ISSN: 2688-8645

Privacy Protection Scheme Based on Time Disturbance and Ring Signcryption

Baoyi Wang *, Tianxiao Hu

North China Electric Power University, Baoding, 071003, China

Abstract

In order to ensure that the data transmitted in the smart grid is true and effective, smart meters need to send users' electricity consumption data to the control center in real time, and these data are fine-grained, which is very useful for analyzing and regulating the usage of electric energy. Hijacking will cause serious privacy leakage problems. Aiming at the problem of user privacy leakage in the process of smart meter data transmission, this paper studies the privacy protection method based on time disturbance and the ring signcryption algorithm, so as to design a privacy protection method based on time disturbance and ring signcryption, staggering the data collection time and Data release time, combined with ring signcryption, simultaneously protects user identity information and user power consumption data information, and improves data privacy and usability. The theory proves that this method can effectively suppress the recognition accuracy of electrical switching events, and eliminates the influence of the number of ring members of the ring signcryption algorithm, and at the same time reduces the computational overhead.

Keywords

Smart meter; Privacy protection; Attributes; Ring signcryption; Time disturbance.

1. Introduction

The traditional power grid has a certain degree of limitations in its use, leading to some problems in power management, and at the same time, there are also abuses in the use of electrical energy. With the development of computer technology, communication technology and the power industry, various countries and power companies have put forward the concept of a new power grid: smart grid. Smart grid has brought great convenience to our daily life and work. However, in recent years, as the economy continues to develop and the construction of smart grids continues to deepen, smart grid information security is also facing huge challenges, and smart grids are highly complex, lack of smart grid security systems, complex information network environments, and user safety. Threats, smart terminal security threats and a series of issues [1]. In addition, the data transmitted in the smart grid communication process is fine-grained and needs to be kept confidential, which is very useful for analyzing and regulating the power usage. Based on this, the problem of user privacy leakage is more serious [2, 3]. Smart meter data provides strong data support for the metering and billing of power resources, the regional distribution of power resources, and third-party data mining and analysis. However, the fine-grained power consumption data has also led to the exposure of user privacy information to attacks. In front of him. By mining the continuous changes of the power consumption curve, the attacker can obtain the usage of different loads in each household, and even to a certain extent, obtain information about the different behavior patterns and living habits of users [4].

The protection methods for the leakage of user privacy information in the smart grid mainly include two aspects. On the one hand, it is a protection method to prevent the leakage of user

ISSN: 2688-8645

identity information [5-8]. The main idea is to use blind signatures, group signatures, and ring signatures. Cryptographic technologies such as signature and signcryption anonymize user identities, making it impossible for the control center to associate user identities with user data, thus protecting user identities. The other is to prevent the leakage of user data information [9-15]. The main ideas include the use of random disturbance, rechargeable battery technology, differential privacy and other methods to protect user electricity data, and send the obscured electricity data Go to the control center, so that the control center cannot obtain the real data of the user.

Literature [5] uses blind signature technology to protect the privacy of users. Blind signatures have the advantages of unforgeability, non-repudiation, blindness and untraceability, which can effectively protect the specific content of the signed message, but blind signatures also have signatures. Disadvantages such as repetition and high computational overhead.

Literature [6] uses group signature technology to protect user privacy. Any member in the group can sign on behalf of each member of the entire group anonymously, and the group signature can be publicly verified, and only a single group Public key to verify. However, there will be group administrators in the group signature, and the existence of the group administrator will destroy the anonymity and leave a security risk to the user's privacy.

Literature [7] uses ring signature technology to ensure anonymity. This method can make up for the shortcomings of the above two methods, but the ring signature algorithm only provides digital signature functions and cannot provide encryption technology.

On the basis of all the above methods, literature [8] combines the advantages of signcryption and ring signature technology, and proposes the concept of ring signcryption, which can efficiently realize the confidentiality and unforgeability of messages while ensuring unconditional anonymity. Since then, a large number of ring signcryption schemes under certificate-free systems have been continuously proposed. These methods reduce the number of bilinear pairing operations to reduce computational overhead and strive to find more effective ring signcryption schemes. However, the signcryption length of all the above methods is related to the number of ring members, and there is also the problem of large computational overhead.

Literature [9] uses rechargeable battery technology to protect user electricity data information. The information flow from electrical appliances through rechargeable batteries and smart meters to the power company can also be reversed bidirectional transmission; power flow from the power company through smart meters and rechargeable batteries to each Electrical appliances. The main function of the rechargeable battery is to transmit the electric energy delivered by the power company downwards to the electrical appliances, and at the same time, part of the electrical energy can be stored for backup and then transmitted to the electrical appliances. At this time, the smart meter cannot complete the task of reflecting the user's electricity consumption information in real time.

Literature [10, 11] proposed a power data aggregation algorithm based on differential privacy and homomorphic encryption technology to achieve data aggregation in the ciphertext domain.

Literature [12] combines data fusion algorithm, homomorphic encryption technology and aggregate signature technology to propose an improved Paillier algorithm to protect user electricity data information. This method greatly improves the efficiency of data transmission without reducing security. .

Literature [13-15] mainly uses data aggregation methods to obscure the user's specific electricity consumption information to achieve the purpose of protecting the user's electricity consumption information. After data aggregation, the information is transmitted to the control center, power company and other receivers, or in transmission In the process, it is obtained by an illegal attacker. No matter which party receives the information, it cannot judge the user's

ISSN: 2688-8645

specific electricity consumption information based on the user's identity, nor can it correspond to the specific electricity user based on the obtained electricity consumption information. However, if the power company wants to analyze the user's fine-grained electricity consumption information to provide other value-added services such as electricity bill calculation or demand response, this method cannot be satisfied.

Based on the advantages and disadvantages of all the above methods to protect user identity and user data, the main contributions of this article can be summarized as follows. First of all, we adopted a delay disturbance mechanism to add a positive time disturbance to the collection time to determine the release time. After the forward disturbance, different collection times may get the same release time. By staggering the collection and Publish time to obscure consumer events. Secondly, we use an improved attribute identity-based ring signcryption algorithm to sign and encrypt the data after forward disturbance, and protect user privacy from the source of the data. Compared with the existing ring signcryption algorithm, the improved algorithm does not require a certificate, and at the same time solves the problem of inefficiency caused by too many ring members, and reduces the computational overhead.

The rest of this article is organized as follows. The second part introduces the related knowledge of time disturbance and ring signcryption. The third part mainly introduces the method of problem description and modeling. The fourth part describes in detail the realization process of this scheme. The fifth part is the program analysis of this program. The sixth part summarizes the thesis.2. Methodology

2. Time Disturbance and Ring Signcryption

2.1. Time Disturbance

At present, one of the most common methods for privacy protection of smart meter electricity data is the data perturbation method. Common data perturbation methods include random perturbation, rechargeable battery technology, and differential privacy. The above methods have their different advantages but all have some shortcomings. Combining the above-mentioned random disturbance and rechargeable battery technology, we propose a new technology: time disturbance technology. We move the idea of random perturbation to the time axis to obtain a time perturbation mechanism. The time disturbance mechanism is based on the location corresponding to the specific record of the mobile user’s power consumption on the time axis. On the one hand, it can improve the anti-filtering ability of the disturbance mechanism, and on the other hand, it can also confuse the power waveform more powerfully. To achieve the purpose of power mode protection. By adding a positive time disturbance to the original data, the data collection time and the data release time are staggered, which can effectively confuse the actual load operation, blur the user's actual power consumption behavior, and achieve the purpose of protecting user privacy.

2.2. Ring Signcryption

Confidentiality, authentication, integrity, and non-repudiation are the four main security goals in cryptography, among which confidentiality and authentication are the two most important security goals. In traditional cryptography methods, confidentiality and authentication are studied separately as two separate parts. The authenticity of the message is generally realized by digital signature technology, and the confidentiality is generally realized by the encryption algorithm in the public key cryptosystem. However, in the actual application process, it is often necessary to ensure that the message is authenticated and confidential. In the past, the solution was to first sign the message, and then encrypt the message based on the signature. This can also achieve authentication at the same time. However, the actual cost of such an approach will be the sum of the signature algorithm and the encryption algorithm, and the cost is relatively

ISSN: 2688-8645

high and the efficiency is low. Literature [16] first proposed: the concept of "signcryption", which combines digital signature technology and encryption technology to achieve two goals at the same time. Compared with the traditional "signature first and then encrypt" approach, the signcryption algorithm has simple algorithms and calculations. Advantages such as low overhead, strong parallelism, and high security level. After that, the document [17] first proposed the concept of "ring signcryption", which organically combines ring signature and signcryption. Any member of the ring can use its own private key and the public key of other members to sign the message. The three functions of signer's anonymity, message authentication, and confidentiality are simultaneously realized in one algorithm. This algorithm has made great progress in reducing overhead and improving efficiency, and is also suitable for resource-constrained smart grid communication environments. After improvement, an identity-based ring signcryption scheme appeared. The length of the ring signature and calculation cost of such schemes are related to the number of members in the ring. The number of members in the ring directly affects the efficiency and anonymity of signcryption. Afterwards, a series of certificateless ring signcryption algorithms were proposed. But they all have huge computational overhead.3. Results and discussion

3. Design and Implementation

This solution mainly adopts a two-layer communication structure, involving four entities including smart meter Mi, data collector DC, control center CC, and power supply service provider SP.

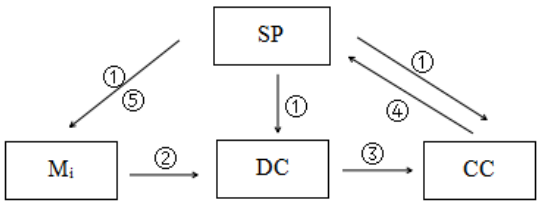

Figure 1. Solution architecture

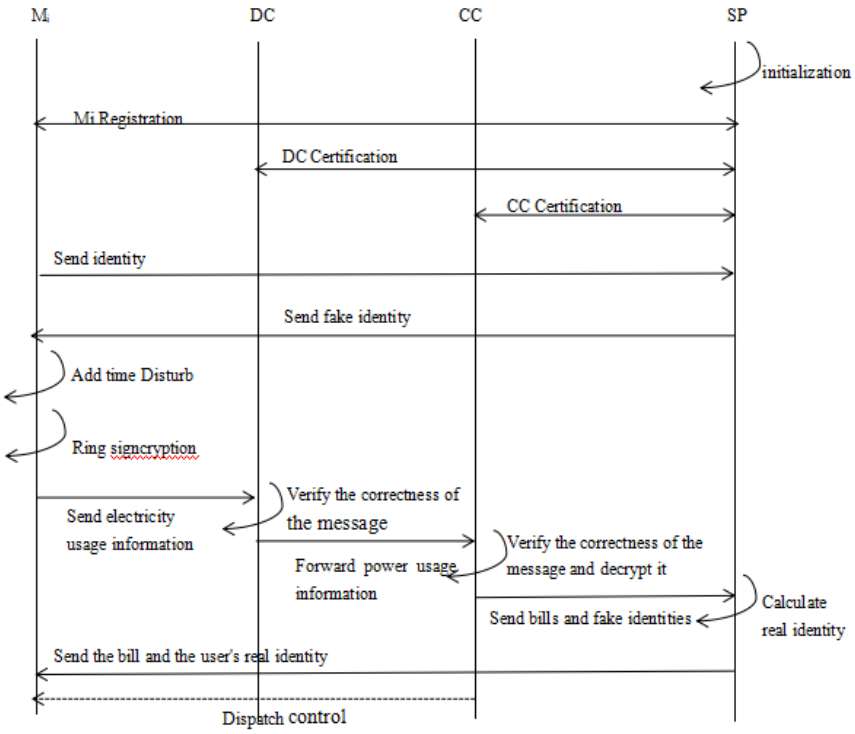

Figure 2. The communication process of this program

ISSN: 2688-8645

We combine ring signcryption technology to perform signcryption transmission of the information after delayed disturbance processing to realize the privacy protection function of power users; when realizing the function of metering electricity bills, DC can only obtain the user's specific power consumption information and the corresponding pseudo-identity , The user's real identity cannot be obtained, so the user's real identity cannot be matched with the specific power information; and the SP can obtain the user's real identity according to the user's pseudo identity and at the same time obtain the user's billing information but cannot obtain the user's specific power consumption. Information, to achieve the purpose of protecting user privacy information. The specific communication process of this scheme is shown in the figure:

3.1. System Initialization Phase

(1) SP initialization

First, SP arbitrarily inputs a parameter t to obtain two prime numbers p and q, and the two prime numbers satisfy the condition q|p-1, let g be a generator of order q in the cyclic group G. SP randomly selects $z \in Z_q^*$ as the master key of the system, among which $Z_q^* = \{1, 2, ..., n\}$. Then calculate the system public key y=zg. On this basis, select the appropriate hash function H_1, H_2, H_3, H_4, where

$H_1 : \{0,1\}^* \to G;\ H_2 : \{0,1\}^* \times G^2 \to Z_q^*;\ H_3 : \{0,1\}^* \times \{0,1\}^n \times G^3 \to Z_q^*;\ H_4 : G \to \{0,1\}^n$ The public system parameter is $\{G,\ p,\ q,\ g,\ y,\ H_1,\ H_2,\ H_3,\ H_4\}$.

(2) User registration

SP randomly selects the identities for users as $I_i \in \{0,\ 1\}^*$, $i = \{1,\ 2,\ ...,\ n\}$, where n is the number of users, randomly selects $x_i \in Z_q^*$, calculates $b_i = x_i g$ as part of the public key of M_i, and sends b_i and I_i to SP. SP randomly selects $s_i \in Z_q^*$, calculates part of the public key $w_i = s_i g$, $t_i = s_i + zH_2(I_i,\ w_i,\ b_i) + H_3(zb_i)$ and sends w_i and t_i to the M_i user. After the M_i user receives and performs $w_i + yH_2(I_i,\ w_i,\ b_i) = gt_i$ verification, if it is established, the partial private key $z_i = t_i + H_3\{x_i y\}$ is calculated, the end user public key pair is generated: $K_i = (w_i,\ b_i)$, and the user private key pair is generated: $T_i = (z_i, x_i)$.

(3) DC public and private key generation

The DC identity is I_B, and its private key and public key are generated in a similar way to the user key generation method. Finally, the DC public key pair $(X_B,\ Y_B)$ and the private key pair $(x_B,\ y_B)$ are generated.

(4) CC public and private key generation is similar to DC

3.2. Delay Disturbance Stage of Electricity Consumption Information

(1) Time disturbance algorithm

A positive time disturbance is added to the electricity consumption information sequence $x_{(i,\ t)}$ collected at time t, so that the release time can be determined, that is, $t' = t + delay(t)$. Then stack all the power information at the same release time, and finally get the total consumption data $x'_{(i,\ t')}$. We define a discriminant function to represent the mapping relationship between and.

$$R(a,\ b)\begin{cases}0,\ a \neq b\\ 1,\ a = b\end{cases} \tag{1}$$

When the parameter is a=b, R=1; otherwise, R=0. The resulting mapping expression

$$x'_{(i,\ t')} = \sum_{t=1}^{t'} s[t',\ t + delay(t)] \cdot x_{(i,\ t)} \tag{2}$$

ISSN: 2688-8645

(2) Delayed Noise Design

According to the requirements of the above-mentioned time disturbance mechanism algorithm, the design delay noise should meet the following requirements:

① The data needs to be processed in real time, and the delay noise should be a positive disturbance.

② In order to avoid excessive errors, the delay of online launch needs to be restricted.

This article selects two commonly used probability distribution methods, uniform distribution and normal distribution. The random number of normal distribution ranges from negative infinity to positive infinity. In order to achieve the purpose of constraining the upper limit of delay, we do the following processing on the normal distribution:

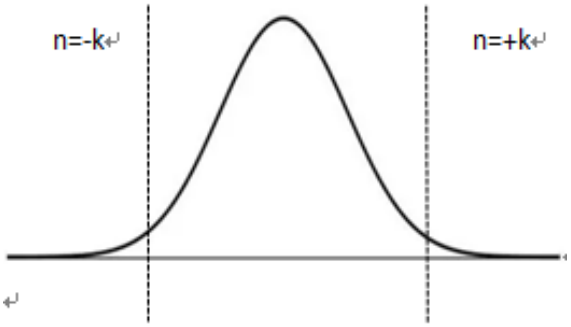

Figure 2. Schematic diagram of normal distribution probability density

Find a specific value of k so that when |n|<k, the cumulative probability is greater than a number AAA that tends to 1, and when |n|>k, n=n mod k. On the one hand, the delay noise is constrained, and on the other hand, making the cumulative probability of all values 1 also meets the integrity requirements of probability. k satisfies the following formula:

$$\int_{-k}^{+k} p(n)dn > \ell \tag{3}$$

Let $\ell = 0.9$ be based on the above formula to get uniformly distributed $k_1 \approx 1$ and normally distributed $k_2 \approx 2$. In summary, the expression of the delay noise required in this article can be obtained:

$$delay(t) = \frac{D_{\max}}{k} \cdot (\lfloor n(t) \rfloor \bmod k) \tag{4}$$

Among them, $D_{\max}$ represents the maximum delay, k represents the maximum delay coefficient, and n(t) represents a random number that meets a specific standard distribution.

Thus, according to $D_{\max}$, k, n(t), the delay noise that needs to be added can be obtained.

3.3. Signcryption Stage of Electricity Usage Information Ring

Before sending the electricity usage information to the DC, the meter user first selects a user M_s representative ring member to signcrypt the delayed perturbed message m, the identity of the selected representative member is I_s, the pseudo-identity is t_s, and the public key It is , and the private key is (z_s, x_s). We now assume that there are n members in t (w_s, b_s) his ring, $M_i = \{M_1, M_2, ..., M_n\}$. The identity of the DC as the information receiver in this area is I_B, the public key is (X_B, Y_B), and the private key is (x_B, y_B). M_s do the following:

ISSN: 2688-8645

(1) First randomly select $r_1 \in Z_q^*$, and then calculate $D = gr_1$.

(2) Generate information that can verify the identity of the electric meter. The previously selected representative user randomly selects $r_2 \in Z_q^*$, and then calculates $E = r_2 g(z_s + x_s)$. In this formula, z_s, x_s is the private key of the representative member.

(3) For any $i \neq s$, select $a_i \in Z_q^*$, $M_i = a_i g$, and then calculate $h_0 = H_2\{I_B, X_B, Y_B\}$, $h_i = H_1\{m, M_i, E, M, X_B\}$. m is the cascade of the user's electricity consumption information and the pseudo-identity that has undergone a positive disturbance, $m = m_i \| t_i$, the above-mentioned X_B, Y_B is part of the public key of the data collector in this area, m_i is the user's electricity consumption information, and t_i is the pseudo-identity.

(4) When i=s, the meter user randomly selects $a_s \in Z_q^*$, and then calculates

$$\begin{cases} M_s = a_s w_s - \sum_{i=1, i \neq s}^{n} M_i + h_i w_i \\ h_s = H_1\{m, M_s, E, M, X_B\} \\ v = h_s y \\ h_0 = H_2\{I_i, w_i, b_i\} \\ f = \dfrac{d}{yh_0 + v} \\ d = r_2(z_s + x_s) \end{cases} \tag{5}$$

In the above formula w_s is the partial public key representing the signcryption member, and w_i is the partial public key of the members in the ring except the sender.

(5) $C = H_4\{(X_B + Y_B + yh_0) r_2 (z_s + x_s)\} \oplus m$ can be obtained by calculating the ciphertext, where $\oplus$ is the exclusive OR operation.

(6) Output the ring sign ciphertext $\partial = \{E, C, f, v, d, M_1, M_2, ..., M_n\}$ to the receiver I_B.

3.4. Electricity Information Verification Stage

After the DC receives the signcryption message, it needs to verify whether the signcryption information is accurate. Perform the following operations:

(1) Calculation:

$$\begin{cases} h_0 = H_2\{I_i, w_i, b_i\} \\ l = [x_B - H_3(y_B y) + y_B] dEg \\ m' = H_4\{1\} \oplus C \\ F = dg \end{cases} \tag{6}$$

The decrypted message m' is recovered. If $m' = m$, the received message is correct.

(2) Verify whether $H_1\{m', M_i, F, M, X_B\} = h_i$ is established, among which $i \in (1, 2, ..., n)$. If DC is established, m' will be accepted, otherwise, the m' received will be abandoned.

(3) The DC forwards the electricity consumption information of the meter user to the CC.

3.5. Electricity Information Data Analysis Stage

After CC receives the signcryption information forwarded by DC, it decrypts and verifies the accuracy of the message. After passing the verification, m can be obtained. According to $m = m_i \| t_i$, the corresponding (m_i, t_i) is found. CC analyzes the decrypted user information, and then responds to it. The information generates the user's electricity information bill T_i, and then

ISSN: 2688-8645

CC sends T_i and t_i together to SP, SP calculates the real identity of the user based on $t_i = S_i + zH_2\{I_i, w_i, b_i\}$, SP sends T_i to the user after obtaining the real identity of the user, and the user can Check the information through the WeChat applet or Alipay account login account and password to complete the activity of paying electricity bills.

4. Safety Analysis

4.1. Legality of Identity

Verify that $H_3\{m', M_i, F, M, X_B\} = h_i$ is established where $i \in (1, 2, ..., n)$,

$$F = dg = r_2(z_s + x_s)g = E \tag{7}$$

Because any user other than M_s will not calculate F and the relative E without knowing its private key, if the $F = E$ is established, the identity receives the m' correctly, otherwise the information is discarded.

4.2. Anonymity

From the perspective of ciphertext, any member of the ring is indistinguishable. Each ring member can perform ring signcryption on behalf of all members in the ring. Even the private keys of all members in the ring are leaked. The probability of an external attacker guessing the signcryptor is no greater than $1/n$, and the probability of an attacker from inside guessing the signcryptor is no greater than $1/n-1$. In summary, this program is anonymous.

4.3. Confidentiality

There are two main types of attackers in ring signcryption. In this scheme, no matter which type of attacker obtains the ciphertext $\partial = \{E, C, f, v, d, M_1, M_2, ..., M_n\}$ sent to DC, if you want to calculate the original message m from it, you need to know $l = [x_B - H_3(y_B y) + y_B]dEg$, but the above two None of these attackers can get the DC private key, so they can't get m, so this scheme is also confidential.

4.4. Completeness

The scheme in this chapter frequently uses hash functions for calculations in the process of ring signcryption and aggregate signcryption. Because the hash function has one-way characteristics, it guarantees the integrity of the message that will not be tampered with in the process of transmission.

5. Conclusion

Aiming at the problem that user privacy security cannot be guaranteed in the advanced measurement system, a privacy protection scheme based on time disturbance and ring signcryption is proposed. In the entire process of uploading data from smart meters to power service providers, combined with time disturbance technology and ring signcryption algorithm, the implementation process of the user privacy protection scheme is designed, which solves the problem of user identity privacy and user electricity data privacy. The privacy security issues in the advanced measurement system ensure that the user's privacy will not be leaked during the upload process. In addition, this solution does not use time-consuming calculations, and is suitable for advanced measurement systems with limited resources. After security analysis, this solution also meets the security requirements of correctness, legitimacy, anonymity, confidentiality, integrity, and availability.

ISSN: 2688-8645

References

[1] P. Ganguly, M. Nasipuri and S. Dutta, "Challenges of the Existing Security Measures Deployed in the Smart Grid Framework," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 1-5, doi: 10.1109/SEGE.2019.8859917.

[2] Yang L, Chen X, Zhang J, et al. Optimal privacy-preserving energy management for smart meters[M]. 2014.

[3] Rubio J E, Alcaraz C, Lopez J. Recommender system for privacy-preserving solutions in smart metering[J]. Pervasive & Mobile Computing, 2017.

[4] Wang, Xiaoyan; Xu, Zhenquan; Cai, Ziwei; Wang, Tao, Novel Temporal Perturbation-Based Privacy-Preserving Mechanism for Smart Meters[J]. MOBILE NETWORKS & APPLICATIONS,2019

[5] Liu, Xuefeng, Zhang, Yuqing, Wang, Boyang,. An anonymous data aggregation scheme for smart grid systems[J]. Security and Communication Networks, 7(3):602-610.

[6] Gong Fan. Smart grid electricity consumption statistics and electricity bill payment scheme based on group signature[D]. Xidian University, 2013.

[7] Wang Wei. Smart grid payment scheme based on ring signature and certificateless signature[D]. 2015.

[8] Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)[C]// Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1997.

[9] Backes M, Meiser S. Differentially Private Smart Metering with Battery Recharging[M]//Data Privacy Management and Autonomous Spontaneous Security. Springer Berlin Heidelberg, 2014:194-212.

[10] Dwork C. Differential Privacy[C]//International Collo- quium on Automata, Languages, and Programming. Springer, Berlin, Heidelberg, 2006:1-12.

[11] Ács G, Castelluccia C. I Have a DREAM! (DiffeRentiallyprivatEsmArt Metering)[C]// International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 2011: 118-132.

[12] Zhai Feng, Xu Wei, Feng Yun, et al. Design of improved Paillier algorithm for smart meter privacy protection scheme[J]. Electric Power Information and Communication Technology, 2016(12):52-57.

[13] Fengjun Li, Bo Luo, Peng Liu. Secure Information Aggregation for Smart Grids Using Homomorphic Encryption[C]// Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010.

[14] ZekeriyaErkin, Gene Tsudik. Private Computation of Spatial and Temporal Power Consumption with Smart Meters[M]// Applied Cryptography and Network Security. 2012.

[15] Li Qi, Chen Jie. Aggregation scheme with privacy protection function in smart grid[J]. Smart Grid, 2014(02):12-19.

[16] Y.Zheng.Digitalsigncryption or how to achieve cost (signature&encryption) cost(signature) +cost(encryption). Advances in Cryptology-Crypto'97, LNCS 1294, Springer-Verlag, 1997:165-179.

[17] Huang Xinyi, Susilo W, Mu Yi. Identity-based ring signcryptionschemes:cryptographic primitives for preserving privacy and authenticity in the ubiquitous words[C].Advanced Information Networking and Application,2005:649-654.