Secure and Fine-grained Electricity Consumption Aggregation Scheme for Smart Grid

Gang Shen[1], Yixin Su[1], Danhong Zhang[1], Huajun Zhang[1], Binyu Xiong[1] and Mingwu Zhang[2]
[1] School of Automation, Wuhan University of Technology
Wuhan, WH 430070 – P. R. China
[e-mail: shengang@whut.edu.cn, suyixin@whut.edu.cn, zhangdh@whut.edu.cn, zhanghj@whut.edu.cn, bxiong2@whut.edu.cn]
[2] School of Computer, Hubei University of Technology
Wuhan, WH 430068 – P. R. China
[e-mail: csmwzhang@gmail.com]
*Corresponding author: Yixin Su

Received July 19, 2017; revised September 22, 2017; accepted November 11, 2017; published April 30, 2018

Abstract

Currently, many of schemes for smart grid data aggregation are based on a one-level gateway (GW) topology. Since the data aggregation granularity in this topology is too single, the control center (CC) is unable to obtain more fine-grained data aggregation results for better monitoring smart grid. To improve this issue, Shen et al. propose an efficient privacy-preserving cube-data aggregation scheme in which the system model consists of two-level GW. However, a risk exists in their scheme that attacker could forge the signature by using leaked signing keys. In this paper, we propose a secure and fine-grained electricity consumption aggregation scheme for smart grid, which employs the homomorphic encryption to implement privacy-preserving aggregation of users' electricity consumption in the two-level GW smart grid. In our scheme, CC can achieve a flexible electricity regulation by obtaining data aggregation results of various granularities. In addition, our scheme uses the forward-secure signature with backward-secure detection (FSBD) technique to ensure the forward-backward secrecy of the signing keys. Security analysis and experimental results demonstrate that the proposed scheme can achieve forward-backward security of user's electricity consumption signature. Compared with related schemes, our scheme is more secure and efficient.

Keywords: Smart grid, fine-grained data, electricity consumption, aggregation, forward-backward security

This work was supported in part by the National Natural Science Foundation of China (No. 61370224, No. 61672010, No. 61702168), the Fundamental Research Funds for the Central Universities (No. 163111005), the Natural Science Foundation of Hubei Province (No. 2016CFB502 and No. 2015CFB586).

http://doi.org/10.3837/tiis.2018.04.009 **ISSN : 1976-7277**

1. Introduction

According to the survey, the cost of power outages is about 100 billion dollars in US traditional power systems each year [1]. The main reason is that the traditional power system lacks the efficient ability to implement diagnostics and self-healing. In the traditional paradigm of power system operations, the electricity is generated in power plants and delivered along the transmission systems to consumers in distribution systems, which lacks the two-way communication of information [2]. Since traditional power grid is inefficient and unreliable, it cannot meet the increasing electricity demand. Compared with traditional power grid, smart grid is one of cyber-physical systems. It may provide two-way electricity and information flow, which not only promotes the rational distribution of energy allocation but also achieves system monitoring and recovery [3]. The two-way interactive power supply of smart grid could realize the information exchange and the demand interaction between the users and the enterprise, which benefits both the alleviation of the energy crisis and environmental protection [4]. Referring to the overview of the entire smart grid infrastructure provided by National Institute of Standards and Technologies (NIST) [5], the architecture of smart grid contains the following seven domains: generation, transmission, distribution, operation, electricity markets, service providers, and customers, as shown in **Fig. 1**.

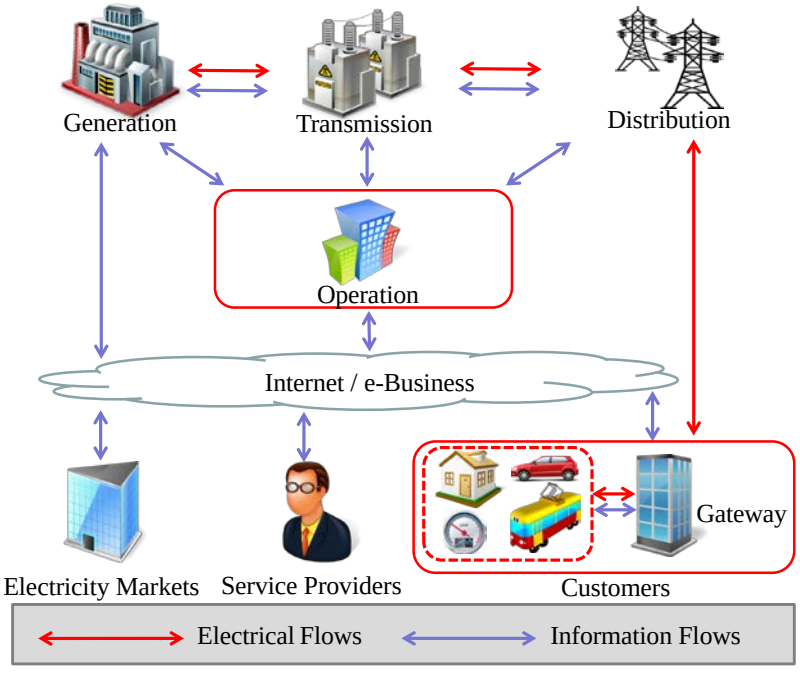

Fig. 1. The architecture of smart grid based on the NIST framework.

As we all know, the privacy preservation is a quite critical issue in the smart grid communications. User's behavior can be easily inferred from the leakage of his electricity information. Thus, the security challenge in smart grid is how to better protect the user privacy. In recent years, many smart grid schemes on communication security have been proposed [6-12]. However, these research works for the smart grid are almost based on a one-level GW topology (i.e., only one GW exists between the CC and the home area networks (HANs)), which the GW only covers the HANs of one residential area (RA). Based on this model, the

system can only achieve the users' electricity consumption aggregation of one RA so that the aggregation granularities of users' electricity consumption are too single, which should lead to non-flexible electricity regulation. Shen et al. [8] introduce a privacy-preserving multilevel users' data aggregation scheme that is the first scheme to propose a practical system model with two-level gateway topology. In their scheme, the residential area gateway (RAGW) achieves fine-grained users' electricity consumption aggregation (i.e., residential area-level users' electricity consumption aggregation); the district gateway (DGW) achieves coarse-grained users' electricity consumption aggregation (i.e., district-level users' electricity consumption aggregation). The CC in smart grid can better monitor and control smart grid by obtaining different region fine-grained data aggregation results.

In addition, privacy-preserving data aggregation schemes also use the digital signature techniques to ensure the data integrity and authenticity [21-22]. The basic principle of digital signature is that signer signs the message with signing keys and verifier decrypts the message with public keys. However, the abovementioned schemes have a common drawback that the signing keys remain unchanged. Once the signing keys are exposed, an adversary can use the signing keys to forge the future message signature or decrypt any previous users' sensitive information. To resist the above attacks, the forward-backward security technology should be considered in the smart grid. As far as we know, many researchers have proposed the schemes about forward-secure signature [7, 13-17]. Forward secrecy means that even if an adversary obtains the current time period's key, he cannot get the message of prior period. Li et al. [7] propose an efficient privacy-preserving demand response scheme with adaptive key evolution. Specifically, their scheme adopts key evolution techniques to realize forward secrecy of users' session keys and evolution of users' private keys. However, they do not consider whether the keys leakage will affect the system future security. Unfortunately, the adversary could deduce the future secret keys in the light of the currently disclosed secret key. Although the security of the past secret keys can be guaranteed, the future secret keys could be compromised. That is to say, the adversary can forge the future signature message by compromising the future secret keys [18]. Therefore, the forward-backward secrecy should be considered to improve the security of the scheme.

Based on the abovementioned issues, we propose a secure and fine-grained electricity consumption aggregation scheme in this paper. This work is a research on the privacy protection of multilevel GW topology of the smart grid, which adopts PSBD signature technology to improve the system security. Concretely, the contributions of this paper are twofold:

- Firstly, inspired by the fact that many existing schemes are based on a one-level gateway topology, which is unable to achieve the flexibility of electricity regulation, we present the scheme that adopts the homomorphic encryption to realize users' electricity consumption privacy-preserving aggregation in the framework of the smart grid with two-level gateway topology. The security analysis shows that the proposed scheme can ensure the confidentiality of user sensitive information in different areas and the flexibility of electricity regulation.
- Secondly, considering the existing schemes could suffer from the risk of secret keys leakage, our scheme adopts the FSBD signature technique to achieve the forward-backward security of the signing keys. Compared with schemes [7-8], the proposed scheme can prevent the adversary who has the current time period's key from obtaining user privacy of prior or posterior time period. In addition, our scheme is more reliable, efficient and practical.

The remainder of the paper is organized as follows. We present related works in Section 2. In Section 3, we introduce the system model, security model and design goal. In Section 4, we review the Paillier cryptosystem [6], the one-way hash chain [19] and FSBD signature [18]. Next, we propose the concrete scheme in Section 5, and security analysis in Section 6. The comparisons of different schemes and performance evaluation are provided in Section 7. Finally, we draw our conclusions in Section 8.

2. Related Work

In the schemes of the smart grid, homomorphic encryption and data aggregation techniques are often adopted to deal with user's electricity consumption. In [8], Shen et al. first propose a practical two-level GW model for smart grid. They realize a multilevel users' electricity consumption aggregation by combining Paillier's additive homomorphic encryption and BLS signature techniques. In [9], Wang et al. present a scheme that based on Paillier's homomorphic encryption, which can prevent the attacks of outside and inside adversaries. In Wang et al.'s scheme, the secure response of user's billing is achieved by the forward secure session. Abdallah and Shen [13] provide a protocol that messages authenticity and integrity are ensured by exploiting lightweight lattice-based homomorphic cryptosystem. Homomorphic and data aggregation schemes are also widely used in other fields. In [23], Cheng et al. present an improved scheme after analyzing the security of the homomorphic signature scheme of network coding, which can effectively deal with the proposed attack. Liu et al. [24] propose a privacy-preserving health data aggregation scheme based on differential privacy, which not only resists against various attacks, but also achieves the robustness.

Since signature techniques can ensure the authenticity and integrity of user data, they are usually used in many aggregation schemes. Aitzhan and Svetinovic [10] propose a secure protocol to solve the problem of providing transaction security in decentralized smart grid. They use multi-signatures to improve the privacy and security of the scheme. In [11], Fan et al. present a scheme with offline trusted third party (TTP), which can prevent internal attackers. They provide the secure and efficient batch verification for signature, which greatly improves the efficiency of the system. Forward secrecy can guarantee that the private key and message of the previous period are confidential. Bellare and Miner [21] describe a digital signature scheme of forward secrecy that the signing key is updated at regular intervals. Therefore, in their scheme, the adversary cannot forge the previous signature even if he compromises the current secret key. In [17], Libert et al. present the method to construct forward secrecy scheme in untrusted update environments. Li et al. [7] propose an EPPDR scheme with adaptive key evolution that adopts key evolution mechanism of round to update the users' private keys. Their schemes can realize the forward secrecy of users' session keys. Lin et al. [18] provide a forward-backward secure signature scheme based on Abdalla and Reyzin's forward secure signature scheme, which can both realize the forward security and backward security for digital signatures.

In this paper, we adopt homomorphic encryption and forward-backward secure signature technology to ensure the security of the smart grid communications.

3. Model and Design Goals

In this section, we formalize the system model, security model, and design goal.

3.1 System Model

In this paper, we present a system model of the smart grid with a two-level GW topology, as shown in **Fig. 2**, which includes control center (CC), district gateway (DGW), residential area gateway (RAGW), and home area networks (HANs). This system model is in line with the administrative division of the practical smart grid. For simplicity, we assume that the CC manages l districts (i.e., the CC covers l DGWs), and the GW of each district corresponds to $\mathrm{DGW}_1, \mathrm{DGW}_2, ..., \mathrm{DGW}_l$. There are m residential areas in each district (i.e., each DGW covers m RAGWs), and the GW of each residential area corresponds to $\mathrm{RAGW}_1, \mathrm{RAGW}_2, ..., \mathrm{RAGW}_m$. There are n Users (i.e., $\mathrm{U}_1, \mathrm{U}_2, ..., \mathrm{U}_l$) in each residential area (i.e., each RAGW covers n HANs). Each HAN is equipped with a smart meter (SM) to achieve automatic two-way communication between HAN users and CC. For the sake of simplicity, we denote the i-th district GW as DGW_i, the j-th residential area GW in district i as RAGW_{ij}, and the k-th user in the j-th residential area in district i as U_{ijk}, respectively, where $i = 1, 2, \cdots, l$, $j = 1, 2, \cdots, m$, $k = 1, 2, \cdots, n$.

The system communication model is described as follows: HANs communicates with the RAGW via WiFi. RAGWs connect to DGW with the wired. Usually, communication between DGWs and CC is through the links with high bandwidth and low delay.

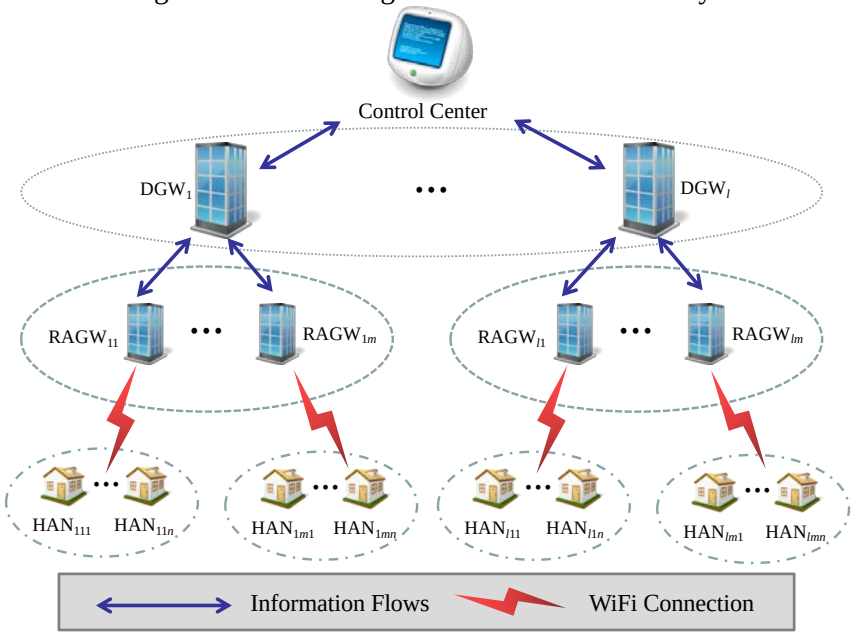

Fig. 2. System model of smart grid with a two-level GW topology.

3.2 Security Model

We consider CC is fully trusted in our security model, and it will not be compromised by the adversaries. Our security model will meet the following security requirements:

1) **Confidentiality of electricity consumption.** In the proposed scheme, an adversary $\mathcal{A}$ cannot decrypt the user electricity information even if it intrudes into the database of RAGWs, DGWs or steals the communication flows. In other words, the message is transmitted between the entities or stored in the entities, the user's privacy will not be leaked. Thus, the user's

electricity consumption can meet the privacy-preserving requirement.

2) **Forward-backward secrecy of signing key.** Even if adversary $\mathcal{A}$ obtains the current time period's signing key, it cannot decrypt any prior time period's messages and forged the posterior time period's message signatures. In other words, if adversary $\mathcal{A}$ compromises a user, it can neither obtain user previous electricity consumption nor forge future electricity information of user. Therefore, the forward-backward secrecy of signing key can be realized.

3) **Authentication and Unforgeability of message signature.** To protect the scheme against the impersonation attacks, the receiver should verify the legitimacy of the received data, which prevents pseudo legitimate entities from transmitting forged messages or modifying data. Therefore, in our scheme, the message signature of the DGWs and users should be authenticated by the CC and RAGWs, and the message signature of RAGWs should be authenticated by the DGWs. In addition, the message signature can not be forged by adversary.

3.3 Design Goal

Based on the aforementioned system models, we design the scheme that has the following two desirable objectives.

1) The proposed scheme should meet the security, i.e., using the forward-backward secrecy of signing keys technology to improve system security.

2) Since the electricity regulation of CC may face a different range, the proposed scheme should meet the practical requirements that the CC can flexibly and effectively control the electricity consumption, i.e., the RAGW achieves fine-grained users' electricity consumption aggregation, the DGW achieves coarse-grained users' electricity consumption aggregation.

4. Preliminaries

We briefly review the Paillier cryptosystem [6], one-way hash chain [19] and FSBD signature [18] in this section. The proposed scheme will be based on them.

4.1 Paillier Cryptosystem

The Paillier cryptosystem is classic homomorphic encryption proposed by Paillier in 1999 [6]. It consists of three algorithms as following:

1) Key generation: Calculate $N = p \cdot q$ and $\lambda = lcm(p-1, q-1)$, where p, q are two large prime numbers, and $|p| = |q| = \kappa$, where κ is a security parameter. Define the function $L(u) = (u-1)/N$, choose generator $g \in \mathbb{Z}^*_{N^2}$, and compute $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod N$. The public key is $pk = (N, g)$, and the corresponding private key is $sk = (\lambda, \mu)$.

2) Encryption: Given plaintext $M \in \mathbb{Z}_N$, choose a random number $r \in \mathbb{Z}^*_N$, and calculate ciphertext $C = E(M) = g^M \cdot r^N \bmod N^2$.

3) Decryption: Given ciphertext $C \in \mathbb{Z}^*_{N^2}$, the corresponding plaintext can be recovered by computing $M = D(C) = L(C^{\lambda \bmod N^2}) \cdot \mu \bmod N$.

4.2 One-Way Hash Chain

The one-way hash chain technique has been widely used in many practical cryptographic [19]. The one-way hash chain is defined as follows:

Definition 1: Let $h(\cdot)$ be a collision-resistant one-way hash function, calculate $h^T(\cdot)=h(h(h^{T-1}(\cdot)))=h(h(h^{T-2}(\cdot)))=\underbrace{h(h...(h}_{T}(\cdot))...)$ and $h^0(\cdot)=\cdot$, where $h^T(\cdot)$ denotes one-way hash chain, and T is the total number of time periods.

4.3 FSBD Signature

FSBD signature is proposed in [18], which includes five algorithms as follows:

Algorithm 1. KeyGen( )

Input: Security parameter κ

Output:

1. Let $N=p\cdot q$, $|Q|\geq 2^{k-3}$,and collision-resistant hash function $H:\{0,1\}^*\rightarrow\{0,1\}^L$, where L denotes the length of hash values
2. Choose $s_0\in Q$, compute $u=1/s_0^{2^{L(T+1)}}\pmod N$, where T denotes the total number of periods
3. Pick $x\in\mathbb{Z}_N^*$, compute $v_0=h^T(x)$
4. Return (s_0, x) and (u, v_0, H)

Algorithm 2. Sign( )

Input: The τ -th message M_τ, private key s_τ and (u, v_0, H)

Output:

1. Pick $r_\tau\in\mathbb{Z}_N$, compute the $(\tau+1)$ -th hash chain number $v_{\tau+1}=h^{T-(\tau+1)}(x)$, $a_\tau=H(\tau,v_0,y_\tau,M_\tau)$ and $z_\tau=r_\tau\cdot(s_\tau)^{a_\tau}\pmod N$, where $y_\tau=r_\tau^{2^{L(T+1-\tau)}}\pmod N$
2. Compute $\sigma_\tau=<\tau,v_{\tau+1},a_\tau,z_\tau,M_\tau>$
3. Return σ_τ

Algorithm 3. Verify( )

Input: The signature for period τ σ_τ

Output:

1. Compute $y'_\tau=z_\tau^{2^{L(T+1-\tau)}}u^{a_\tau}\pmod N$ and $a'_\tau=H(\tau,v_0,y'_\tau,M_\tau)$
2. Check $a_\tau\overset{?}{=}a'_\tau$
3. Return 1 if the equation in Step 2 holds or 0 otherwise

Algorithm 4. BackDet( )

Input: The $(\tau+1)$ -th hash chain number $v_{\tau+1}=h^{T-(\tau+1)}(x)$

Output:

1. Compute $v'_0=h^{\tau+1}(v_{\tau+1})$, where $h^{\tau+1}(v_{\tau+1})=h^{\tau+1}(h^{T-(\tau+1)}(x))=v'_0$
2. Check $h^T(x)\equiv v_0\overset{?}{=}v'_0$
3. Return 1 if the equation in Step 2 holds or 0 otherwise

Algorithm 5. KeyUpdate( )

Input: The τ -th period signing key s_τ

Output:

1. Compute $s_{\tau+1}=s_\tau^{2^L}\pmod N$
2. Return $s_{\tau+1}$

Definition 2: (The Blum Factorization Problem) Let N is the product of two large primes p and q with the same length $p \equiv q \equiv 3(\mathrm{mod}\,4)$, find p or q.

5. Proposed Concrete Scheme

We propose the concrete scheme in this section. The proposed scheme consists of five phases: system initialization, user electricity report generation, privacy-preserving electricity report aggregation, user electricity report reading, and key evolution. For convenience, we list the main notations in **Table 1.**

Table 1. Notation used in the proposed scheme

Notation	Description
DGW_i	The i-th district GW $(i = 1,2,\cdots,l)$
RAGW_{ij}	The j-th residential area GW in district i $(j = 1,2,\cdots,m)$
U_{ijk}	The k-th user in the j-th residential area in district i $(k = 1,2,\cdots,n)$
L	The length of hash values
T	The total number of periods
$h^T(x)$	The one-way hash chain
$d_{ijk,w}$	User U_{ijk}'s electricity consumption in the w-th period
$sk_{ijk,w}$	User U_{ijk}'s private key in the w-th period
$sk_{ij,w}$	RAGW_{ij}'s private key in the w-th period
$sk_{i,w}$	DGW_i's private key in the w-th period
$C_{ijk,w}$	The w-th period encrypted user report
$C_{ij,w}$	The w-th period aggregated and encrypted user report
$C_{i,w}$	The encrypted user report of the second times aggregation in period w
$\sigma_{ijk,w}$	The w-th period user report's signature
$\sigma_{ij,w}$	The w-th period user fine-grained aggregated report's signature
$\sigma_{i,w}$	The w-th period user coarse-grained aggregated report's signature

5.1 System Initialization

1) System parameter generation: We assume the CC will bootstrap the whole system. Concretely, given the security parameter κ, CC first chooses two large prime numbers p, q and calculates the Paillier cryptosystem's public key ($N = p \cdot q, g$), and the corresponding private key (λ, μ), where $p \equiv q \equiv 3(\mathrm{mod}\,4)$ and $|p| = |q| = \kappa$, $g \in \mathbb{Z}^*_{N^2}$. Given the set of non-zero quadratic residues modulo N Q, where $|Q| \geq 2^{\kappa-3}$. Then CC also chooses a collision-resistant hash function $H: \{0,1\}^* \to \{0,1\}^L$.

2) System entity registration: In the DGW_i registration phase, it first chooses a random number $sk_i \in Q$ as the private key, and computes the corresponding public key $u_i = 1/sk_i^{2^{L(T+1)}}$.

Then DGW_i picks a random number $x_i \in \mathbb{Z}_N^*$ and computes $v_{i,0} = h^T(x_i)$. When $\mathrm{RAGW}_{ij} \in \mathrm{DGW}_i$ registers itself into the system, RAGW_{ij} chooses a random number $sk_{ij} \in Q$ as its private key, and computes the corresponding public key $u_{ij} = 1/sk_{ij}^{2^{L(T+1)}}$. RAGW_{ij} also chooses a random number $x_{ij} \in \mathbb{Z}_N^*$ and computes $v_{ij,0} = h^T(x_{ij})$. Similarly, when $\mathrm{U}_{ijk} \in \mathrm{RAGW}_{ij}$ registers itself into the system, U_{ijk} chooses a random number $sk_{ijk} \in Q$ as its private key, and computes the corresponding public key $u_{ijk} = 1/sk_{ijk}^{2^{L(T+1)}}$. U_{ijk} also chooses a random number $x_{ijk} \in \mathbb{Z}_N^*$ and computes $v_{ijk,0} = h^T(x_{ijk})$. Finally, CC publishes the system parameters as $\{N, g, H, Q\}$, and keeps $\{\lambda, \mu\}$.

5.2 User electricity report generation

Each HAN user U_{ijk} uses SM to collect his electricity consumption $d_{ijk,w}$ in the w-th period, and performs the following steps, as shown in **Fig. 3**:

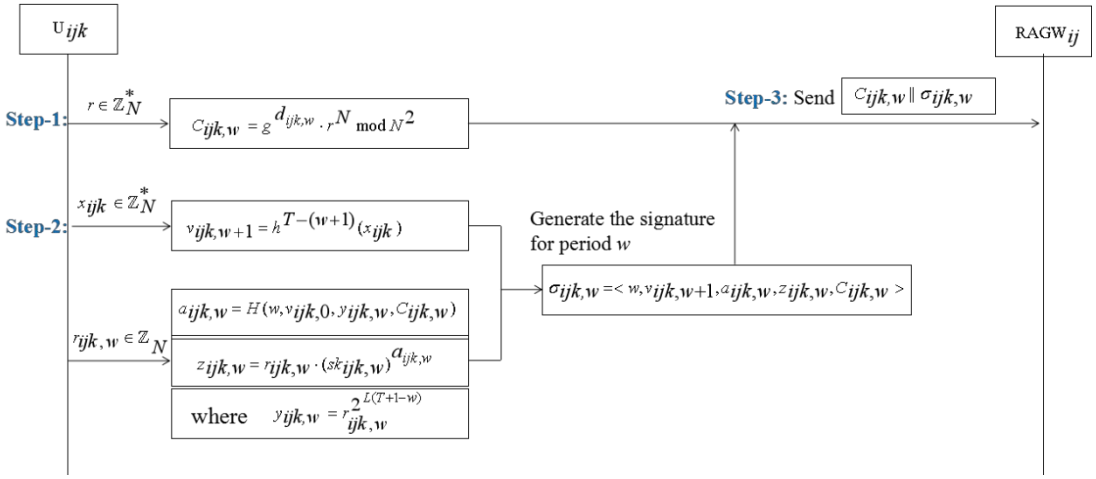

Fig. 3. The steps of user's signature electricity report generation.

5.3 Privacy-preserving electricity report aggregation

1) RAGW privacy-preserving electricity report aggregation: After receiving total n encrypted electricity reports $C_{ijk,w} \| \sigma_{ijk,w}$, RAGW_{ij} first checks signature $\sigma_{ijk,w}$ to verify its validity. RAGW_{ij} computes $y'_{ijk,w}$ as $y'_{ijk,w} = z_{ijk,w}^{2^{L(T+1-w)}} u_{ijk}^{a_{ijk,w}}$ and computes $a'_{ijk,w}$ as $a'_{ijk,w} = H(w, v_{ijk,0}, y'_{ijk,w}, C_{ijk,w})$. The signature is valid if $a_{ijk,w} = a'_{ijk,w}$. The correctness of the signature verification will be demonstrated as follow:

$$
\begin{aligned}
y'_{ijk,w} &= z_{ijk,w}^{2^{L(T+1-w)}} \cdot u_{ijk}^{a_{ijk,w}} \pmod N \\
&= (z_{ijk,w})^{2^{L(T+1-w)}} \cdot (1/sk_{ijk,w}^{2^{L(T+1)}})^{a_{ijk,w}} \\
&= (r_{ijk,w} \cdot (sk_{ijk,w})^{a_{ijk,w}})^{2^{L(T+1-w)}} \cdot (1/sk_{ijk,w}^{2^{L(T+1)}})^{a_{ijk,w}} \\
&= (r_{ijk,w} \cdot (sk_{ijk,w})^{a_{ijk,w}})^{2^{L(T+1-w)}} \cdot (1/sk_{ijk,w}^{2^{L(T+1)}})^{a_{ijk,w}} \\
&= r_{ijk,w}^{2^{L(T+1-w)}} \cdot sk_{ijk,w}^{a_{ijk,w}2^{L(T+1)}} \cdot (1/sk_{ijk,w}^{2^{L(T+1)}})^{a_{ijk,w}} \\
&= r_{ijk,w}^{2^{L(T+1-w)}} \pmod N \\
&= y_{ijk,w} \pmod N
\end{aligned}
\tag{1}
$$

After the validity checking, RAGW_{ij} computes $v'_{ij,0}$ as $v'_{ij,0} = h^{w+1}(v_{ij,w+1})$, where $h^{w+1}(v_{ij,w+1}) = h^{w+1}(h^{T-(w+1)}(x_{ij})) = v'_{ij,0}$, then it check that $h^T(\mathrm{x}_{ij}) \equiv v_{ij,0} \stackrel{?}{=} v'_{ij,0}$. Finally, RAGW_{ij} can obtain fine-grained aggregated ciphertext by performing the following steps, as shown in **Fig. 4**:

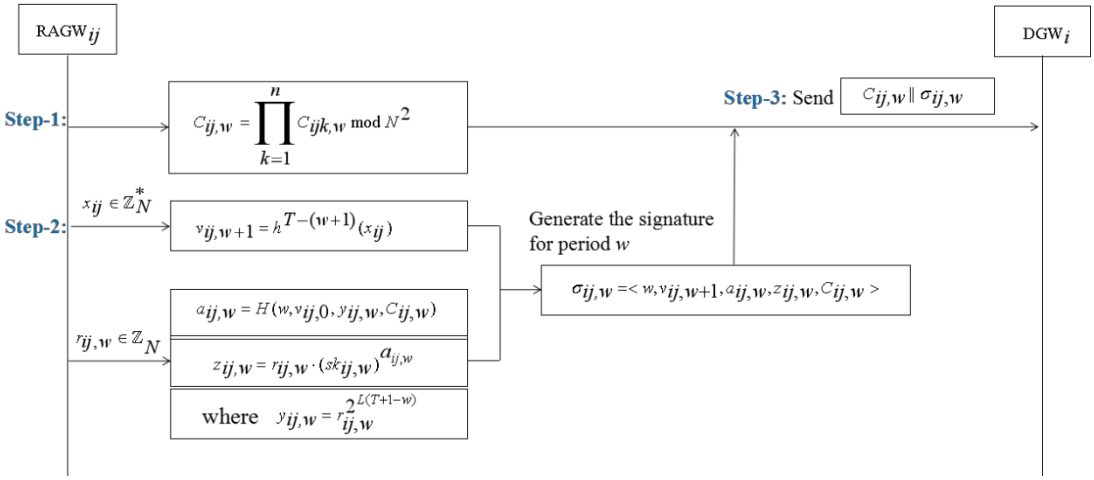

Fig. 4. The steps of RAGW_{ij} obtaining fine-grained aggregated ciphertext.

2) DGW privacy-preserving electricity report aggregation: After receiving total m fine-grained encrypted electricity reports $C_{ij,w} \| \sigma_{ij,w}$, DGW_i first checks signature $\sigma_{ij,w}$ to verify its validity. DGW_i computes $y'_{ij,w}$ as $y'_{ij,w} = z_{ij,w}^{2^{L(T+1-w)}} u_{ij}^{a_{ij,w}}$ and computes $a'_{ij,w}$ as $a'_{ij,w} = H(w, v_{ij,0}, y'_{ij,w}, C_{ij,w})$. The signature is valid if $a_{ij,w} = a'_{ij,w}$. The method of the signature verification's correctness is similar to the method mentioned in Section 5.3 -1).

After the validity checking, DGW_i computes $v'_{i,0}$ as $v'_{i,0} = h^{w+1}(v_{i,w+1})$, where $h^{w+1}(v_{i,w+1}) = h^{w+1}(h^{T-(w+1)}(x_i)) = v'_{i,0}$, then it check that $h^T(\mathrm{x}_i) \equiv v_{i,0} \stackrel{?}{=} v'_{i,0}$. Finally, DGW_i can obtain coarse-grained aggregated ciphertext by performing the following steps, as shown in **Fig. 5**:

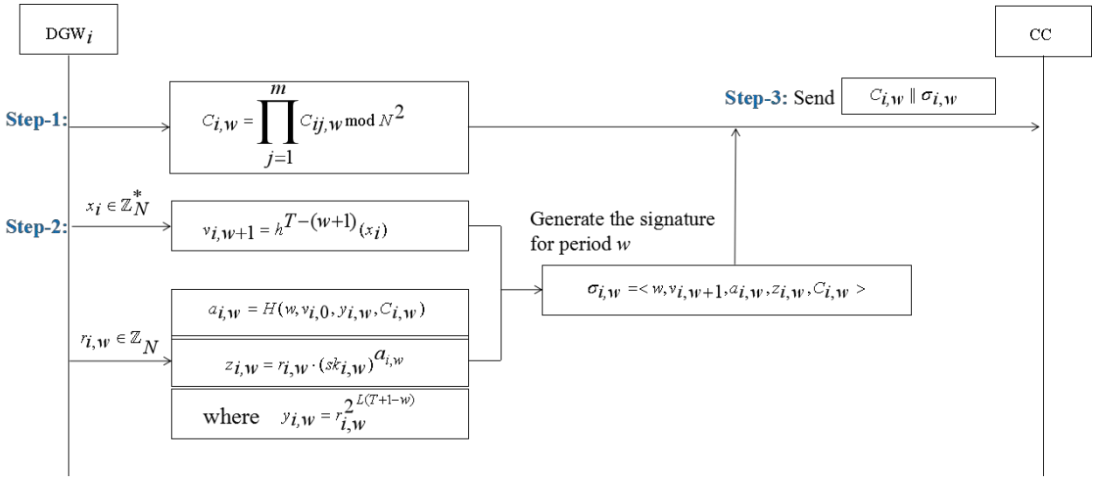

Fig. 5. The steps of DGW$_i$ obtaining coarse-grained aggregated ciphertext.

5.4 User electricity report reading

Upon receiving total l coarse-grained encrypted electricity usage data $C_{i,w} \| \sigma_{i,w}$, the CC first checks signature $\sigma_{i,w}$ to verify its validity. CC computes $y'_{i,w}$ as $y'_{i,w} = z_{i,w}^{2^{L(T+1-w)}} u_i^{a_{i,w}} (\bmod N)$ and computes $a'_{i,w}$ as $a'_{i,w} = H(w, v_{i,0}, y'_{i,w}, C_{i,w})$. The signature is valid if $a_{i,w} = a'_{i,w}$. The method of the signature verification's correctness is similar to the method mentioned in Section 5.3 -1).

After the validity checking, CC performs the following steps to read the aggregated electricity usage data C_w, where C_w is implicitly formed by

$$
\begin{aligned}
C_w &= \prod_{i=1}^{l} C_{i,w} \\
&= \prod_{i=1}^{l} (\prod_{j=1}^{m} C_{ij,w}) \\
&= \prod_{i=1}^{l} (\prod_{j=1}^{m} (\prod_{k=1}^{n} C_{ijk,w})) \\
&= \prod_{i=1}^{l} (\prod_{j=1}^{m} (\prod_{k=1}^{n} g^{d_{ijk,w}} \cdot r^N \bmod N^2)) \\
&= \prod_{i=1}^{l} (\prod_{j=1}^{m} (g^{\sum_{k=1}^{n} d_{ijk,w}} \cdot (\prod_{k=1}^{n} r)^N \bmod N^2)) \\
&= \prod_{i=1}^{l} (g^{\sum_{j=1}^{m} (\sum_{k=1}^{n} d_{ijk,w})} \cdot (\prod_{j=1}^{m} (\prod_{k=1}^{n} r))^N \bmod N^2) \\
&= g^{\sum_{i=1}^{l} (\sum_{j=1}^{m} (\sum_{k=1}^{n} d_{ijk,w}))} \cdot (\prod_{i=1}^{l} (\prod_{j=1}^{m} (\prod_{k=1}^{n} r)))^N \bmod N^2
\end{aligned}
\tag{2}
$$

Let $M=\sum_{i=1}^{l}(\sum_{j=1}^{m}(\sum_{k=1}^{n}d_{ijk,w}))$ and $R=\prod_{i=1}^{l}(\prod_{j=1}^{m}(\prod_{k=1}^{n}r))$, then $C_w=g^M\cdot R^N \bmod N^2$ is a ciphertext form of Paillier Cryptosystem, and so CC can use the private key (λ,μ) to recover M as $M=\sum_{i=1}^{l}(\sum_{j=1}^{m}(\sum_{k=1}^{n}d_{ijk,w}))$.

5.5 Key Evolution

For the entities in the system (i.e., the U_{ijk}, $RAGW_{ij}$ and DGW_i), their private keys are only valid until the specified expiry date *w*. After *w*, if the new private keys are generated, the private keys before expiration date *w* will be automatically revoked. Via key-updating mechanism, the entities updating the w-th period private key s_w into $s_{w+1}=s_w^{2^L} \pmod N$. After that, the entities in the system delete the previous private keys. Even if an adversary $\mathcal{A}$ compromises the U_{ijk}, $RAGW_{ij}$ or DGW_i, it cannot obtain any previous private keys. Therefore, the forward secrecy of private keys (i.e., signing keys) is achieved.

6. Security Analysis

In this section, we will make the security analysis for proposed scheme based on the security requirements discussed in Section 3.2.

6.1 The confidentiality of user's electricity consumption

Theorem 1. The proposed scheme can ensure the confidentiality of user's electricity consumption.

Proof. In our scheme, the user's electricity consumption is encrypted as a Paillier homomorphic cipthertext. Since Paillier cryptosystem is semantic secure against the chosen plaintext attack (CPA) [6], the user's electricity consumption is semantic secure and confidential. Thus, even if adversary $\mathcal{A}$ obtains the ciphertext, he still cannot recognize the corresponding electricity consumption. In proposed scheme, DGW and RAGW only perform the work of aggregating and relaying data, they cannot decrypt the electricity consumption. Therefore, adversary $\mathcal{A}$ will not get the electricity consumption, even though he compromises the database of DGW or RAGW. In addition, if adversary $\mathcal{A}$ intrudes the CC's database and obtains the private key to recover the aggregated electricity consumption $\sum_{i=1}^{l}(\sum_{j=1}^{m}(\sum_{k=1}^{n}d_{ijk,w}))$. However, since $\sum_{i=1}^{l}(\sum_{j=1}^{m}(\sum_{k=1}^{n}d_{ijk,w}))$ and $\sum_{k=1}^{n}d_{ijk,w}$ are aggregated results, $\mathcal{A}$ cannot obtain the each user's electricity consumption yet. Therefore, the proposed scheme can protect user's electricity consumption privacy.

6.2 Forward-backward secrecy of signing key

In our scheme, the achievement of communication confidentiality between the entities is based on the signing keys forward-backward secrecy.

Theorem 2. The proposed scheme can ensure the forward secrecy of signing key.

Proof. Forward secrecy indicates that even if the adversary $\mathcal{A}$ obtains the current time period's signing key, he cannot decrypt the previous messages. In other words, the current time period's signing key is only used to sign the message of this time period, i.e., if the w-th time period secret key is exposed, adversary $\mathcal{A}$ cannot decrypt the previous messages with this secret key. The reason is that the computation of s_{w-1} from $s_{w-1}^{2^L} (\mathrm{mod}\, N)$ is irreversible, which is equivalent to factor *N*. Accordingly, the proposed scheme realizes the forward secrecy of signing key.

On the other hand, backward secrecy means that even if the adversary $\mathcal{A}$ obtains the current time period's signing key, he cannot forge the future signing key. In message signature phase, each entity computes the hash chain number v_{w+1}. If adversary $\mathcal{A}$ has forged a valid message signature (w, v_{w+1}, a_w, z_w), he has to provide the $(w+1)$-th hash value v_{w+1} for calculation of $v'_0 = h^{w+1}(v_{w+1})$, whilst the receiver has to check $a'_j = H(w, v'_0, y'_w, M_w)$. However, since the computation of v_{w+1} from v_0 is irreversible, the adversary $\mathcal{A}$ cannot obtain the correct hash chain number v_{w+1} to computer valid v'_0.

Theorem 3. The proposed scheme can ensure the backward secrecy of signing key.

Proof. We suppose that there exists an adversary $\mathcal{A}$ with non-negligible probability. He can compromise the future secret key (i.e., signing key). Without losing generality, assuming that adversary $\mathcal{A}$ can obtain all the secret parameter $(1, v_2, a_1, z_1), \ldots, (w, v_{w+1}, a_w, z_w)$ before the *w*-th time period, and he can forge a valid signature $(w', v_{w'+1}, a_{w'}, z_{w'}, M_{w'})$ for the *w*-th time period, where $w < w'$. This signifies that the adversary $\mathcal{A}$ has to gain the hash value $v_{w'+1} = h^{T-(w'+1)}(x)$ from $v_{w+1} = h^{T-(w+1)}(x)$ without the *x* value. However, we can gain the hash values $v_{w+2}, v_{w+3}, \ldots, v_{w'-w}$ with the same probability ε. Apparently, this contradicts the definition of collision-resistant one-way hash function [18]. As much, the proposed scheme can ensure the backward secrecy of signing key.

As such, the forward-backward secrecy of signing key can be realized in our scheme.

6.3 Authentication and unforgeability of message signature

Theorem 4. The proposed scheme can achieve the authentication and the unforgeability of message signature.

Proof. In our scheme, each entity uses its private key to generate a signature for the message before sending a message. When receiving a message packet, the receiver uses the corresponding verification key to verify the message packet. As mentioned in Section 6.2, the signing key meets forward-backward secrecy, which ensures that the adversary $\mathcal{A}$ cannot forge the message signature in any time, and each entity cannot repudiate the authenticity of the past signature. Therefore, the authentication and unforgeability of message signature are guaranteed in our scheme.

7. Comparative analysis and performance evaluation

In this section, we first compare our scheme with schemes [7-8] in terms of main characteristics. Then we evaluate the performance of our scheme in terms of the computational cost and communication overhead.

7.1 Comparative analysis

Shen et al. [8] achieve a multilevel users' electricity consumption aggregation by adopting homomorphic Paillier cryptosystem and signature technique. In our scheme and scheme [8], the system models are all two-level gateway topology for smart grid, which the CC be able to monitor smart grid much better by obtaining different region fine-grained data aggregation results. However, scheme [8] exists a risk that the adversary could forge the signature with leaked signing key. Since the private key of each entitiy in scheme [8] is always the same at any time, using the private key, the adversary may modify the signature message for any prior time period and forge the future valid message signature. Therefore, scheme [8] can better achieve the flexibility of electricity regulation, but it cannot provide the forward-backward secrecy of signing key.

In scheme [7], Li et al. propose the scheme that realizes secure and efficient electricity demand aggregation based on the homomorphic encryption and key evolution techniques. They adopt key evolution techniques to realize forward secrecy of users' session keys. However, they did not consider whether the keys leakage will affect the future security of system.

Compared with the schemes [7-8], our scheme can better achieve both the flexibility of electricity regulation, and provide the forward-backward secrecy of signing key. We present the main characteristic comparison of the abovementioned three schemes in **Table 2**.

7.2 Computational costs

We evaluate the computational cost performance of each entity in the system (i.e., User, RAGW, DGW and CC). In this paper, the experiments are conducted on a computer of 3-GHz Pentium IV processor with 512 MB memory. The cryptography operation time is obtained according to the MIRACL [27] and PBC [28] libraries. Compared with other operations, the multiplication in $\mathbb{Z}_{N^2}^*$ is negligible. In our scheme, User U_{ijk} performs 3 exponentiation operations in $\mathbb{Z}_{N^2}^*$ to generate $C_{ijk,w}$ as $C_{ijk,w} = g^{d_{ijk,w}} \cdot r^N \bmod N^2$, and performs 1 exponentiation operations in $\mathbb{Z}_{N^2}^*$ for $\sigma_{ijk,w} =< w, v_{ijk,w+1}, a_{ijk,w}, z_{ijk,w}, C_{ijk,w} >$. In privacy-preserving report aggregation phase, $RAGW_{ij}$ performs $(2n+1)$ exponentiation operations in $\mathbb{Z}_{N^2}^*$, and DGW_i performs $(2m+1)$ exponentiation operations in $\mathbb{Z}_{N^2}^*$. The CC performs 2 exponentiation operations in $\mathbb{Z}_{N^2}^*$ in user report reading phase. The computational costs of schemes [7-8] and our scheme are compared in **Table 3** .

Table 2. Comparison of main characteristics

Characteristics	Scheme [7]	Scheme [8]	Our scheme
Multi-area	Yes	Yes	Yes
Two-level GW	No	Yes	Yes
Two-level aggregation	No	Yes	Yes
Data confidentiality	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes
Key evolution	Yes	No	Yes
Forward secrecy	Yes	No	Yes
Backward secrecy	No	No	Yes
Electricity control flexibility	Inflexible	Flexible	Flexible

Table 3. Comparison of computational costs

Entity	Scheme [7]	Scheme [8]	Our scheme
User/User/User	$2T_e+2T_m$	$2T_e+T_m$	$3T_e$
BG/RAGW/RAGW	$3nT_p+2T_m$	$(n+2)T_p+T_m$	$(2n+1)T_e$
-/DGW/DGW	-	$(m+2)T_p+T_m$	$(2m+1)T_e$
CC/CC/CC	$3mT_p$	$2T_p$	$2T_e$

-: No entity
m: The number of residential area
n: The number of users in a residential area
T_e : The computational cost of an exponentiation operation in $\mathbb{Z}_{N^2}^*$
T_m : The computational cost of a multiplication operation in $\mathbb{G}_1$
T_p : The computational cost of a pairing operation

The comparisons of the computational costs of each user and CC are shown in **Fig. 6** and 7, respectively. From **Figs. 6** and **7**, it can be seen that the efficiency of our scheme for reducing the computational complexity of the CC is higher than that of scheme [7]. The computational cost of each user is almost same to that of scheme [8]. Since the system model of our scheme is same as that of scheme [8], we compare the computational cost of the DGW between our scheme and scheme [8]. **Fig. 8** shows the computational cost of DGW in scheme [8] and **Fig. 9** shows the computational cost of DGW in our scheme. Obviously, the computational cost of DGW in our scheme is lower than that of DGW in scheme [8].

The above analysis indicates that our scheme is more efficient in reducing computational cost than schemes [7-8].

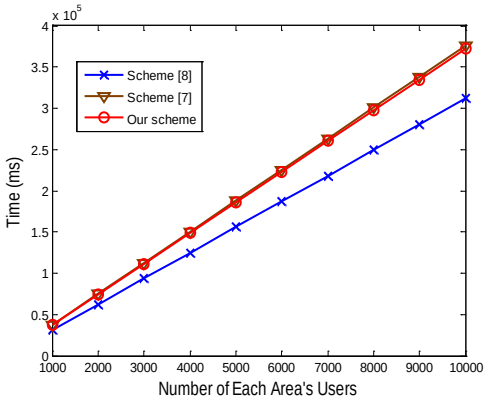

Fig. 6. Computational cost of each user.

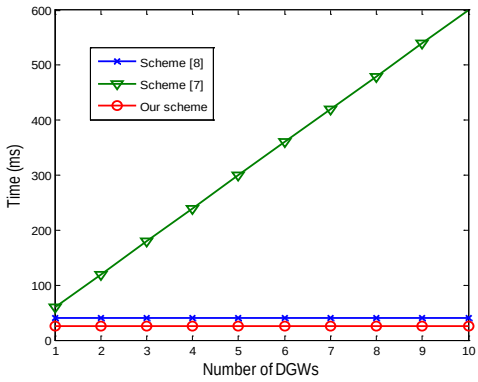

Fig. 7. Computational cost of CC.

7.3 Communication overhead

The communication overhead between the entities in system is described as follows:

1) Communication overhead between HANs and RAGW. In user electricity report generation phase, HAN user U_{ijk} sends encrypted electricity report $C_{ijk,w} \| \sigma_{ijk,w}$ to the $RAGW_{ij}$ in the RA. Since the electricity consumption is encrypted by Paillier cryptosystem, as shown in eqation $C_{ijk,w} = g^{d_{ijk,w}} \cdot r^N \bmod N^2$, the length $C_{ijk,w}$ is 2048 bits (If

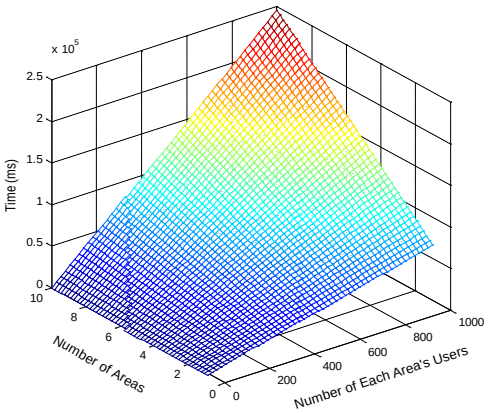

Fig. 8. Computational cost of DGW in scheme [8].

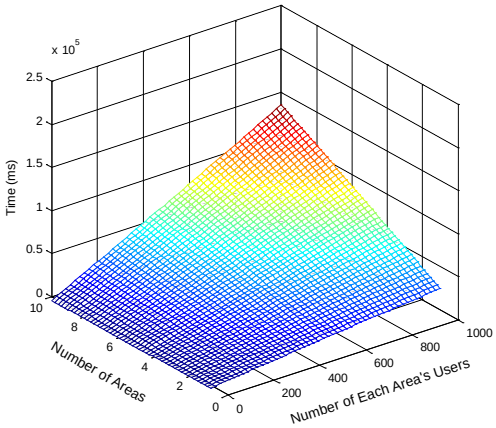

Fig. 9. Computational cost of DGW in our scheme.

choose $|N|=1024$). Let $|\mathbb{G}_1|=160$ bits, the length of signature is 160 bits. The communication overhead between HANs and RAGW is $2208*l*m*n$, where *l*, *m*, *n* denotes the number of DGW, RAGW, and HAN users, respectively.

2) Communication overhead between RAGW and DGW. After completing the signature, RAGW_j sends the fine-grained encrypted electricity report $C_{ij,w}\|\sigma_{ij,w}$ to the DGW_i in the district. So the communication overhead between RAGW and DGW is $2208*l*m$.

3) Communication overhead between DGW and CC. After completing the signature, DGW_i sends the coarse-grained encrypted electricity report $C_{i,w}\|\sigma_{i,w}$ to CC. So the communication overhead between RAGW and DGW is $2208*l$.

The compare of communication overheads is shown in **Table 4**.

Table 4. Comparison of communication overheads

	Scheme [8]	**Our scheme**
User to RAGW	$2308*l*m*n$	$2208*l*m*n$
RAGW to DGW	$2308*l*m$	$2208*l*m$
DGW to CC	$2308*l$	$2208*l$

From **Table 4**, it is easy to see that our scheme greatly reduces the communication overhead of between the entities compared to the related scheme.

8. Conclusion

In this paper, we propose a secure and fine-grained electricity consumption aggregation scheme. It realizes efficient and secure electricity consumption aggregation with the Paillier homomorphic encryption technology in the system model of two-level gateway topology. Since the proposed scheme can aggregate multiple users' electricity consumption from multiple residential areas with different granularities, the CC can achieve flexibly and effectively electricity regulation to the users of different residential areas. Security analysis demonstrates that the proposed scheme can realize privacy-preservation of users' sensitive

information and forward-backward secrecy of user's electricity consumption signature. Compare with other related schemes, our scheme is more secure and efficient. In the future work, we will consider the scheme's fault tolerance, and how to further reduce the computational cost and communication overhead of the scheme.

References

[1] United States Department of Energy, "The smart grid: an introduction," Jan. 2011. Article(CrossDef Link)

[2] H. He and J. Yan, "Cyber-physical attacks and defenses in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13-27, Nov. 2016. Article (CrossRef Link)

[3] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Computer Communications*, s 91-92, pp. 17-28, Oct. 2016. Article(CrossRef Link)

[4] J. Gao, Y. Xiao, J. Liu, W. Liang and C.L.P. Chen, "A survey of communication/networking in smart grids," *Future Generation Computer Systems*, vol. 28, no.2, pp. 391-404, Feb. 2012. Article(CrossRef Link)

[5] US Department of Commerce, NIST, "NIST framework and roadmap for smart grid interoperability standards, release 3.0," *NIST Special Publication*, 2014. Article(CrossRef Link)

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of Advances in Cryptology-EUROCRYPT 99*, pp. 223-238, May 2-6, 1999. Article(CrossRef Link)

[7] H. Li, X. Lin, H. Yang, X. Liang, R. Lu and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel & Distributed Systems*, vol. 25, no.8, pp. 2053-2064, Aug. 2014. Article(CrossRef Link)

[8] H. Shen, M. Zhang and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme and smart grids," *IEEE Transaction on Information Forensics and Security*, vol. 12, no.6, pp. 1369-1381, Jan. 2017. Article(CrossRef Link)

[9] X. Wang, Y. Mu and R. Chen, "An efficient privacy-preserving aggregation and billing protocol for smart grid," *Security & Communication Networks*, vol. 9, no.17, pp. 4536-4547, Nov. 2016. Articl(CrossRef Link)

[10] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 99, pp. 1-1, Oct. 2016. Article(CrossRef Link)

[11] C. Fan, S. Huang and Y. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no.1, pp. 666-675, Feb. 2014. Article(CrossDef Link)

[12] 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, Nov. 2015. Article(CrossDef Link)

[13] A. Abdallah and X. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1-1 Apr. 2016. Article(CrossDef Link)

[14] M. Abdalla and M. Bellare, "Increasing the lifetime of a key: A comparative analysis of the security of re-keying techniques," in *Proc. of Advances in Cryptology-ASIACRYPT 2000*, vol. 1976, no.7, pp. 546-559, Dec 3-7, 2000. Article(CrossDef Link)

[15] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in *Proc. of The 3th International Conference on Security in Communication Networks*, vol. 2576, pp. 241-256, Sep 11-13, 2002. Article(CrossDef Link)

[16] R. Canetti, S. Halevi and J. Katz, "A forward-secure public-key encryption scheme," *Journal of Cryptology*, vol. 20, no.3, pp. 265-294, Feb. 2007. Article(CrossDef Link)

[17] B. Libert, J. Quisquater and M. Yung, "Key evolution systems in untrusted update environments," *ACM Transactions on Information and System Security*, vol. 13, no.4, pp. 12-21, Dec. 2009. Article(CrossDef Link)
[18] D. Lin, C. I. Wang and D. J. Guan, "A forward-backward secure signature scheme," *Journal of Information Science & Engineering*, vol. 26, no.6, pp. 2319-2329, Nov. 2010. Article(CrossDef Link)
[19] S. M. Yen and Y. Zheng, "Weighted One-Way hash chain and its applications," in *Proc. of The 3th International workshop on Information Security (ISW 2000)*, vol. 1975, pp. 135-148, Dec 20-21, 2000. Article(CrossDef Link)
[20] Abdalla, Michel, and L. Reyzin, "A New Forward-Secure Digital Signature Scheme," in *Proc. of Advances in Cryptology-ASIACRYPT 2000*, vol. 20, pp. 116-129, Dec 3-7. 2000. Article(CrossDef Link)
[21] M. Bellare and S.K. Miner, "A forward-secure digital signature scheme," in *Proc. of Advances in Cryptology-CRYPTO'99*, pp. 431-448, Aug. 15-19, 1999. Article(CrossDef Link)
[22] T. W. Chim, S. M. Yiu, V. O. K. Li, L. C. K. Hui and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no.1, pp. 85-97, Jan/Feb. 2015. Article(CrossDef Link)
[23] C. Cheng, T. Jiang, Y. Liu, and M. Zhang, "Security analysis of a homomorphic signature scheme for network coding," *Security and Communication Networks*, vol. 8, no. 18, pp. 4053-4060, Aug. 2015. Article(CrossRef Link)
[24] Y. Liu, G. Liu, C. Cheng, Z. Xia, and J. Shen, "A privacy-preserving health data aggregation scheme," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 8, pp. 3852-3864, Aug. 2016. Article(CrossDef Link)
[25] S. He, W. Zeng, K. Xie, H. Yang, M. Lai and X. Su, "PPNC: Privacy preserving scheme for random linear network coding in smart grid," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1510-1532, Mar. 2017. Article(CrossDef Link)
[26] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors Journal*, vol. 16, no. 3, pp. 836–842, Feb. 2016. Article(CrossDef Link)
[27] Multiprecision integer and rational arithmetic c/c++ library. [Online]. Available: Article(CrossDef Link)
[28] B. Lynn.: PBC library. [Online]. Available: Article(CrossDef Link)

Gang Shen received the B.S. degree in electrical automation from Wuhan Institute of Chemical Technology, Wuhan, China, in 2002, and the M.S. degree in control theory and control engineering from School of Automation, Huazhong University of Science and Technology, Wuhan, China, in 2009. He is currently working toward his Ph.D. degree in transportation information engineering and control from the School of Automation, Wuhan University of Technology, Wuhan, China. His current research interests include cryptography, network security, and privacy preservation.

Yixin Su received the B.S. degree in process control from Wuhan Hydraulic & Electric University, Wuhan, China, in 1985, the M.S. degree in control theory and application from Institute of Automation, Southeast University, Nanjing, China, in 1988, the Ph.D. degree in mechanical manufacturing & automation from Huazhong University of Science and Technology, Wuhan, China, in 2006, respectively. He is currently a professor with the School of Automation, Wuhan University of Technology, Wuhan, China, and also with the deputy dean of the School of Automation, Wuhan University of Technology, Wuhan, China. His current research interests include intelligent control, system optimization and marine motion control.

Danhong Zhang received the B.S. degree in industrial electrification & automation from Wuhan Institute of Technology, Wuhan, China, and the M.S. degree in industrial automation from Wuhan Automotive Polytechnic University, Wuhan, China, in 1989 and 1998, respectively. She is currently a professor with the School of Automation, Wuhan University of Technology, Wuhan, China. Her current research interests include intelligent control theory and application, system optimization and HEV control.

Huajun Zhang received the B.S. degree in electrical engineering and M.S. degree in control theory and application from Wuhan University of Technology, China, in 2003 and 2006, and the Ph.D. degree in control theory and application from Huazhong University of Science and Technology, China, in 2010, respectively. He is an associate professor of electrical engineering at the School of Automation, Wuhan University of Technology, Wuhan, China. His current interests include adaptive control, system optimization and control of ocean vehicles.

Binyu Xiong (S' 2011 M'2016) is currently an assistant professor in School of Automation, Wuhan University of Technology, Wuhan China. He received the MSc. and Ph.D. degree in power engineering from Nanyang Technological University, Singapore in 2011 and 2016 respectively. His research interests include electrical and thermal modeling of batteries, battery state of charge estimation, large-scale energy storage systems, power electronics, and renewable energy generations.

Mingwu Zhang is a professor at School of Computer Sciences, Hubei University of Technology, Wuhan, China. He received his M.Sc. in Computer Science and Engineering from Hubei Polytechnic University in 2000 and the Ph.D. degree in South China Agric University, in 2009, respectively. From August 2010 to August 2012, he has been a JSPS postdoctoral fellow at Institute of Mathematics for Industry in Kyushu University. From June 2015 to June 2016, he is a senior visiting professor at School of Information and Computing Science, University of Wollongong. His research interests include cryptography technology for network and data security, secure computation and privacy preservation.