$$

Step 2: The verifier compares the monthly electricity charge ciphertext calculated by himself and AN by formula (19), where k may be multiple users.

$$\prod_{k \in L} Cha'_k \stackrel{?}{=} \prod_{k \in L} Cha_k \tag{19}$$

If established, we deem that AN does not modify the power consumption data of SM_k. Instead, ESP will hold AN accountable and re-decrypt Cha'_k to SM_k's total monthly electricity charge.

7. **Security Analysis.** In this part, we give a detailed security analysis for the design goals proposed in Section 5.2. We mainly focus on confidentiality, data integrity and non-repudiation, and resist malicious AN attack.

Confidentiality. In our scheme, the SMs use the public key $PK = (n, g)$ published by ESP to encrypt power consumption data, and the AN uses the additive homomorphism of Paillier encryption algorithm to process ciphertext data. Firstly, in user report generation phase, the power consumption data $d_{i,\gamma}$ collected by SM is encrypted into the standard Paillier cipher system ciphertext form to ensure that the power consumption information is not compromised. Secondly, in blockchain network data process phase, AN cannot recover plaintext information from the ciphertext without obtaining the private key $SK = (\lambda, \mu)$ of ESP, but can aggregate the ciphertext received, and the result is an effective Paillier cryptosystem ciphertext form. Therefore, even if AN is semi-trusted, the confidentiality of power consumption data uploaded by SM can still be guaranteed.

Data integrity and non-repudiation. In our scheme, both the power consumption data provided by SM and the aggregated ciphertext data aggregated by AN are signed by the BLS short signature algorithm. Considering that the BLS short signature algorithm is provably secure, it can not be forged in the adaptive selective plaintext attack under the random oracle model, and its security is based on the computational Diffie-Hellman [29-30] assumption. In this way, even if the adversary can tamper with the message, the signature verification program can not get the correct result, so the tampered data is considered invalid, and the data integrity and non-repudiation are guaranteed. In addition, once the data is stored on the blockchain, the characteristics of the blockchain can ensure the integrity and unforgeability of the data on the chain.

Resist malicious AN attack. In our scheme, the AN selected by Raft algorithm has high credibility, but it is not completely credible. A malicious AN may do the following for the benefit of the attack method proposed in Section 4.

During the peak periods, malicious AN may reduce the electricity b of SM_α according to formula (4), and increase the electricity b of SM_β according to formula (5), where $\alpha, \beta \in [1, n]$. Similarly, in the trough periods, malicious AN may increase the electricity b of SM_α according to formula (6), and reduce the electricity b of SM_β according to formula (7).

Through the above operation, the electricity of SM_α and SM_β in a billing period remains unchanged. However, due to TOU prices, electricity charges for SM_α and SM_β are variable in a billing period. In order to prevent malicious AN, anyone (e.g., HAN or ESP) can obtain the power consumption data ciphertext of $L \subseteq [1, n]$ HAN from the blockchain, and then verify the electricity bills by $\prod_{k \in L} Cha'_k \stackrel{?}{=} \prod_{k \in L} Cha_k$ to verify whether malicious AN tampers with power consumption data.

8. **Performance Evaluation.** In this part, we compare the proposed scheme with the existing scheme in terms of performance and computational overhead.

8.1. **Comparison of performance.** We compare our scheme with the existing schemes [14,20-21,31] in terms of confidentiality, aggregate billing, data integrity and non-repudiation, resists malicious AN attack and trusted authority. The comparison results are shown in TABLE 2.

TABLE 2. Performance comparison of different schemes

Comparison	[14]	[20]	[21]	[31]	Our
Confidentiality	yes	yes	yes	yes	yes
Aggregate billing	yes	-	yes	-	yes
Data integrity and non-repudiation	no	yes	no	yes	yes
Resist malicious AN attack	no	-	no	-	yes
Trusted authority	yes	no	no	no	no

Without trusted authority, our scheme uses Paillier encryption algorithm to protect data privacy, and uses its additive homomorphism to aggregate HAN's power consumption data ciphertext and calculate HAN's the electricity charge ciphertext. In addition, we also use BLS signature algorithm to ensure data integrity and non-repudiation. In scheme [14], the control center (CC) can perform fine-grained analysis, but scheme [14] relies on trusted authority. Once the trusted authority are attacked by external attacks, scheme [14] will disclose user privacy. Furthermore, scheme [14] cannot guarantee data integrity and non-repudiation. By contrast, our scheme can meet these security requirements. Schemes [20,31] do not consider the billing problem, so we consider that schemes [20,31] cannot resist malicious AN attacks proposed in this paper. At the end of scheme [14], however, a rough extension of scheme [14] to calculate electricity charges was made, but no detailed billing process was given. Although scheme [21] uses the improved Paillier encryption algorithm to aggregate the power consumption data, the scheme does not consider that the gateway may use the additive homomorphism of the Paillier encryption algorithm to modify the power consumption. In addition, scheme [21] does not use a signature algorithm, so the scheme cannot guarantee data integrity and non-repudiation. Finally, we propose a new attack (i.e., malicious AN attack) for scheme [21], and introduce an electricity charge verification process to resist this attack. Based on the above analysis, our scheme is more suitable for the practical application of smart grid.

8.2. **Computation overhead.** Compared with exponentiation operation and pairing operation, multiplication operation in $Z_{N^2}^*$, aggregation and hash operation can be ignored. In order to compare the computational overhead between our scheme and the existing schemes [12,16,20-21], we use the java pairing-based cryptography (JPBC) [32] library to obtain the computational time of cryptographic operations, as shown in TABLE 3, where N is 1024 bits and G is 160 bits. The experiment runs on a laptop with Intel Core i7-7700HQ (2.80GHz) processor, 8GB memory and 64-bit Window10 operating system. Here, we assume that there are n smart meters and m aggregators.

By comparison, we get the computation overhead for each entity of our scheme and existing schemes [12,
16,20-21], as shown in TABLE 4. For convenience, the GW of schemes [12,16], the aggregator of scheme [20] and the gateway and service provider of scheme [21] are denoted as AN, and the OA of scheme , the CC of scheme [16], the BK of scheme [20] and the power utility of scheme [21] are denoted as ESP. Since scheme [20] does not give a specific signature algorithm, it is assumed that they use the same signature algorithm as ours.

As shown in FIGURE 3, the computational cost of our scheme at the SM side is lower than that of scheme [16], which is equal to that of schemes [12,20], but slightly higher than that of scheme [21]. However, this is acceptable because no signature algorithm is used in scheme [21] to ensure the integrity and undeniableness of data. As shown in FIGURE

TABLE 3. Computational time of cryptographic operations

Symbol	Description	Times(ms)
T_p	Time of paring operation	6.85
T_m	Time of multiplication operation in G	0.88
T_e	Time of exponentiation operation in $Z^*_{N^2}$	9.45
TE_p	Time of Paillier encryption operation	5.33
TD_p	Time of Paillier dncryption operation	9.82

TABLE 4. Comparing computation overhead of different schemes

Scheme	[12]	[16]	[20]	[21]	Our
Overhead SM(ms)	$TE_p + T_m$	$TE_p + T_p$	$TE_p + T_m$	TE_p	$TE_p + T_m$
Overhead AN(ms)	$(n+1)T_p + T_m$	$(2n+1)T_p$	$m[(n+1)T_p + T_m]$	$2T_e$	$(n+1)T_p + T_m + T_e$
Overhead ESP(ms)	$2T_p + TD_p$	$T_p + TD_p$	$(m+1)T_p + TD_p$	TD_p	$(m+1)T_p + 3TD_p$

4, the computational cost of our scheme on the AN side is lower than that of scheme [16], which is basically the same as that of schemes [12,20], but slightly higher than that of scheme [21]. This is because our scheme aggregate billing, improve performance while the computational overhead will increase accordingly.

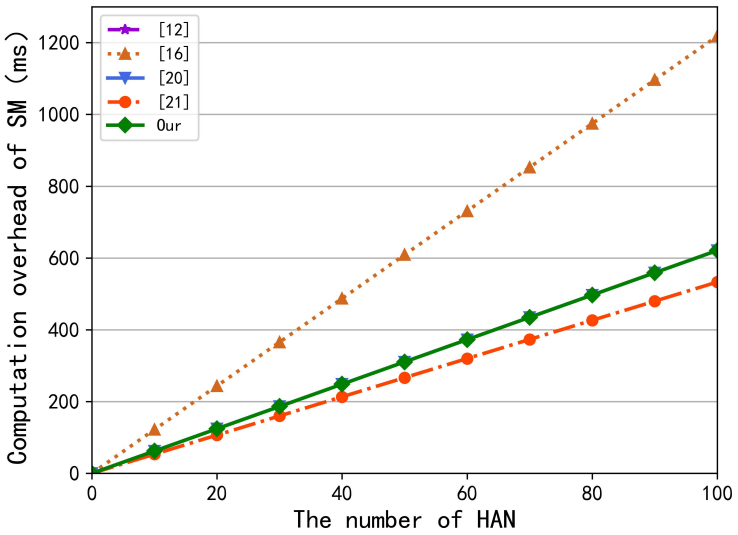

FIGURE 3. The comparison of computation overhead on SM(or HAN)

In addition, when m=1 (i.e., there is only one aggregator), the Raft algorithm of our scheme and the PBFT algorithm of scheme [20] will fail, and the computational overhead of our scheme at the AN and ESP ends is basically the same as that of scheme [20]. When $m \neq 1$ (i.e., there are multiple aggregators), the overhead of our scheme on AN side is slightly better than that of scheme [20]. This is because the Raft consensus algorithm used in our scheme is more efficient than the PBFT algorithm used in scheme [20]. Assuming that a system may have n nodes to fail, the PBFT algorithm requires at least $3n$+1 nodes

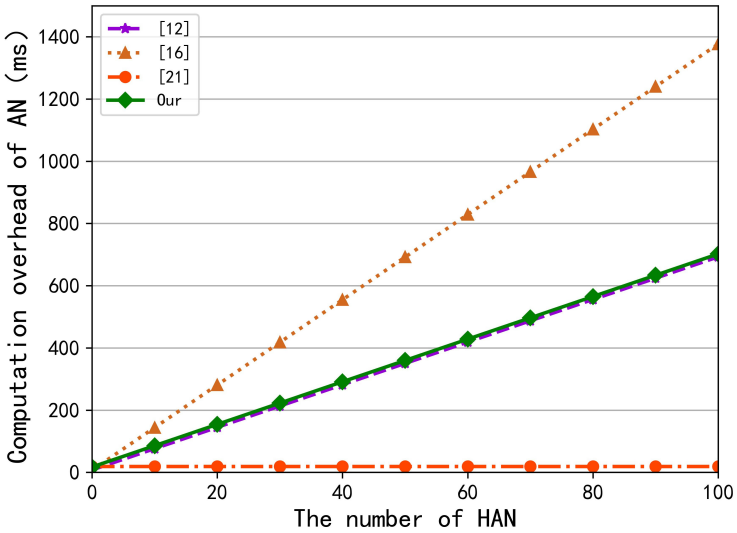

FIGURE 4. The comparison of computation overhead on AN

in the system, while the Raft consensus algorithm only needs $2n+1$ nodes to deal with the fault, so the Raft consensus algorithm has lower computational overhead than the PBFT algorithm. Finally, our scheme has aggregated billing, although on the ESP side our scheme is slightly higher than the schemes [12,16,20-21], but this is within reasonable scope. In addition, our scheme also introduces the electricity tariff verification stage to resist malicious AN attack proposed in this paper. Based on the above analysis, our scheme is more suitable for smart grid applications than the existing schemes [12,16,20-21].

9. **Conclusions.** We design an effective, secure and privacy protected smart grid aggregation billing scheme. Firstly, we use Paillier homomorphic encryption technology to protect the privacy of user data; Secondly, we introduce blockchain technology to provide a distributed consensus algorithm to improve the credibility of the aggregation scheme and ensure data integrity; Thirdly, we use the BLS signature algorithm to ensure the integrity and non repudiation of the user's power data; Finally, we added the electricity charge verification stage to resist malicious AN attack. Security analysis and performance evaluation show that our scheme can not only meet the requirements of privacy protection and security, but also has certain advantages in computing efficiency. In the future, we will focus on the combination of more new technologies and smart grid power data collection methods to design better data aggregation schemes.

Acknowledgment. This work is supported by Natural Science Foundation of Fujian Province of China (No. 2021J011066); Opening Foundation of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund, Fujian Normal University (No. NSCL-KF2021-01); Scientific Research Staring Foundation of Fujian University of Technology (No. GY-Z20171); Undergraduate Teaching Reform Research Project of Fujian University of Technology (No. jg2021060, No. jg2021092).

REFERENCES

[1] F. F. Wu, K. Moslehi and A. Bose, "Power system control centers: Past, present, and future," *Proceedings of the IEEE*, vol. 93, no. 11, pp. 1890-1908, 2005.

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C.Buccella, C. Cecati and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.

[3] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian and N. A. Al-Nabhan, "An enhanced pairing-based authentication scheme for smart grid communications," *Journal of Ambient Intelligence and Humanized Computing*, 2021. [Online]. Available: https://doi.org/10.1007/s12652-020-02740-2.

[4] J.-N. Chen, Y.-P. Zhou, Z.-J. Huang, T.-Y. Wu, F.-M. Zou and R. Tso, "An efficient aggregate signature scheme for healthcare wireless sensor networks," *Journal of Network Intelligence*, vol. 6, no. 1, pp. 1-15, 2021.

[5] T. Namerikawa, N. Okubo, R. Sato, Y. Okawa and M. Ono, "Real-time pricing mechanism for electricity market with built-in incentive for participation," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2714-2724, 2015.

[6] H. Manoochehri and A. Fereidunian, "A multimarket approach to peak-shaving in Smart Grid using time-of-use prices," in *2016 8th International Symposium on Telecommunications (IST)*. IEEE, 2016, pp. 707-712.

[7] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari and M. K. Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," Computers & Security, vol. 95, 101871, 2020.

[8] Q. Mei, H. Xiong, Y.-C. Chen and C.-M. Chen, "Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing," *IEEE Transactions on Engineering Management*, 2022. [Online]. Available: https://doi.org/10.1109/TEM.2022.3159311.

[9] M. Yavari, M. Safkhani, S. Kumari, S. Kumar and C.-M. Chen, "An improved blockchain-based authentication protocol for IoT network management," *Security and Communication Networks*, vol. 2020, 8836214, 2020.

[10] C.-M. Chen, X. Deng, W. Gan, J. Chen and S. K. H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 9046-9068, 2021.

[11] W. Lu, Z. Ren, J. Xu and S. Chen, "Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1246-1259, 2021.

[12] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621-1631, 2012.

[13] L. Chen, R. Lu and Z.Cao, "PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1122-1132, 2015.

[14] S. Li, K. Xue, Q. Yang and P. Hong, "PPMA: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462-471, 2018.

[15] A. Karampour, M. Ashouri-Talouki and B. T. Ladani, "An efficient privacy-preserving data aggregation scheme in smart grid," in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 2019, pp. 1967-1971.

[16] Y. Chen, J. Martínez-Ortega, P. Castillejo and L. López, "A homomorphic-based multiple data aggregation scheme for smart grid," *IEEE Sensors Journal*, vol. 19, no. 10, pp. 3921-3929, 2019.

[17] S. Chen, L. Yang, C. Zhao, V. Varadaraian and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," *Engineering*, vol. 8, pp. 159-169, 2022.

[18] H. Fan, Y. Liu and Z. Zeng, "Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain," *Sensors*, vol. 20, no. 18, 5282, 2020.

[19] Y. Wang, F. Luo, Z. Dong, Z. Tong and Y. Qiao, "Distributed meter data aggregation framework based on Blockchain and homomorphic encryption," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 1, pp. 30-37, 2019.

[20] X. Luo, K. Xue, J. Xu, Q. Sun and Y. Zhang, "Blockchain based secure data aggregation and distributed power dispatching for microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5268-5279, 2021.

[21] K. Xue, Q. Yang, S. Li, D. S. L.Wei,M. Peng, I. Memon and P. Hong, "PPSO: A privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2486-2496, 2019.

[22] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 USENIX Annual Technical Conference (Usenix ATC 14)*. 2014, pp. 305-319.

[23] F. R. S. Taka, "Secure communication by combined Diffe-Hellman key exchange based AES encryption and arabic text steganography," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 12, no. 4, pp. 186-198, 2021.

[24] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1999, pp. 223-238.

[25] N. Karandikar, A. Chakravorty and C. Rong, "Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure," *Sensors*, vol. 21, no. 11, 3822, 2021.

[26] Q. Feng, D. He, S. Zeadally, M. K. Khan and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45-58, 2019.

[27] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Berlin, Heidelberg, 2001, pp. 514-532.

[28] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 3, pp. 381-388, 2011.

[29] J.-N. Chen, F.-M. Zou, T.-Y. Wu and Y.-P. Zhou, "A new certificate-based aggregate signature scheme for wireless sensor networks," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 5, pp. 1264-1280, 2018.

[30] J.-N. Chen, Z.-J. Huang, Y.-P. Zhou, F.-M. Zou, C.-M. Chen, J. M.-T. Wu and T.-Y. Wu, "Efficient certificate-based aggregate signature scheme for vehicular ad hoc networks," *IET Networks*, vol. 9, no. 6, pp. 290-297, 2020.

[31] X. Zuo, L. Li, H. Peng, S. Luo and Y. Yang, "Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid," *IEEE Systems Journal*, vol. 15, no. 1, pp. 395-406, 2021.

[32] B. Lynn, "PBC Library," Accessed: Jul.8, 2022.[Online].Available: http://crypto.stanford.edu/pbc/.