Enabling Fine-grained Access Control with Efficient Attribute Revocation and Policy Updating in Smart Grid

Hongwei Li [12], Dongxiao Liu [1], Khalid Alharbi[3], Shenmin Zhang [1], and Xiaodong Lin[3]
[1] School of Computer Science & Engineering, University of Electronic Science and Technology of China
Chengdu, 610054 – China
[e-mail: hongweili@uestc.edu.cn, haohhaha@gmail.com, 18200292562@163.com]
[2]State Key Laboratory of Information Security (Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093)
[3]Faculty of Business and Information Technology, University of Ontario Institute of Technology,
Oshawa, ON, L1H7K4 – Canada
[e-mail: Khalid.Alharbi@uoit.ca, xiaodong.lin@uoit.ca]

Received January 31, 2015; revised March 10, 2015; accepted March 20, 2015;
published April 30, 2015

Abstract

In smart grid, electricity consumption data may be handed over to a third party for various purposes. While government regulations and industry compliance prevent utility companies from improper or illegal sharing of their customers' electricity consumption data, there are some scenarios where it can be very useful. For example, it allows the consumers' data to be shared among various energy resources so the energy resources are able to analyze the data and adjust their operation to the actual power demand. However, it is crucial to protect sensitive electricity consumption data during the sharing process. In this paper, we propose a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid. Specifically, by introducing the concept of Third-party Auditor (TPA), the proposed FAC achieves efficient attribute revocation. Also, we design an efficient policy updating algorithm by outsourcing the computational task to a cloud server. Moreover, we give security analysis and conduct experiments to demonstrate that the FAC is both secure and efficient compared with existing ABE-based approaches.

Keywords: Smart grid, attribute-based encryption, attribute revocation, policy updating

This manuscript is an extended version based on a conference paper published in ICC 2014 (Sydney, Australia, June 9-14, 2014.)This work is supported by the National Natural Science Foundation of China under Grants 61472065, U1233108, and U1333127, the International Science and Technology Cooperation and Exchange Program of Sichuan Province, China under Grant2014HH0029, China Postdoctoral Science Foundation funded project under Grant 2014M552336, and State Key Laboratory of Information Security Open Foundation under Grant 2015-MS-02.

http://dx.doi.org/10.3837/tiis.2015.04.008 **ISSN : 1976-7277**

1. Introduction

Compared to the traditional power grid, smart gird integrates power and communication networks to achieve a two-way communication [1, 2]. Smart grid can improve the efficiency, sustainability and reliability between the energy producers and customers. As shown in **Fig. 1**, a general structure of smart grid consists of six logical domains [3-5]. Each one of the four (Bulk Generation, Transmission, Distribution and User) can generate, store and deliver electricity in two-way. Control center (CC) is the core component of the smart grid which can manage all the electricity and information movement of the whole system. Users of three types (Home Area Network (HAN), Building Area Network (BAN), Industrial Area Network (IAN)) are connected to the smart grid system by Smart Meters. And the Markets are where grid assets are bought and sold [6, 14].

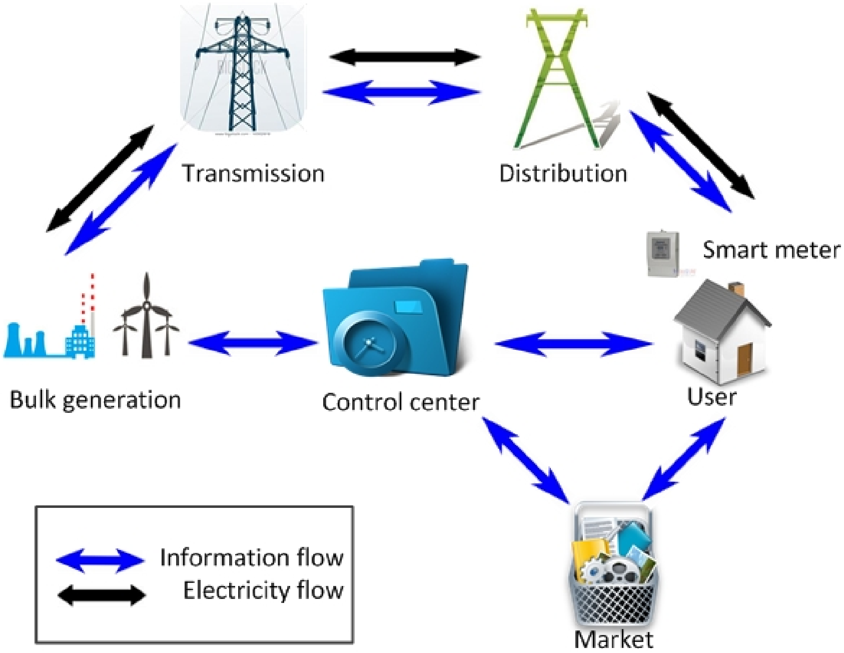

Fig. 1. General architecture of smart grid

The information flows in smart grid are of great significance [12, 13]. CC collects the generation and consumption data from the generators and the consumers. These data can help CC make decisions on system-level to improve the efficiency of the electricity flows. In smart grid, users' electricity data are collected by the smart meters and aggregated at the control center. Then, the control center intends to release the sensitive aggregated data to the markets that are very interested in them in a privacy-preserving manner. By analyzing the electricity usage information such as the air-conditioner or the television usage data in a specific period of time, the advertisers can obtain the time people usually watch TV in this area and then adjust their strategies. The television sellers can determine whether users prefer to watch videos online rather than watching televisions.

To handle the data release efficiently and securely, existing literature [7, 8] adopt the Attribute-based Encryption (ABE) technique to provide fine-grained access control over the sensitive data. For practical uses, the proposed scheme must support attribute revocation since the role of the markets may dynamically change in the system. Fadlullah et al. [7] introduce Key-policy ABE technique to achieve a targeted data broadcast in smart grid but do not take the problem of attribute revocation into considerations. Ruj et al. [8] utilize ciphertext-policy ABE for data release in smart grid. However, their attribute revocation method lacks efficiency since it requires updating all the ciphertexts that contain the revoked attribute. Moreover, the access policy of the sensitive data may need to be updated. A naïve way is that CC retrieves the data and re-computes the ciphertext, which may incur heavy computation and communication cost.

On addressing the above issues, we propose a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid in this paper.

Our Contributions. The contributions of this paper can be summarized as follows.

- First, we utilize CP-ABE technique [17] to achieve a fine-grained data access control in smart grid. And by leveraging Third-party Auditor [16], the FAC could support efficient and secure attribute revocation.
- Second, to meet the requirements for practical uses, we modify the policy updating algorithm in [23] for the access structure in the FAC. Moreover, by outsourcing most of the computation task to the cloud server, the policy updating algorithm is also efficient.
- Third, we give a thorough security analysis and demonstrate that the FAC can achieve confidentiality and privacy, fine-grained access control, collusion resistance, and secure attribution revocation and policy updating. Then, we conduct real experiments and show that the FAC is more efficient in terms of functionalities as well as computation and communication overhead compared with existing scheme [7] and [8].

Compared with the preliminary conference version [14] of this paper, this journal version studies dynamic access policy updating problem for the control center. Specifically, we present the policy updating algorithm for the access control structure in the FAC to make the FAC more suitable for practical uses. Moreover, we show the policy updating algorithm is secure and efficient by giving the analysis and evaluation of the new scheme.

Organization. The remainder of this paper is organized as follows. In Section 2, the system model, security requirements and design goals are formalized. We recall bilinear pairing and CP-ABE in Section 3. In Section 4, we propose our FAC scheme. Its security analysis and performance evaluation of the FAC are shown in Section 5 and Section 6, respectively. In Section 7, we present related works. Finally, we conclude this paper in Section 8.

2. System Model, Security requirements and Design goals

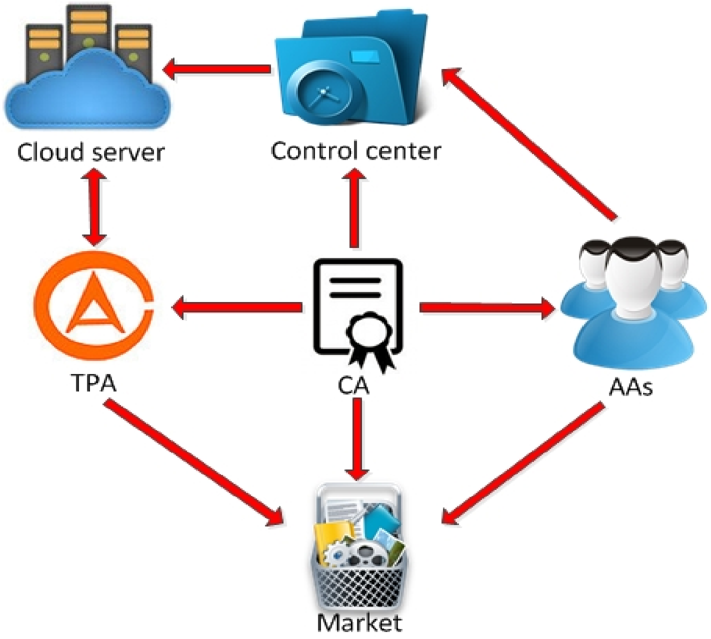

Fig. 2. System model

2.1 System Model

The FAC consists of the following six entities: Certificate Authority (CA), Control Center (CC), Markets, Third Party Auditor (TPA), Cloud Sever (CS), and Attribute Authorities (AAs).

In smart grid, there are two types of networks including power network and communication network. In this paper, we mainly focus on the information flow between the control center and market. Specifically, the user electricity data are collected by the smart meters and aggregated at the control center. Then, the control center intends to distribute the sensitive aggregated to the markets securely and efficiently. On addressing the above problem, we utilize the attribute-based encryption and third-party auditor technique to outsource the data to the cloud server. Therefore, we introduce some other entities including certificate authority, attribute authorities, cloud server and third-party auditor. Specifically, CA is a globally trusted certificate authority and may be audited by the government office. CA would initialize the system by setting up the parameters for AAs and authenticating the markets. AAs are responsible for the attribute key generation including public attribute key for CC and private attribute key for markets. Every attribute is associated with a single AA, but each AA can manage a set of attributes.

As shown in **Fig. 2**, to securely and efficiently distribute the electricity data to the markets, the system operates in the following steps. CC first obtains the public attribute keys from AAs. Then, CC defines the access policy for the different kinds of the aggregated user electricity data and encrypts them using public attribute keys before outsourcing them to CS. Markets may first register themselves in CA and obtain private attribute keys from the AAs according to their roles in the system. When markets intend to access the electricity data on the cloud server, they would ask TPA to check the legality of their identities to help the legal markets decrypt the data by generating a decryption Token.

When attribute revocation occurs and some of the market's attribute keys may need to be changed, CA and AAs would assign a new set of private keys to the market and update the associated information in TPA. And when CC intends to update the access policy, CC would only need to generate the update token and send it to CS. CS would do the updating job using the old access policies.

2.2 Security Requirements

In the FAC, the control center is the core component of the smart grid and is run by the government. Therefore, we assume it to be trusted. And we assume CA is also trusted, but we still need to prevent it from decrypting the data. AAs and TPA are curious but honest, i.e., they execute the task assigned by CA and never collude with markets to get the unauthorized data. It is reasonable since TPA and AAs are audited by government offices. CS is also curious but honest [9, 10]. Markets are dishonest and may collude to get access to the unauthorized data. Specifically, the security requirements in FAC cover the following four aspects [15].

- **Confidentiality and Privacy:** Since the aggregated electricity data contain sensitive information about the users, it should be kept secret from CS and unauthorized markets. Moreover, markets may want to keep their identities from being exposed to CS and AAs.
- **Fine-grained Access Control:** Markets may be assigned a set of attributes according to its role in the system. To efficiently distribute the aggregated data, the access control policy should be fine-grained. In specific, CC pre-defines the access policy and encrypts the data. The access policy should support both "AND" and "OR" gate. Only a market with correct market attribute keys that satisfy the policy embedded in the ciphertext can decrypt the data.
- **Collusion Resistance:** Since markets are not trusted in the system, two or more markets cannot combine their market attribute keys and get access to the data which they cannot access individually.
- **Secure Attribute Revocation and Policy Updating:** A market cannot use the revoked market attribute keys to decrypt the data which they should not get access to. Moreover, the policy updating algorithm should not leak any useful information to CS.

2.3 Design goals

In order to design an efficient and secure fine-grained data release scheme in smart grid, our design goals should focus on the following aspects:

- **Covering All the Security Requirements**: Under the security assumption introduced above, the proposed FAC should cover all the security requirements.
- **Efficient Decryption for Markets:** By using the token-based decryption method, the proposed FAC should achieve efficient decryption for markets.
- **Efficient Attribute Revocation:** By adopting the TPA technique, the proposed FAC should achieve efficient attribute revocation which incurs less cost than the existing scheme in computation and communication overhead.
- **Efficient Access Policy Updating:** By outsourcing the computational task of access policy updating from CC to CS, the proposed FAC should achieve efficient policy updating at CC.

3. Preliminaries

3.1 Bilinear Paring

Let$G$, G_T be two multiplicative cyclic groups of the same prime order q, and g be generator of group G. Suppose G and G_T are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : G \times G \rightarrow G_T$ such that $e\left(P_1^a, Q_1^b\right) = e(P_1, Q_1)^{ab} \in G_T$ for all $a, b \in Z_q^*$ and any $P_1, Q_2 \in G$. We can obtain more comprehensive descriptions of pairing technique through reference [18].

3.2 Ciphertext-Policy Attribute-based Encryption

In ciphertext policy attribute-based encryption (CP-ABE) [17], ciphertexts are created with an access structure (usually an access tree) which defines the access policy. A user can decrypt the data only if the attributes embedded in her attribute keys satisfy the access policy in the ciphertext. In CP-ABE, the encrypter holds the ultimate authority of the access policy [11].

4. Proposed Scheme

In the FAC, the electricity data are already collected by the smart meters and aggregated by the control center. Then, the control center could first encrypt the data and outsource the data to the cloud server to enjoy a flexible and efficient data access service. Markets who are interested in the aggregated data could connect to the cloud server and access to the data with their attribute keys. In this section, we propose our FAC, which consists of the following seven phases: System Initialization, Market Attribute Keys Generation, Encryption by CC, Auditing by TPA, Decryption by Market, Attribute Revocation and Access Policy Updating.

Table 1. Notations

Symbols	Meanings
x_i	global id of attribute i
$para$	system parameters
L_j	a set of attributesAA_jmanages
$SK_{x_i,j}$	secret attribute key for attribute $x_i \in L_i$
$PK_{x_i,j}$	public attribute key for attribute $x_i \in L_i$
v_m	market version number
GMK	global market key
LMK	local market key
MGK	market generation key
I_m	attributes that the market u_m includes
mak	market attribute key
In	set of row indexes
UK_{Data}	update key for policy updating

4.1 System Initialization

1) *CA Setup*

At the beginning of system initialization, CA selects a prime q, two cyclic groups G, G_T of prime order q, a generator g of G, a map $e: G \times G \rightarrow G_T$, two functions $H : \{0,1\}^* \rightarrow G$, $F : \{0,1\}^* \rightarrow Z_q$ and a secure symmetric encryption algorithm $Enc()$, e.g., AES. In addition, CA defines a dictionary for all the attributes of the system. For attribute i, CA generates a global attribute id x_i. Then CA chooses two random numbers $\beta, \gamma \in Z_q$ as the system master secret key and computes $e(g,g)^{\beta}, g^{\gamma}, e(g,g)^{\gamma}$. Finally, CA publishes the system parameters as:

$$Para = \{g, G, G_T, q, e, H, F, Enc(), e(g,g)^{\beta}, g^{\gamma}, e(g,g)^{\gamma}\} \tag{1}$$

2) *AA Setup*

CA distributes a set of attributes to each AA and makes sure that every two AAs do not manage the same attributes. Let L_j be the set of attributes that AA$_j$ manages. For each attribute $x_i \in L_j$, AA$_j$ chooses two random numbers $\alpha_{x_i}, \mathscr{y}_{x_i} \in Z_q$ as the secret attribute key:

$$SK_{x_i,j} = \{\alpha_{x_i}, \mathscr{y}_{x_i}\} \tag{2}$$

Then AA$_j$ computes the public attribute key for each attribute $x_i \in L_j$ as

$$PK_{x_i,j} = \{\, e(g,g)^{\alpha_{x_i}}, g^{\alpha_{x_i}}, g^{\mathscr{y}_{x_i}}\} \tag{3}$$

3) *Market Registration*

If a market is legal in the system, CA assigns a global market id u_m to it. Then CA chooses a random number $z_m \in Z_q$ and a random market version number $v_m \in Z_q$. And then CA generates a pair of global market key GMK and local market key LMK for the marketu_m as follows:

$$GMK = \{z_m, g^{\frac{1}{z_m}}\} \quad , LMK = g^{\frac{\beta}{z_m v_m}} \cdot g^{\frac{\gamma}{v_m}} \tag{4}$$

Next, CA sends theGMK, LMK to the market and$\{u_m, v_m\}$ to TPA secretly. In addition, CA computes the market generation key MGK as follows:

$$MGK = \{g^{\frac{1}{v_m}}, H(u_m)^{\frac{1}{v_m}}\} \tag{5}$$

CA publishes MGK to AAs.

4.2 Market Attribute Keys Generation

AAs assign a set of attributes I_m to this market according to its role. Then for each attribute $x_i \in I_m$, AAs generate the related market attribute key mak_{x_i,u_m}using the market's MGK as

$$mak_{x_i,u_m} = \{g^{\frac{\alpha_{x_i}}{v_m}} H(u_m)^{\frac{\mathscr{y}_{x_i}}{v_m}}, g^{\frac{F(u_m)\mathscr{y}_{x_i}}{v_m}}\} \tag{6}$$

Finally, AAs send the $maks$ to markets through a secure channel.

4.3 Encryption by CC

CC encrypts the aggregated electricity data, denoted as $Data$, by using a symmetric encryption key κ. The encrypted data is represented as $Enc_\kappa(Data)$. Then CC constructs the Linear Secret-Sharing Schemes (LSSS) matrix $\mathcal{R}$ according to the pre-defined access policy [19]. Each row of $\mathcal{R}$ is associated with one attribute that is involved in the access policy. Then CC defines a map π, mapping the row of matrix $\mathcal{R}$ to the attributes. And then CC encrypts the symmetric key κ using the related public attribute keys and system parameters as follows:

Step 1: CC chooses a random number $s \in Z_q$ and a random vector $v \in Z_q^l$ with s as its first entry, where l represents the number of the attributes involved in the $\mathcal{R}$ and is equal to the number of rows in the $\mathcal{R}$.

Step 2: For each row of $\mathcal{R}$, CC computes $\lambda_x = \mathcal{R}_x \cdot v$, where $\mathcal{R}_x$ is the x^{th} row of the matrix $\mathcal{R}$. Then CC chooses a random vector $\omega \in Z_q^l$ with 0 as its first entry and computes $\omega_x = \mathcal{R}_x \cdot \omega$.

Step 3: For each row of $\mathcal{R}$, CC chooses a random number $k_x \in Z_q$ and computes the ciphertext as follows:

$$\begin{gathered} C = \kappa e(g,g)^{\beta s} \\ C' = g^s \\ C_{1,x} = e(g,g)^{\gamma\lambda_x} e(g,g)^{\alpha_{\pi(x)} k_x}, \forall x \\ C_{2,x} = g^{k_x}, \forall x \\ C_{3,x} = g^{\mathscr{y}_{\pi(x)} k_x} g^{\omega_x}, \forall x \end{gathered} \tag{7}$$

where $\pi(x)$ maps the x^{th} row of $\mathcal{R}$ to attribute x_i.

Step 4: The ciphertext Cph is as follows:

$$Cph = \{\mathcal{R}, \pi, C, C', \{C_{1,x}, C_{2,x}, C_{3,x}, \forall x\}\} \tag{8}$$

Finally, CC sends the $CT = \{Enc_\kappa(Data), Cph\}$ to CS.

4.4 Auditing by TPA

All registered markets can query any interested encrypted data from CS. However, only if a market's attributes satisfy the access policy embedded in the ciphertext and the market attribute keys $maks$ contain the right market version number v_m, the market u_m can decrypt the ciphertext with the help of TPA. Specifically, the Auditing by TPA phase consists of the following four steps:

Step1: The market u_m sends its market attribute keys $maks$ and local market key LMK to TPA. TPA firstly checks the validity of $maks$ by using the market version number v_m which is generated in the Market Registration phase. TPA checks the following equation.

$$(g^{\frac{F(u_m)\mathscr{y}_{x_i}}{v_m}})^{v_m} = (g^{\mathscr{y}_{x_i}})^{F(u_m)} \tag{9}$$

Step 2: If equation (9) holds, TPA computes the set of attributes $\{\pi(x): x \in X\} \cap I_m$, where I_m and X represent the attributes that the market u_m includes and the set of rows of LSSS matrix $\mathcal{R}$ in ciphertext CT, respectively. For these attributes, TPA checks if there is a subset X' of them in which (1, 0, 0…, 0) is their linear combination. If yes, it computes a set of $c_x \in Z_q$ such that $\sum_{x \in X'} c_x \mathcal{R}_x = (1,\ 0, 0 \cdots, 0)$, where $\mathcal{R}_x$ represents the x^{th} row of $\mathcal{R}$. Otherwise, the market's attributes do not satisfy the access policy of ciphertext CT and decryption is impossible.

Step 3: TPA computes the $dec(x)$ for each x as follows:

$$dec(x) = \frac{C_{1,x} e(H(u_m), C_{3,x})}{e(\left(g^{\frac{\alpha_{x_i}}{v_m}} (H(u_m))^{\frac{y_{x_i}}{v_m}}\right)^{v_m}, C_{2,x})}, \forall x \in X' \tag{10}$$

$$= e(g,g)^{\gamma \lambda_x} e(H(u_m), g)^{\omega_x}$$

Step 4: According to reference [17], $\sum_{x \in X'} \lambda_x c_x = s$ and $\sum_{x \in X'} \omega_x c_x = 0$. TPA computes $Token$ as

$$Token = \frac{e(C', LMK^{v_m})}{\prod_{x \in X'} \left(dec(x)\right)^{c_x}}$$

$$= \frac{e(g^s, (g^{\frac{\beta}{z_m v_m}} \cdot g^{\frac{\gamma}{v_m}})^{v_m})}{\prod_{x \in X'} (e(g,g)^{\gamma \lambda_x} e(H(u_m), g)^{\omega_x})^{c_x}} \tag{11}$$

$$= \frac{e(g,g)^{\frac{\beta s}{z_m}} e(g,g)^{\gamma s}}{e(g,g)^{\gamma \sum_{x \in X'} \lambda_x c_x} e(H(u_m), g)^{\sum_{x \in X'} \omega_x c_x}}$$

$$= e(g,g)^{\frac{\beta s}{z_m}}$$

4.5 Decryption by Market

Upon receiving the $Token$, the market u_m can simply decrypt the ciphertext C to get the symmetric key κ by using its GMK as

$$\kappa = C / Token^{z_m} \tag{12}$$

Then market u_m can use the symmetric key κ to further decrypt the encrypted data $Enc_\kappa(Data)$.

4.6 Attribute Revocation

When a market's role has been changed and some of its attributes are revoked, AAs need to re-compute a set of $maks$ for the market. Firstly, CA chooses a new random market version number v_m' and secretly sends $\{u_m, v_m'\}$to TPA. Then, CA computes the new local market key as:

$$LMK' = g^{\frac{\beta}{z_m v'_m}} \cdot g^{\frac{\gamma}{v'_m}} \tag{13}$$

and sends it to the market. And then CA computes the market generation key as:

$$MGK' = \{g^{\frac{1}{v'_m}}, H(u_m)^{\frac{1}{v'_m}}\} \tag{14}$$

and publishes $MGK'$to AAs. Finally, AAs re-compute the new mak for each non-revoked attribute of market $u_m$using the market's new MGK' as

$$mak_{x_i,u_m} = \{g^{\frac{\alpha_{x_i}}{v'_m}} H(u_m)^{\frac{y_{x_i}}{v'_m}}, g^{\frac{F(u_m) y_{x_i}}{v'_m}}\} \tag{15}$$

Thus, the revoked market attribute keys are invalid for its outdate market version number v_m. TPA cannot compute the $Token$ for the market if it uses the revoked market attribute keys.

4.7 Access Policy Updating

In this subsection, we leverage the policy updating algorithm in [23] to achieve efficient updating operation. Specifically, when CC finds the access policy defined in LSSS [19] matrix is changed, it only needs to run the update key generation algorithm to construct the update keys and send them to CS. The update key generation algorithm is defined as follows. **Update Key Generation:** The update key generation algorithm $UKGen$ takes asinputs the old secret s, the previous access policy $(\mathcal{R}, \pi)$ with the previous random vector v, ω, and the new one $(\mathcal{R}', \pi')$, where l' represents the number of the attributes involved in the new access policy $\mathcal{R}'$ and π' represents the new map mapping the rows of $\mathcal{R}'$to the associated attributes. Since π and π' are non-injective, we define $num_{\pi(x),\mathcal{R}}$ and $num_{\pi(x),\mathcal{R}'}$ as the number of attribute $\pi(x)$ in $\mathcal{R}$ and $\mathcal{R}'$, respectively.

Step 1: CC runs the $PolicyCompare$ algorithm to compare the new policy $(\mathcal{R}', \pi')$ with the previous one $(\mathcal{R}, \pi)$ as follows.

```
Algorithm   $PolicyCompare$
Input:      previous policy $(\mathcal{R}, \pi)$ with $l \times n$ matrix
Output:     $In_{1,\mathcal{R}'}$, $In_{2,\mathcal{R}'}$, $In_{3,\mathcal{R}'}$ ⊳ three subsets of row indexes in $\mathcal{R}'$
            $In_{\mathcal{R}} \leftarrow$ index set of rows in $\mathcal{R}$
            for $y = 1$ to $l'$ do
            if $\pi'(y)$ in $\mathcal{R}$ then
            if $In_{\mathcal{R}} != \emptyset \ \& \ \exists x \in In_{\mathcal{R}}\ s.t.\ \pi(x) == \pi'(y)$ then
                add $(y, x)$ into $In_{1,\mathcal{R}'}$
            delete $x$ from $In_{\mathcal{R}}$
            else
                find any $x \in [1, l]\ s.t.\ \pi(x) == \pi'(y)$
                add $(y, x)$ into $In_{2,\mathcal{R}'}$
            end if
            else
              add $(y, 0)$ into $In_{3,\mathcal{R}'}$
```

```
        end if
        end for
```

Step 2: Then CC obtains three sets of row indexes $In_{1,\mathcal{R}'}$, $In_{2,\mathcal{R}'}$, $In_{3,\mathcal{R}'}$ of $\mathcal{R}'$, where $In_{1,\mathcal{R}'}$ and $In_{2,\mathcal{R}'}$ represent the set of row indexes y of $\mathcal{R}'$ such that $\pi'(y)$ exists in $\mathcal{R}$. Moreover, $L_{2,\mathcal{R}'}$ will include those exceeding $num_{\pi'(x),\mathcal{R}'} - num_{\pi'(x),\mathcal{R}}$ indexes y, If $num_{\pi'(x),\mathcal{R}'} \geq num_{\pi'(x),\mathcal{R}}$. $In_{3,\mathcal{R}'}$ represents the set of indexes y such that $\pi'(y)$ is a new attribute. Let $In_{\mathcal{R}} = \{1, \cdots, l\}$ be the index set of the rows of $\mathcal{R}$. Further, CC chooses two new random vectors $v', \omega' \in Z_q^{l'}$ with the old secretsand 0 as its first entry, respectively and computes $\lambda'_x = \mathcal{R}'_x \cdot v'$and $\omega'_x = \mathcal{R}'_y \cdot \omega'$, where $\mathcal{R}'_y$ represents they^{th} row of new LSSS matrix $\mathcal{R}'$.

Step 3: CC computes the update key for each type of index$y \in [1, l']$. Specifically, they could be divided into three types. If $(y, x) \in In_{1,\mathcal{R}'}$, it is Type1; If $(y, x) \in In_{2,\mathcal{R}'}$, it is Type 2; If $(y, x) \in In_{3,\mathcal{R}'}$, it is Type 3..

For Type 1, CC computes the update key as follows:

$$UK = (UK^1 = g^{\gamma(\lambda'_y - \lambda_x)}, UK^2 = g^{\omega'_y - \omega_x}) \tag{16}$$

And set s$k'_y = k_x$.

For Type 2, CC first chooses random numbers $k'_y, a_y \in Z_q$ and computes the update key as follows:

$$UK = (a_y, UK^1 = g^{\gamma(\lambda'_y - a_y \lambda_x)}, UK^2 = g^{\omega'_y - a_y \omega_x}) \tag{17}$$

For Type 3, CC chooses a number $k'_y \in Z_q$, where $k'_y = a_y k_x$ and computes the update key as follows:

$$UK = (UK^1 = g^{\gamma \lambda'_y} \cdot g^{\alpha_{\pi'(y)} k'_y}, UK^2 = g^{k'_y}, UK^3 = g^{\mathcal{Y}_{\pi'(y)} k'_y} g^{\omega'_y}) \tag{18}$$

Step 4: The update key UK_{Data} is constructed as

$$UK_{Data} = ((Type\ 1, \{UK\}_{(y,x) \in In_{1,\mathcal{R}'}}), \tag{19}$$

$$(Type\ 2, \{UK\}_{(y,x) \in In_{2,\mathcal{R}'}}),\ (Type\ 3, \{UK\}_{(y,x) \in In_{3,\mathcal{R}'}}))$$

Then, CC sends the update key UK_{Data} to CS.

Next, upon receiving the update key UK_{Data}, CS will update the ciphertext from the previous access policy to the new policy as follows:

For Type 1, CS updates the ciphertext as

$$C'_{1,y} = C_{1,x} \cdot e(g, UK^1) = e(g,g)^{\gamma \lambda'_y} \cdot e(g,g)^{\alpha_{\pi'(y)} k'_y} \tag{20}$$

$$C'_{2,y} = C_{2,x}$$

$$C'_{3,y} = C_{3,x} \cdot UK^2 = g^{\mathcal{Y}_{\pi'(y)} k'_y} \cdot g^{\omega'_y}$$

where $k'_y = k_x$.

For Type2, CS updates the ciphertext as

$$C'_{1,y} = (C_{1,x})^{a_y} \cdot e(g, UK^1) = e(g,g)^{\gamma \lambda'_y} \cdot e(g,g)^{\alpha_{\pi'(y)} k'_y} \tag{21}$$

$$C'_{2,y} = (C_{2,x})^{a_y} = g^{k'_y}$$
$$C'_{3,y} = (C_{3,x})^{a_y} \cdot UK^2 = g^{\mathcal{Y}_{\pi'(y)} k'_y} \cdot g^{\omega'_y}$$

where $k'_y = a_y k_x$.

For Type3, CS updates the ciphertext component as

$$C'_{1,y} = e(g, UK^1) = e(g,g)^{\gamma\lambda'_y} \cdot e(g,g)^{\alpha_{\pi'(y)} k'_y} \tag{22}$$
$$C'_{2,y} = UK^2 = g^{k'_y}$$
$$C'_{3,y} = UK^3 = g^{\mathcal{Y}_{\pi'(y)} k'_y} \cdot g^{\omega'_y}$$

The ciphertext Cph' is as follows:

$$C' = \{\mathcal{R}', \pi', C, C', \{C'_{1,y}, C'_{2,y}, C'_{3,y}, \forall y \in [1, l']\}\} \tag{23}$$

Finally, CS changes the CT as $CT' = \{Enc_\kappa(Data), Cph'\}$

5. Security Analysis

Given the assumptions presented in Section 2, we analyze the security properties of the FAC. Specifically, our analysis focuses on how the FAC could achieve confidentiality and privacy, fine-grained access control, collusion resistance, and secure attribute revocation and policy updating.

5.1 Confidentiality and Privacy

The aggregated user electricity data are first encrypted using the symmetric encryption method. As long as the symmetric key is well kept and distributed, the confidentiality of the data would be well preserved. Note that, CS cannot decrypt the data since it does not know the market attribute keys kept by markets and market version number v_m kept by TPA. In addition, though TPA does much decryption for the markets, it still cannot get access to the electricity data without the global market key GMK. That is, only a market with valid attributes that satisfy the access policy can decrypt the ciphertext. In the system, each AA is only in charge of one kind of attribute. That is, markets obtain their market attribute keys from different AAs and each AA only knows part of their attributes. Thus, single AA cannot recover all the markets' attribute information. Moreover, markets communicate with AAs or TPA using their global market id, i.e., only CA knows markets' true identities. Therefore, the confidentiality of the data and markets' privacy are well protected in the FAC.

5.2 Find-grained Access Control

CC firstly defines the access policy and uses the corresponding public attribute keys to encrypt the symmetric key that is used to encrypt the electricity data before outsourcing it to CS. The access policy defined in LSSS [19] matrix supports complex Boolean operations including both AND and OR gate. For more details about the construction of the LSSS matrix, we direct the readers to reference [17]. That is, the FAC can achieve a fine-grained access control.

5.3 Collusion Resistance

In the FAC, markets are dishonest and may intend to combine their market attribute keys to get access to the electricity data which they cannot get access individually. To address this problem, AAs would generate market attribute keys with a market's identity and the market version number v_m. If two or more markets combine their market attribute keys to satisfy the ciphertext's access policy, $(g^{\frac{F(u_m)y_{x_i}}{v_m}})^{v_m'} \neq (g^{y_{x_i}})^{F(u_m)}$ in the Auditing by TPA phase. Therefore, TPA would not compute $Token$ for the colluding markets. Thus, the proposed FAC scheme is collusion-resistant.

5.4 Secure Attribute Revocation and Policy Updating

When attribute revocation happens and some of the market's attribute are revoked, CA would choose a new random market version number v_m' and sends it to TPA. Then AAs re-calculate the market attribute keys for the non-revoked attributes of the market. We assume that a market tries to decrypt the ciphertext using the revoked market attribute key. Unfortunately, in the auditing by TPA phase, $(g^{\frac{F(u_m)y_{x_i}}{v_m}})^{v_m'} \neq (g^{y_{x_i}})^{F(u_m)}$ and $(mak_{x_i,u_m})^{v_m'}$ cannot be computed correctly since the revoked market attribute key does not contain the true version number v_m'. During the policy updating operations, CC would first obtain the old access policy and then compute the updating token using public parameters. The aim of this token-based policy updating algorithm is to make full use of the ciphertext on the cloud server to reduce the computation cost in CC. That is, all the information leaked in the policy updating phase to the CS is some relationship between the old policies and the new policies. It is acceptable since knowing this does not mean that CS could further pry into the encrypted data. That is, the FAC could achieve secure attribute revocation and policy updating.

6. Performance Evaluation

In this section, we evaluate the performance of FAC in terms of functionality as well as computation and communication overhead.

Table 2. Notations

Symbols	Meanings
T_e	time for an exponentiation operation in G
T_{et}	time for an exponentiation operation in G_T
T_p	time for a pairing operation
N_c	number of attributes in a ciphertext
N_m	number of markets
$N_{ct,atr(i)}$	number of ciphertexts that contain attribute x_i
$N_{m,atr}$	number of attributes a market includes
$N_{m,atr(i)}$	number of non-revoked market including x_i
$N_{atr,j}$	number of attributes AA_j manages
N_i'	number of attributes of $Typei$ in update ciphertext

6.1 Functionality

As shown in **Table 3**, we compare functionalities among the FAC, Ruj's scheme [8] and Faslullah's scheme [7]. Specifically, all the above schemes achieve access control over the outsourced data. However, Faslullah's scheme [7] cannot achieve attribute revocation and policy updating while Ruj's scheme [8] only supports attribute revocation. The FAC could achieve all the above functionalities.

Table 3. Comparison of Functionalities

	Fadlullah's [7]	Ruj's [8]	FAC
Access Control	√	√	√
Attribute Revocation		√	√
Policy Updating			√

Further, we would compare Ruj's and the FAC in terms of computation and communication overhead as follows.

6.2 Computation Overhead

In this subsection, we focus on the computation overhead of the FAC and compare it with Ruj's scheme [8]. Since the performance is mainly affected by the time cost of exponentiation operations in G, exponentiation operation in G_T and pairing operation, we ignore the other operations. And we give the notations of symbols that are used in this subsection in **Table 2**.

As for the data encryption, time cost of the FAC and Ruj's scheme [8] are almost the same, which are $(2N_c+1)T_{et}+(3N_c+1)T_e$ in the FAC and $2N_cT_{et}+2N_cT_e$ in [8], respectively. In the Decryption by Market phase, since most of the decryption computation are moved to TPA, the market u_m only needs to perform an exponentiation operation in G_T to decrypt the decryption token, resulting in T_{et} time cost in the FAC. In Ruj's scheme, the market needs to do all the decryption tasks, and the computation overhead is $(2N_c+1)T_p+5N_cT_{et}$ [8].

In the Attribute Revocation phase, when one of the market's attributes is revoked, FAC only requires to re-compute a set of market attribute keys $maks$ and local market key LMK for the non-revoked attributes of the market. That is, the computation overhead is $3(N_{m,atr}T_e+T_e)$. However, in Ruj's scheme which requires CS to update every ciphertext that contains the revoked attribute, the computation overhead is $3N_{ct,atr(i)}T_{et}$.

In the policy updating phase, CC only needs to compute the update key for each type rather than re-compute the ciphertext. For Type 1, CC needs $2N_1'T_e$ time; For Type 2, CC needs $2N_2'T_e$; For Type 3, CC needs $5N_3'T_e$ time. The operations that cost most time are moved from CC to CS. Compared with the time cost for re-computing the ciphertext that cost $(2N_c+1)T_{et}+(3N_c+1)T_e$, this token-based updating algorithm could significantly reduce the computation overhead of CC, especially when the new access policy is little different from the old one and CS could fully make use of the previous ciphertext. The comparison of computation overhead is shown in **Table 4**.

Moreover, we conduct simulation experiments on a 2.53Hz-processor, 4GB memory computing machine with MIRACL library [20] to study the execution time. In the FAC, we assume that market can include at most 20 attributes. That is, $N_{m,atr}=20$. As for encryption phase shown in **Fig. 3**, the FAC achieves almost the same cost compared with

Ruj's. This is reasonable since the encryption is only required once. The computation overhead of Decryption and Revocation of FAC and Ruj's is shown in **Fig. 4** and **Fig. 5**. As we can see, the computation overhead for Decryption and Revocation in Ruj's scheme linearly increase while they are constant in FAC. Then, we show the execution time of the policy updating phase in **Fig. 6**. We denote $\mathrm{k} = \frac{N_3'}{N_1'+N_2'+N_3'}$. As we can see, updating operation for all the three types incurs less computation overhead compared with re-computing the ciphertext.

Table 4. Comparison of Computation overhead

	Ruj's [8]	FAC
Encryption	$2N_cT_{et} + 2N_cT_e$	$(2N_c + 1)T_{et} + (3N_c + 1)T_e$
Decryption	$(2N_c + 1)T_p + 5N_cT_{et}$	T_{et}
Revocation	$3N_{ct,atr(i)}T_{et}$	$3(N_{m,atr}T_e + T_e)$
Policy Updating	$2N_cT_{et} + 2N_cT_e$	$2N_1'T_e$+$2N_2'T_e$+$5N_3'T_e$

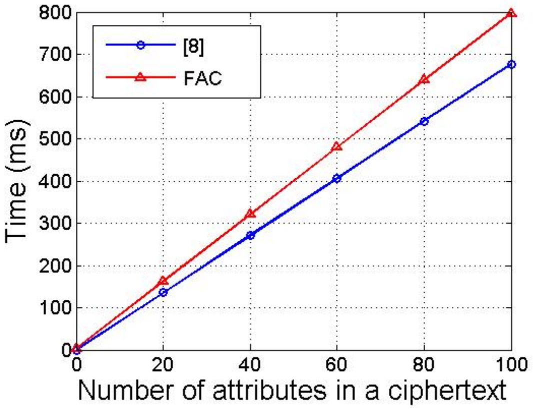

Fig. 3. Comparison of computation overhead for encryption

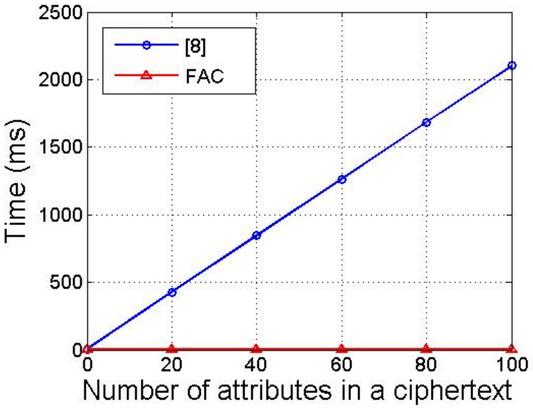

Fig. 4. Comparison of computation overhead for decryption

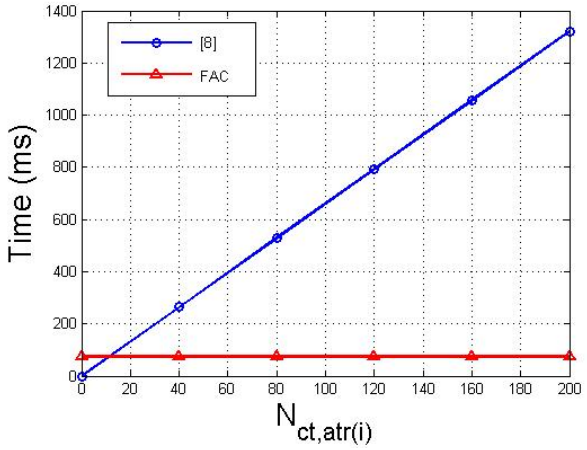

Fig. 5. Comparison of computation overhead for revocation

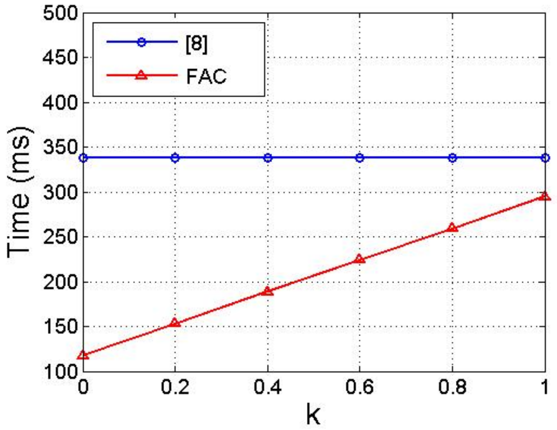

Fig. 6. Comparison of computation overhead for policy updating (k $= \frac{N'_3}{N'_1+N'_2+N'_3}$)

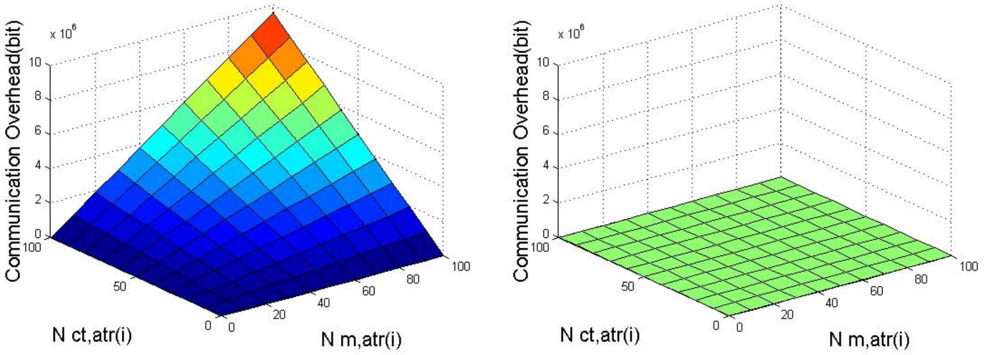

Fig. 7. Comparison of communication overhead for attribute revocation

6.3 Communication Overhead

In this subsection, we mainly focus on the communication overhead of the attribute revocation. When one of the market's attributes is revoked, the FAC only requires AAs to re-compute the market attribute keys for the market and send the keys to it, resulting in at most $(2N_{m,atr}+1)|G|$ communication overhead. In Ruj's scheme, it requires the CS to send all the ciphertexts that contain the revoked attribute to every non-revoked user which includes the revoked attribute, which incurs $\left(N_{ct,atr(i)}N_{m,atr(i)}+1\right)|G_T|$ size of transmitted messages.

If we choose a 160-bit G, and 960-bit G_T with embedded degree 6 [20], we can get the comparison of communication overhead between FAC and Ruj's as shown in **Fig. 7**. As we can see, the communication overhead in the FAC is constant while it is lineally increasing in Ruj's scheme.

7. Related Works

Much research effort has been directed to the security of smart grid recently. Li et.al. [1] propose an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid, which employs a homomorphic encryption to achieve privacy-preserving demand aggregation and efficient response. Yang et.al. [13] propose a ranked range query scheme in smart grid auction market, which can support both range query and ranked search.

Attribute-based encryption (ABE) is a promising technique that can achieve fine-grained access control of the encrypted data. The first ABE scheme is introduced by Sahai and Waters [21]. Then, Goyal et al. [22] classify ABE into two new forms Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, the attribute key is generated with access control policy and the ciphertext is associated with attributes. While in CP-ABE, the ciphertext is created with access policy. Later Lewko and Waters propose a multi-authority CP-ABE scheme [17]. However their work does not consider the attribute revocation and the policy updating problem. Yu et.al. [24] propose a secure, scalable, and fine-grained data access control scheme in cloud computing by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Yuan et.al. [25] propose a secure and constant cost public cloud storage auditing scheme with deduplication.

Some research works based on ABE technique have been directed to achieve access control in smart grid. Fadlullah et al. [7] utilize KP-ABE technique to achieve targeted broadcast in smart grid. But their scheme does not consider the revocation problem. Based on Lewko and Water' ABE scheme [17], Ruj et al. propose an access control infrastructure with revocation for smart grid [8]. However, in their scheme, attribute revocation incurs a heavy computation and communication overhead since it requires updating all the ciphertexts which contain the revoked attribute and sending them to every non-revoked user. Moreover, both the above schemes do not consider the policy updating problem. Yang et.al. [23] propose an efficient access control scheme with dynamic policy updating, which outsources the updating work to the cloud and supports different types of access policies.

8. Conclusion

In this paper, we proposed a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid. The proposed FAC is more suitable for practical access control issues since it supports dynamic operations. Moreover, we gave thorough security analysis and demonstrated that the FAC can achieve high level security guarantees. In addition, performance evaluation and analysis show that the FAC is more efficient compared with the existing schemes through comprehensive experiments. For the future work, we would explore privacy-preserving data aggregation problem in smart grid.

References

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

[2] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An efficient merkle tree based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no.2, pp. 655 - 663, 2014. Article (CrossRef Link)

[3] H. Li, X. Liang, R. Lu, X. Lin, X. Shen, "Edr: An efficient demand response scheme for achieving forward secrecy in smart grid," in *Proc. of GLOBECOM*, pp. 929-934, 2012. Article (CrossRef Link)

[4] H. Liang, B. Choi, W. Zhuang, X. Shen, "Towards optimal energy store-carry-and-deliver for phevs via v2g system," in *Proc. of INFOCOM*, pp. 167-1682, 2012. Article (CrossRef Link)

[5] H. Liang, B. Choi, A. Abdrabou, W. Zhuang, X. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE journal on Selected Areas in communications*, vol. 30, no. 6, pp. 1061-1074, 2012. Article (CrossRef Link)

[6] J. Liu, Y. Xiao, S. Li, W. Liang, C. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 981-997, 2012. Article (CrossRef Link)

[7] Z. M. Fadlullah, N. Kato, R. Lu, X. Shen, Y. Nozaki, "Toward secure targeted broadcast in smart grids," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 150-156, 2012. Article (CrossRef Link)

[8] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 196-205, 2013. Article (CrossRef Link)

[9] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, "Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost," in *Proc. of GLOBECOM*, pp. 775-780, 2014. Article (CrossRef Link)

[10] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, 2015. Article (CrossRef Link)

[11] H. Li, D. Liu, Y. Dai， T. H. Luan, and X. S. Shen, "Enabling Efficient Multi-keyword Ranked Search over Encrypted Cloud Data through Blind Storage," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 127-138, 2015. Article (CrossRef Link)

[12] H. Li, Y. Yang, M. Wen, H. Luo, and R. Lu, "EMRQ: An Efficient Multi-keyword Range Query Scheme in Smart Grid Auction Market," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 11, pp. 3937- 3954, 2014. Article (CrossRef Link)

[13] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving Ranked Range Query in Smart Grid Auction Market," in *Proc. of ICC*, Sydney, Australia, pp. 951-956, 2014. Article (CrossRef Link)

[14] D. Liu, H. Li, Y. Yang, and H. Yang, "Achieving Multi-Authority Access Control with Efficient Attribute Revocation in Smart Grid," in *Proc. of ICC*, pp. 634-639, 2014. Article (CrossRef Link)

[15] H. Li, Y. Dai, L. Tian, H. Yang, "Identity-Based Authentication for Cloud Computing," *Lecture*

Notes of Computer Science (LNCS), vol. 5931, 157-166, 2009. Article (CrossRef Link)

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. of INFOCOM*, pp. 1-9, 2010. Article (CrossRef Link)

[17] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. of EUROCRYPT*, pp. 568-588, 2011. Article (CrossRef Link)

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO*, Springer, pp. 213-229, 2001. Article (CrossRef Link)

[19] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. of PKC*, Springer, pp. 53-70, 2011. Article (CrossRef Link)

[20] "Miracl cryptographic sdk," Article (CrossRef Link)

[21] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT*, Springer, pp. 457–473, 2005. Article (CrossRef Link)

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of the 13th ACM conference on Computer and communications security*. ACM, pp. 89-98, 2006. Article (CrossRef Link)

[23] K. Yang, X. Jia, K. Ren, R. Xie and L. Huang, "Enabling efficient access control with dynamic policy updating for big data in the cloud," in *Proc. of INFOCOM*, pp. 2013-2021, 2014. Article (CrossRef Link)

[24] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. of INFOCOM*, pp. 1-9, 2014. Article (CrossRef Link)

[25] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 145-153, 2013. Article (CrossRef Link)

Hongwei Li received his M.S. degree in Computer Application from Southwest Jiaotong University (SWJTU) and Ph.D. degree in Computer Software and Theory from University of Electronic Science and Technology of China (UESTC) in 2004 and 2008 respectively. From 2011 to 2012, he worked as a Postdoctoral Fellow at University of Waterloo, Canada. Currently, he is an associate professor at the School of Computer Science and Engineering, UESTC, China. His research interests include cryptography, and the secure smart grid. Dr. Li serves as the Associate Editor of Peer-to-Peer Networking and Applications, the Guest Editor for Peer-to-Peer Networking and Applications Special Issue on Security and Privacy of P2P Networks in Emerging Smart City. He also serves on the technical program committees for many international conferences such as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE WCNC, etc. He is a member of IEEE, a member of China Computer Federation and a member of China Association for Cryptologic Research.

Dongxiao Liu received the B.S. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2013, where he is currently pursuing the master's degree with the School of Computer Science and Engineering. He serves as a reviewer of Peer-to-Peer Networking and Application. His research interests include cryptography, cloud computing security, and the secure smart grid.

Khalid Nawaf Alharbi received the B.Sc. degree in Mathematics, Saudi Arabia, in 1999 and the Master of Information Technology Security (MITS) from University of Ontario Institute of Technology (UOIT), Canada, in 2012. He is an instructor at Northern Border University, Saudi Arabia and is currently working toward a Ph.D. degree in Computer Science, University of Ontario Institute of Technology (UOIT), Canada. His research interests include applied cryptography, and security and privacy issues in web applications, cloud computing, mobile social networks, and smart grid.

Shenmin Zhang is currently an undergraduate of the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, and will receive the B.S. degree in 2015. Her interests include cryptography, cloud computing security and outsourcing computation.

Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an associate professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), and IEEE International Conference on Communications (ICC 2007). He is a senior member of the IEEE.