Protecting User Privacy Based on Secret Sharing with Fault Tolerance for Big Data in Smart Grid

Zhitao Guan\textsuperscript{1}, Guanlin Si\textsuperscript{1}, Xiaojiang Du\textsuperscript{2}, Peng Liu\textsuperscript{3*}, Zijian Zhang\textsuperscript{4}, Zhenyu Zhou\textsuperscript{1}

1. School of Control and Computer Engineering, North China Electric Power University, China
2. Department of Computer and Information Science, Temple University, Philadelphia PA, USA
3. School of Computer, Hangzhou Dianzi University, Hangzhou, China
4. School of Computer, Beijing Institute of Technology, Beijing, China

*Corresponding author: perryliu@hdu.edu.cn

Abstract—In smart grid, large quantities of data is collected from various applications, such as smart metering substation state monitoring, electric energy data acquisition, and smart home. Big data acquired in smart grid applications is usually sensitive. For instance, in order to dispatch accurately and support the dynamic price, lots of smart meters are installed at user’s house to collect the real-time data, but all these collected data are related to user privacy. In this paper, we propose a data aggregation scheme based on secret sharing with fault tolerance in smart grid, which ensures that control center gets the integrated data without revealing user’s privacy. Meanwhile, we also consider fault tolerance during the data aggregation. At last, we analyze the security of our scheme and carry out experiments to validate the results.

Keywords—big data; smart grid; fault tolerance; privacy-preserving

I. INTRODUCTION

With the support of information technology, smart grid has emerged as the next-generation power network, in which electricity is generated according to the real-time demand from electric equipment or household appliances. To realize the optimal energy scheduling, control center needs to collect and analyze large quantities of data from various applications [1]. However, big data acquired in smart grid applications is usually sensitive to user’s privacy [2]. For instance, smart meters are adopted to collect the real-time data from users to control center, but these data may disclose user’s family behaviors. Thus, if a thief gets the real-time data from user’s smart meter, he may gain entry to user’s house when he notices that there is nobody home. If user’s sensitive data isn’t preserved very well, the implement of smart grid will meet resistance. Therefore, the privacy-leaking in smart grid becomes an extremely important problem.

For the privacy-preserving in smart grid, there are various solutions. As we know, privacy-preserving strategy can be divided into two ways. One is to hide the user’s identity, the other way is to protect the user’s sensitive data [3]. Besides real-time data, location message also belongs to sensitive data [4] [5], but their strategies are similar. In this paper, we adopt Paillier cryptosystem to encrypt user’s real-time data and distribute secret shares into each user for further obfuscating their data. Our contributions are summarized as follows:

1) In case that data aggregation device (DA) and control center (CC) launch differential attack based on two data sets differing on at most one element, the threshold of secret shares is the same with the number of group members. If the number of SMs participating data aggregation isn’t equal to the number of group members, CC can’t get the right result.

2) We mask user’s identity through anonymity and use the group’s hash table to search the malfunctioning SM by comparing with other groups while don’t disclose user’s identity.

3) We realize the fault tolerance through the substitution strategy. Each member in a group has the same secret share with other group members. When there is a malfunctioning SM in a group, we can use other user’s data in other groups to substitute.

The rest of this paper is organized as follows. Section II introduces the related work. Section III shows the system model and design goals. In section IV, some preliminaries are given. In section V, our scheme is stated. In section VI, security analysis is given. In Section VII, the performance of our scheme is evaluated. In Section VIII, the paper is concluded.

II. RELATED WORK

To protect the privacy of users in smart grid, many scholars have proposed various strategies. These strategies can be classified into two aspects: 1) protect user’s privacy by masking the real identity; 2) protect user’s privacy by masking their real-time data.

Some works are focused on masking user’s identity. A simple solution adopting a trusted-party to manage the identity list is proposed in [6]. However, finding a trusted-party is not easy. Cheung proposes a scheme based on blind signature to solve the privacy-preserving and validity-authentication in [7]. It ensures that the verifier can authenticate sender’s signature while has no information about his privacy. Zhang, H proposes k-anonymity to protect user’s privacy [8]. An effective scheme based on virtual ring is presented in [9]. It groups the users by their geographical positions and distributes each member in the same group with the same ID. In this way, control center can...
obtain all of the users’ data without knowing the senders’ ID. However, the validity-authentication can’t be guaranteed because of the anonymity. Riesch, P. J analyzes the authentication problems during the identity-preserving [10]. Privacy-preserving scheme based on pseudonym is also very common such as [11], and it always combines with the ring signature or blind signature to mask user’s identity.

Some works are focused on masking user’s real-time data. Solutions using a house-battery to hide the real-time data are popular [12] [13]. In these schemes, smart grid and the household battery provide users with electricity at the same time to mask the electricity data. The downside of this method is that the battery charging and discharging frequently may reduce the lifetime of battery. Data aggregation is also popular in smart grid for privacy-preserving. The Paillier encryption [14] [15] [16] and Bone-Goh-Nission encryption [17] [18] are classical homomorphic encryption algorithms for data aggregation. Besides, bilinear mapping is also a common solution for data aggregation [19]. Remarkably, it is often used to realize the key-exchange. Secret sharing scheme is proposed to realize the data aggregation. It often adopts the Shamir technique to encrypt the electricity data [20]. Beussink, A shows a scheme based on data obfuscation [21], which adds a random number to each electricity data, but it will cause some large errors if the random numbers are not reasonable. In [14], Shi, Z and Sun, R discuss about the fault tolerance and differential privacy. However, the error rate and computational complexity is not very ideal. Zhang, H also analyzes differential privacy on cloud computing [22].

In our scheme, we use substitution to realize the fault tolerance based on secret sharing during the data aggregation. Comparing with other fault tolerance schemes such as [14], our scheme has lower error rate and less computational cost. Besides, we also use secret sharing scheme to defend differential attack. The process of our scheme is shown in figure 1.

![Fig.1 System Model](image-url)

### III. SYSTEM MODEL AND DESIGN GOALS

#### A. System model

As shown in figure 1, smart grid is divided into four parts, which are comprised of the control center (CC), the Key initialization center (KIC), the data aggregation device (DA), and residential users.

1) **Residential users**: We divide all the users into different groups in accordance with their geographical locations. Each residential user’ house is installed with a smart meter (SM) to collect the real-time data of the house applications every 15 minutes.

2) **Data aggregation device**: The data aggregation device is responsible for collecting all the data sent by SMs, calculating the sum of ciphertexts by running the homomorphic algorithm and uploading the sum to the control center. In addition, it has a fault-tolerance function. When a SM is malfunctioning in a group, his data would be replaced by the other group’s SM which has the same secret key.

3) **Key initialization center**: The key initialization center is responsible for initializing all of the keys for SMs and CC. It generates encrypted parameters for each SM and send the decrypted key to CC. Additionally, each group has the same number of SMs, and the encrypted parameters assigned to each group correspond to equal.

4) **Control center**: The control center can acquire a summary of real–time data in smart grid from DA by decrypted key. With these data, the CC can get the trend of power consumption and make the power generation plan or dynamic price immediately.
B. Adversarial Model

We assume that smart meter installed on the user side is vulnerable to external attacks. The communication channel is not secure and adversary may eavesdrop on the channel. CC and DA are honest-but-curious. That is to say, they do not destroy or modify user’s data, but always attempt to snoop the user's private information through the background knowledge. What’s more, CC may conspire with DA to increase the probability of successful attack.

C. Design goals

Considering the above scenarios, our design goals can be divided into three aspects.

1) Privacy-preserving: A residential user’s data are inaccessible to any other users. No matter the outside adversary, DA or CC should not acquire the real-time data of users even if he knows the cipher text and encryption algorithms.

2) Resistance to differential attack: For two formulas during the data aggregation:

\[ C_{\text{sum1}} = C_1 C_2 \cdots C_n \]  
\[ C_{\text{sum2}} = C_1 C_2 \cdots C_n C_{\#} \]

The data aggregation device can compute \( M_{\text{sum1}} \) and \( M_{\text{sum2}} \) by corresponding homomorphic encryption. Then, the plain text of the \( SM_{\#} \) will be disclosed easily through

\[ M_{\#} = M_{\text{sum2}} - M_{\text{sum1}} \]

We call this attack method differential attack. Therefore, resistance to this kind of differential attack is one of our design goals.

3) Fault tolerance: As we set the threshold of secret shares same with the number of group members, only DA aggregates all the ciphertexts in a group and sends to CC, can CC get the right result. Therefore, if there is a SM damaged, the data aggregation can’t run in the right way. Fault tolerance means that we must ensure that the data aggregation still run normally, when there are several malfunctioning SMs in a group.

IV. PRELIMINARIES

A. Paillier cryptosystem

Paillier cryptosystem is an asymmetric encryption algorithm, which has additive homomorphism properties. It includes three procedures: key generation, encryption and decryption.

1) Key generation: Chooses two prime numbers \( p, q \) with the same length and calculates \( n = pq \). \( g \) is a generator of cyclic group \( \mathbb{Z}_n^* \), and \( \gcd(L(g^2 \mod n^2), n) = 1 \). The public key is \((n, g, \lambda)\), and the private key is \( \lambda \).

\[ \lambda = \text{lcm}(p-1, q-1) \]  

2) Encryption phase: For the plain text \( m \in \mathbb{Z}_n \), we can select a random number \( r < n \). Then, the ciphertext can be calculated as follows:

\[ C = g^n r^\lambda \mod n^2 \]  

3) Decryption phase: After receiving the cipher text \( C \), the receiver can get the plain text \( m \) with the secret key \( \lambda \) by the following formula

\[ m = \frac{L(C^2 \mod n^2)}{L(g^2 \mod n^2)} \mod n \]  

B. Secret sharing scheme

The secret sharing scheme is a scheme which splits a secret into \( \alpha \) pieces and distributes these pieces with different valid members. If an adversary captures a member in the system, he can only get a piece of the secret. Only if the adversary get at least \( d \) pieces of the secret, can he get the whole secret. We call \( d \) threshold and usually adopt the Shamir technique to realize this result.

The trusted-party chooses a polynomial to split a secret.

\[ G(x) = \theta + a_1 x + a_2 x^2 + \ldots + a_d x^d \]  

\((x_i, G(x_i))\) is the corresponding share. Remarkably, the Shamir secret sharing scheme is the fully homomorphic and can be designed as a better scheme to realize the data aggregation. According to the lagrange interpolation polynomial, we have

\[ G(x) = \sum_{j=1}^{d} \left( \prod_{\substack{i=1, \ldots, d \atop i \neq j}} \frac{x-x_i}{x_j-x_i} \right) G(x_j) \]  

\[ \beta_{x_i} = \prod_{\substack{j=1, \ldots, d \atop j \neq i}} \frac{x-x_i}{x_j-x_i} \]

Then, we can easily compute \( \theta \) as follows:

\[ \sum_{x_i} G(x_i) \beta_{x_i} = G(0) = \theta \]

C. Signal-to-noise ratio

Signal-to-noise ratio (SNR) is a common ratio and it is often used to measure the performance of electronic systems. SNR is calculated as follows:

\[ SNR = 10 \log_{10} \frac{P_s}{P_n} \]  

\( P_s \) represents the power producing the normal signal and \( P_n \) represents the power producing the noise. The higher is the SNR, the stronger is the signal. Generally speaking, the image SNR is greater than 30 dB, which will not affect the resolution of the picture. In this paper, we take the sum of normal SMs’ data as the signal and take the sum of malfunctioning SMs’ data processed by substitution as the noise. Then, we can measure the error rate of our scheme through the image SNR.
D. Notations

| Acronym | Descriptions |
|---------|--------------|
| SM      | Smart meter  |
| CC      | Control center |
| EK      | Encrypted key |
| DK      | Decrypted key |
| KIC     | Key initialization center |
| DA      | Data aggregation device |
| SNR     | Signal to noise ratio |
| C_{sum}\_n | Aggregation of normal SMs’ value |
| C_{sum}\_i | Aggregation of malfunctioning SMs’ value |
| C_{sum} ’ | Aggregation of the value processed by fault tolerance |
| t       | Time stamp |
| m_t     | Plaintext of SM |
| c_i     | Ciphertext of SM |
| r       | Random number |
| \bar{m} | The average value of plaintext |
| \bar{c} | The average value of ciphertext |
| N       | The total number of all the SMs |
| F       | The number of the malfunctioning SMs |
| gcd     | Greatest common denominator |
| lcm     | Least common multiple |
| x_i     | The serial number of SM |
| y_j     | The serial number of group |

V. OUR SCHEME

A. System initialization

The KIC first chooses two big primes \( p, q \), and computes \( n = pq \). Then, it chooses an integer \( \theta \) from \( \mathbb{Z}_{\phi(n)}^* \), where \( \gcd(L(g^d \mod n^2), n) = 1 \) and \( \lambda = \text{lcm}(p-1, q-1) \).

It constructs a formula \( G(x) = \theta + a_1 x + a_2 x^3 + \ldots + a_m x^{m-1} \). Here, we set \( \theta = 0 \). All the SMs in smart grid are divided into different groups, and each group has \( d \) members. For each SM in a group, the KIC assigns the private key \( \{ x_i, y_i, G(x_i), \beta_{x_i} \} \) to the SM \( i \). While, \( x_i \) is a random number representing the SM \( i \)’s serial number. \( y_i \) is the group serial number and \( \beta_{x_i} = \prod_{i=1}^{d} \frac{x_j}{x_j - x_i} \). Particularly, the set of SM serial numbers \( \{ x_1, x_2, \ldots, x_d \} \) in each group is the same. That is to say, for a special SM, it can find members with the same private key except for the group serial number in other groups.

At last, KIC publishes \( (n, \theta, g, H_1, H_2) \) and sends \( \lambda \) to CC in a secure way. \( h, H_1 \) and \( H_2 \) are three hash functions.

B. Encryption

The SM collects the electricity data every 15 minutes from all the house applications. For the time \( t \), it computes

\[
C_t = (g^{x_t r_t} \mod n^2) \cdot h(t)^{\ell_{t, G(x_t)}} \tag{12}
\]

\[
H_1(t \mid G(x_t) \beta_{x_t}) \tag{13}
\]

\[
H_2(y_i \mid C_t \mid H_1(t \mid G(x_t) \beta_{x_t})) \tag{14}
\]

Then, SM encrypts the total electricity data and sends \( y_i C_t H_1(t \mid G(x_t) \beta_{x_t}) H_2(y_i \mid C_t \mid H_1(t \mid G(x_t) \beta_{x_t})) \) to the DA.

C. Data aggregation

When the DA receives a message from a SM, it verifies \( H_2(y_i \mid C_t \mid H_1(t \mid G(x_t) \beta_{x_t})) \) to authenticate the message integrity. If the hash value is right, the data aggregation will be performed.

1) Normal aggregation: If the DA receives all the SMs’ data in a group, it runs the data aggregation as follows:

\[
C_{sum} = \prod_{i=1}^{d} C_i \tag{15}
\]

\[
= (g^{\sum_{i=1}^{d} r_i} \mod n^2) \cdot h(t)^{\ell_{t, G(x)}} \tag{16}
\]

\[
M_{sum} = \frac{L(C_{sum}^{\ell_{t, G(x)}} \mod n^2)}{L(g^{d \mod n^2})} \tag{17}
\]

\[
M_{sum} \text{ denotes the sum of users’ plaintexts.}
\]

2) Fault tolerance: As DA only knows which group a SM belongs to according to their group serial number, we can use \( H_1(t \mid G(x_t) \beta_{x_t}) \) to find the malfunctioning SM while mask user’s identity. If there is a malfunctioning SM in a group, the DA runs the following steps:

First, it compares this group of hash table constituted by \( H_1(t \mid G(x_t) \beta_{x_t}) \) with other complete groups to find the malfunctioning SM.

Then, selects a SM \( j \) from other groups with the same hash value \( H_1(t \mid G(x_j) \beta_{x_j}) \) to replace the malfunctioning SM \( i \). Theoretically, if there is a malfunctioning SM, we shouldn’t consider this user’s data. To further reduce the error, the data of SM \( j \) is processed before the data aggregation as follows:

\[
- \sum_{i=1}^{d} m_i \tag{17}
\]

\[
C'_j = \frac{C_j}{g^{x_j r_j} \mod n^2} \cdot h(t)^{\ell_{t, G(x_j)}} \tag{18}
\]

\[
\sum_{i=1}^{d} m_i \text{ represents the sum of the electricity data of the previous period. } C'_j \text{ represents the processed data of } C_j \text{ and replaces the missing data } C_i \text{ to run the data aggregation.}
D. Power dispatching

After receiving the sum of the electricity data in smart grid, CC can draw the real-time load curve and create the dynamic price, power generation plan and other scheduling strategies.

VI. Security Analysis

A. Privacy-preserving

For a SM in smart grid, we can analyze the security of data from following aspects: external attacker, DA, CC and conspiracy attack

1) External attacker: When an external attacker compromises the user's SM, the cipher text $C_s$ sent by the user can be obtained. However, because the attacker doesn’t know the other $d{-1}$ users’ private key and the decrypted key $\mathcal{K}$, so it can’t acquire the plain text.

2) DA: After receiving all the data from SMs, DA can only perform the data aggregation and replace the malfunctioning one when it’s necessary. However, it can’t obtain a single user’s plaintext due to the lack of $h(t)^{g(x)}$, therefore, the security of the user's data can be ensured.

3) CC: CC can only get all the users’ aggregated data, so it can’t snoop to a single user's real-time data. Thus, user’s privacy can be ensured in our scheme.

4) Conspiracy attack: If DA gets the decrypted key from CC and tries to acquire the plaintext of a single user, user’s privacy can still be preserved because they don’t know the secret shares $h(t)^{g(x)}$. What’s more, if the DA is in collusion with a SM to attack some SMs from other groups with the same SM key, our scheme can also protect the users’ privacy because of anonymity.

B. Resistance to differential attack

Differential attack needs to calculate the integrated data of $d{+1}$ users and the integrated data of $d$ users. After computing their difference, the attacker can acquire the privacy information of the individual user. For this scheme, there is no risk of differential attack. Because the secret sharing scheme can only calculate the $d$ users’ integrated data. If the number of SMs participating in the data aggregation is less than $d$ or more than $d$, the key $\mathcal{B}$ can’t be synthesized.

C. Fault tolerance

Because we set the threshold of secret shares same with the number of group members, only DA aggregates all the ciphertexts in a group and sends to CC, can CC get the right result. In this paper, when a certain SM is damaged, we can replace its data by other SMs in other groups. So, our encryption system will run normally even there are some malfunctioning SMs. Because real-time data is collected for scheduling, creating the power generation strategies, and dynamic price, error caused by substitution is negligible for the big data in smart grid. When there are too many malfunctioning SMs, the KIC should re-assign the keys.

VII. Performance Evaluation

The most important idea of our paper is to use substitution to realize the fault tolerance, so it is necessary to prove the substitution between two members in different groups to be right for the power dispatching in smart grid.

Here, we take the sum of the normal SMs’ data as the signal and take the sum of malfunctioning SMs’ data processed by substitution as the noise. Then, we can use the SNR to measure the error rate of our scheme and the detailed formula is presented as follows.

$$SNR_{CB} = 10\log \frac{C_{\text{sum}1} - C_{\text{sum}3}}{C_{\text{sum}1}} = 10\log \frac{N \text{e}^{FC}}{FC / g^x} = 10\log \frac{N}{F} - 10g^5$$ (21)

By inputting the number of malfunctioning SMs and the total number of the SMs in smart grid into the formula (21), where $C_{\text{sum1}}$ denotes the sum of normal SMs’ data and $C_{\text{sum}3}$ denotes the sum of malfunctioning SMs’ data and $C_{\text{sum}}$ denotes the sum of the data processed by the fault tolerance, we can get the curve of SNR as figure 2.

For the number of SMs is from 1000 to 5000, we can find that the SNR of our scheme is more than 35 dB in the worst case and the average rate is close to 40 dB, which is allowed in smart grid for the power scheduling. As the formula (21) shows, the SNR is related to the value of $\mathcal{B}$. Therefore, we can increase the accuracy by adjusting the value of $\mathcal{B}$.

We use $T_{\text{exp}}$ to denote the time of exponentiation and use $T_{\text{mul}}$ to denote the time of multiplication. $T_{\text{ran}}$ denotes the time of generation of random number and $T_{\text{pro}}$ denotes the time of Pollard’s lambda method. We can calculate computational cost of our scheme and DG-APED as follows:

$$T_{\text{exp}} = (N + 4)T_{\text{mul}} + 5T_{\text{exp}}$$ (21)

$$T_{\text{DG-APED}} = 7T_{\text{exp}} + (N + 5)T_{\text{mul}} + T_{\text{ran}} + T_{\text{pro}}$$ (22)

As far as we know, DG-APED scheme proposed by Shi, Zhiguo is also a subtle group-based scheme with fault tolerance [14]. As figure 3 shows, we can find our scheme has great advantage than DG-APED when the number of SM varies from 1000 to 5000.
We also calculate the SNRs of our scheme and DG-APED in figure 4. The SNRs of two schemes are shown as follows:

$$SNR_{SN} = 10 \log \frac{C_{SN} - C_{SND}}{C_{SN}} = 10 \log \frac{N_{C} - F_{C}}{F_{C} / g} = 10 \log \frac{N}{F} - 10 \log g$$

$$SNR_{DG} = 10 \log \frac{2(N_{C} - F_{C})}{(k-1)F_{C}} = 10 \log \frac{2(N - F)}{(k-1)F}$$

\(k\) is the number of SMs in a group at DG-APED scheme.

Through the figure 4, we can find that the SNR of our scheme is much higher than DG-APED.

**REFERENCES**

[1] Zhang H, Zhang Q, Zhou Z, et al. Processing geo-dispersed big data in an advanced mapreduce framework[J]. IEEE Network, 2015, 29(5):24-30.

[2] Huang X, Du X. Achieving big data privacy via hybrid cloud[C]// IEEE INFOCOM 2014 - IEEE Conference on Computer Communications Workshops. IEEE, 2014:512-517.

[3] Zhou Z, Zhang H, Du X, et al. Prometheus: Privacy-aware data retrieval on hybrid cloud[J]. 2013:2643-2651.

[4] Zhang H, Xu Z, Yu X, et al. LPPS: Location privacy protection for smartphones[C]// ICC 2016 - 2016 IEEE International Conference on Communications. IEEE, 2016:1-6.

[5] Zhang H, Xu Z, Zhou Z, et al. CLPP: Context-aware location privacy protection for location-based social network[C]// IEEE International Conference on Communications. IEEE, 2015:1164-1169.

[6] Effyymiou C, Kalognidis G. Smart Grid Privacy via Anonymization of Smart Metering Data[C]// First IEEE International Conference on Smart Grid Communications. IEEE Xplore, 2010:238-243.

[7] Cheung J C L, Chim T W, Yiu S M, et al. Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network[C]// Global Communications Conference. IEEE, 2011:5-9 December 2011, Houston, Texas, USA. DBLP, 2011:1-5.

[8] Zhang H, Zhou Z, Du X, et al. Practical and privacy-secured data indexes for outsourced cloud data[C]// GLOBECOM 2013 - 2013 IEEE Global Communications Conference. IEEE, 2013:671-676.

[9] Badra M, Zeadally S. Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy[J]. IEEE Transactions on Information Forensics & Security, 2014, 9(9):321-329.

[10] Riesch P J, Du X. Audit based privacy preservation for the OpenID authentication protocol[C]// Homeland Security. IEEE, 2012:348-352.

[11] Tan X, Zheng J, Zou C, et al. Pseudonym-based privacy-preserving scheme for data collection in smart grid[J]. 2016, 22(2):120.

[12] Yao J, Venkitasubramaniam P. The privacy analysis of battery control mechanisms in demand response: Revealing state approach and rate distortion bounds[C]// Decision and Control. IEEE, 2014:1377-1382.

[13] Kalogridis G, Fan Z, Basutkar S. Affordable Privacy for Home Smart Meters[C]// Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops. IEEE, 2011:77-84.

[14] Shi Z, Sun R, Lu R, et al. Diverse Grouping-Based Aggregation Protocol With Error Detection for Smart Grid Communications[J]. IEEE Transactions on Smart Grid, 2015, 6(6):1-1.

[15] Chen L, Lu R, Cao Z. PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communication[J]. Peer-to-Peer Networking and Applications, 2015, 8(6):1122-1132.

[16] Borges F, Muhlhauser M. EPPPSMS: Efficient Privacy-Preserving Protocol for Smart Metering Systems and Its Simulation Using Real-World Data[J]. IEEE Transactions on Smart Grid, 2014, 5(6):2701-2708.

[17] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts[C]// Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings. DBLP, 2005:325-341.

[18] Chen L, Lu R, Cao Z, et al. MUDA: Multifunctional data aggregation in privacy-preserving smart grid communications[J]. Peer-to-Peer Networking and Applications, 2015, 8(5):1-16.

[19] Gong Y, Cai Y, Guo Y, et al. A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid[J]. IEEE Transactions on Smart Grid, 2015, 7(3):1-1.

[20] Barletta A, Callegari C, Giordano S, et al. Privacy preserving smart grid Communications by verifiable secret key sharing[C]// International Conference on Computing and Network Communications. IEEE, 2015:199-204.

[21] Beussink A, Akkaya K, Senturk I F, et al. Preserving consumer privacy on IEEE 802.11s-based smart grid AMI networks using data obfuscation[J]. Openaccess, 2014.

[22] Zhang H, Zhou Z, Ye L, et al. Towards Privacy Preserving Publishing of Set-valued Data on Hybrid Cloud[J]. IEEE Transactions on Cloud Computing, 2015, 1-1.