Internet of Things (IoT) and Engineering Applications (2019) 4: 1-6
Clausius Scientific Press, Canada
DOI: 10.23977/iotea.2019.41001
ISSN 2371-8617

An Electricity Blockchain Transaction Privacy Protection Scheme based on Homomorphic Encryption

Zhang Shaomin[a], Zhang Qiqi[b], Wang Baoyi[c]

School of Control and Computer Engineering, North China Electric Power University, Baoding 071003, China
[a]zhangshaomin@126.com, [b]zhangqiqi0952@163.com, [c]wangbaoyi@126.com

Keywords: decentralization, blockchain, smart contract, privacy protection, additional homomorphic encryption, LWE

Abstract: An electricity blockchain based on smart contract is designed by introducing decentralization into smart grid in this paper. The data in blockchain may reveal user privacy due to transparency. Therefore, a blockchain privacy protection scheme based on additive homomorphic encryption algorithm is proposed. The electricity and account balance of users are encrypted by the homomorphic encryption algorithm in the scheme to realize the confidentiality of data ensuring electricity billing. Finally, the security of the scheme is proved and the performance of the scheme is analyzed. The encryption algorithm of the scheme has less computational complexity and higher efficiency.

1. Introduction

At present, the centralized processing method is adopted to settle the electricity bills of users. The grid company settles the electricity bill based on the power consumption data sent by the smart meter, and then feeds back the monthly billing result to the user. Users can't get their own power consumption information in time, which is not conducive to users' control of real-time power consumption. In addition, it is less efficient for the grid company to transfer data over long distances and process large amounts of user power data in a centralized method. Simultaneously, When the centralized organization fails, all billing services need to be stopped. So the safety of the centralized method is too dependent on the central organization. In response to these problems, this paper introduces the idea of decentralization, and adopts blockchain technology to construct the electricity blockchain based on smart contract.

Blockchain technology is born out of bitcoin. In the paper titled Bitcoin: A Peer-to-Peer Electronic Cash System published by Satoshi Nakamoto in 2008, blockchain was proposed as the core underlying technology of the Bitcoin system[1]. Blockchain technology is rapidly becoming the focus of attention of governments, international organizations, large consortia and scientific research institutions due to its decentralization, anonymity, verifiability, and tamper resistance. Various blockchain projects are emerging one after another[2,3]. The data in the blockchain is mostly transparent (such as bitcoin) to ensure the verifiability of the data. An attacker can analyze the transaction records to determine the association between multiple accounts in the blockchain, and even determine the true identity of the trader. This is a huge threat to the privacy of blockchain [4,5].

At present, there are two main aspects of privacy protection in the blockchain, namely, identity privacy protection and transaction privacy protection[6]. Traditional digital currencies use the "coinjoin" mechanism to protect user identity privacy. In addition, many people introduce cryptographic tools into digital currencies, such as ring signatures, zero-knowledge proofs and so on.

Ring signature technology is introduced to CryptoNote[7], Monero[8], etc. Anonymous collections are used to protect privacy. Essentially the real trading behaviors are just hiden in an anonymous collection. In practice, if the user improperly selects an anonymous collection, it will also cause anonymity and privacy protection. For example, Miler et al. analyze Monero's transaction records, indicating that 80% of Monero is linkable[9].

Zerocoin[10] and Zerocash[11] use zero-knowledge proof technology to protect privacy of users. Zero-knowledge proof technology is slow and inefficient although it has high security. For example, Zerocash adopts the simple non-interactive zero-knowledge proof technique zk-SNARKs[12], which usually takes 1 minute to generate a certificate.

There is the user's real-time power usage data in the electricity blockchain, which is closely related to the user's privacy[13]. The criminals can infer the personal information of the user's personal hobbies and lifestyles by analyzing the actual data associated with the user. Therefore, the paper designs a privacy protection scheme based on the power blockchain. In this paper, the BGN-type addition homomorphic encryption algorithm based on LWE is used to encrypt the power consumption and account balance, and the confidentiality of the data can be guaranteed when the electricity billing can be completed.

2. Design of Power Blockchain Privacy Protection Scheme Based on Homomorphic Encryption

2.1. Design Ideal

Traditionally, smart meters upload the user's real-time electricity to the control center (CC) of the grid company, and the CC bills are uniformly settled by the CC. And the electricity billing is uniformly performed by the CC. This method has high dependence on CC. And the real-time performance is poor and the efficiency and security is low. The decentralization idea is introduced and the electricity blockchain is designed. Smart meters publish electricity of user to the blockchain network, and smart contracts enable electricity bills to be settled, improving real-time and efficiency. The transparency of blockchain data threatens the privacy of users. This paper proposes a scheme to protect user privacy by using homomorphic encryption technology based on the power blockchain. The smart contract encrypts the user's real-time electricity data released by the smart meter and writes it into the blockchain. No user can read plaintext directly from the blockchain. Smart contracts implement electricity billing and value transfer on ciphertext.

2.2. Design of Electricity Blockchain

In the power blockchain, each account address corresponds to a user and a smart meter. The real-time electricity data of the user is saved in the blockchain. The smart contract encrypts the real-time electricity data, and performs electricity billing and value transfer according to the electricity and electricity price to determine whether the user is in arrears. In the electricity blockchain, the account balance is allowed to be negative, which means that the account is in arrears and the value transfer can still be carried out. Smart contract issues arrears message to users when account balance is negative. The architecture is shown in Figure 1.

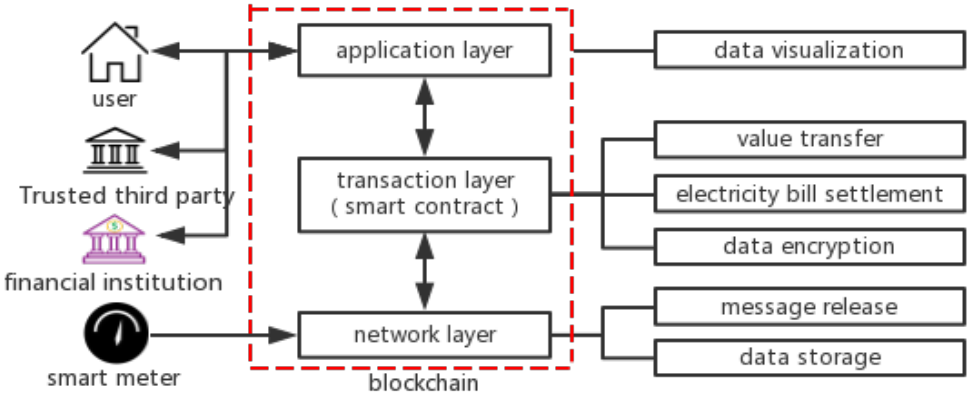

Figure 1: Electricity blockchain architecture diagram

2.3. Design of Smart Contract

A smart contract is a piece of code stored in the blockchain[14] that is automatically executed when an event triggers a clause. In the scheme of this paper, the functions of the smart contract are as follows: (1) data encryption, encrypting the user's account balance and electricity data according to the user's public key, and then saving the ciphertext to the blockchain; (2) electricity billing, calculating electricity charges according to the electricity and price; (3) value transfer, updating user account balance according to calculated electricity charges and then completing value transfer.

3. Implementation of Power Blockchain Privacy Protection Scheme Based on Homomorphic Encryption

3.1. Data Encryption

3.1.1. Initialization

Assume that the security parameter of the system is n, and other parameters include Odd prime number q=poly(n), large enough integer m=O($n$log$q$), prime number $p>n^{3\varepsilon+1}\cdot\log^5 n$ satisfying $p<q<p^3$ and Gaussian noise distribution parameter β=poly(n). Public key matrix is $\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$. Private key matrix is $\boldsymbol{R}\in\boldsymbol{Z}_q^{m\times m}$ which is reversible. And its inverse matrix is $\boldsymbol{R}^{-1}$.

3.1.2. Key Generation

According to Lemma 1, a random matrix $\boldsymbol{A}\in\boldsymbol{Z}_q^{n\times m}$ and a trapdoor matrix $\boldsymbol{R}\in\boldsymbol{Z}_q^{m\times m}$ satisfying $\boldsymbol{AR}=\boldsymbol{0}(\mathrm{mod}\ q)$ can be obtained as the public key matrix and the private key matrix by the trapdoor generation algorithm GenTrap[15]. Immediately, $(\boldsymbol{A},\boldsymbol{R})$=GenTrap$(1^n,1^m,q)$.

3.1.3. Encryption

The data that this scheme needs to encrypt includes the meter data and account balance of the user U marked as $b<mp$. Encode plaintext data b as a vector $\boldsymbol{b}=\left(b_1,\ldots,b_m\right)^t\in\boldsymbol{Z}_p^m$ satisfying $b=\sum_{i=1}^m b_i$. Select a vector $\boldsymbol{s}$ subjecting to random uniform distribution from $\boldsymbol{Z}_q^n$. Select an error vector $\boldsymbol{e}\in\boldsymbol{Z}_q^m$ from $\boldsymbol{\Psi}_\beta^m(q)$. According to the plaintext vector $\boldsymbol{b}\in\boldsymbol{Z}_p^m$, calculate the ciphertext

vector $\boldsymbol{c}^t = \boldsymbol{s}^t\boldsymbol{A}+p\boldsymbol{e}^t+\boldsymbol{b}^t(\text{mod } q)$. And then output ciphertext vector $\boldsymbol{c} \in \boldsymbol{Z}_q^m$.

3.1.4. Decryption

Calculate $\boldsymbol{v}^t = \boldsymbol{c}^t\boldsymbol{R}(\text{mod } q)$ and then $\boldsymbol{b}^t = \boldsymbol{v}^t\boldsymbol{R}^{-1}(\text{mod } p)$. So, plaintext $b = \sum_{i=1}^m b_i$.

Proof: At first, let $\boldsymbol{v}^t=\boldsymbol{c}^t\boldsymbol{R}(\text{mod } q)=(\boldsymbol{s}^t\boldsymbol{A}+p\boldsymbol{e}^t+\boldsymbol{b}^t)\boldsymbol{R}(\text{mod } q)=(p\boldsymbol{e}^t+\boldsymbol{b}^t)\boldsymbol{R}(\text{mod } q)$. If the parameter q=poly(n) is large enough and the Gaussian noise distribution parameter β=poly(n) is small enough that each element in $p\boldsymbol{e}^t+\boldsymbol{b}^t$ is less than q, then $\boldsymbol{v}^t\boldsymbol{R}^{-1}(\text{mod } p)=(p\boldsymbol{e}^t+\boldsymbol{b}^t)\boldsymbol{R}(\text{mod } q)\boldsymbol{R}^{-1}(\text{mod } p)=p\boldsymbol{e}^t+\boldsymbol{b}^t(\text{mod } p)=\boldsymbol{b}^t$ and $b = \sum_{i=1}^m b_i$.

3.1.5. Homomorphic Analysis

Theorem 1 The BGN-type encryption algorithm based on DLWE problem[15,16] in this paper has the characteristics of additive homomorphism.

Proof: For any given two ciphertexts $\boldsymbol{c}_1{}^t=\boldsymbol{s}_1{}^t\boldsymbol{A}+p\boldsymbol{e}_1{}^t+\boldsymbol{b}_1{}^t(\text{mod } q)$ and $\boldsymbol{c}_2{}^t=\boldsymbol{s}_2{}^t\boldsymbol{A}+p\boldsymbol{e}_2{}^t+\boldsymbol{b}_2{}^t(\text{mod } q)$, the corresponding plaintext are $\boldsymbol{b}_1{}^t=(b_{11},\ldots,b_{1m})^t$ and $\boldsymbol{b}_2{}^t=(b_{21},\ldots,b_{2m})^t$, $b_1 = \sum_{i=1}^m b_{1i}$ and $b_2=\sum_{i=1}^m b_{2i}$. Just need to prove that $\boldsymbol{c}^t=\boldsymbol{c}_1{}^t+\boldsymbol{c}_2{}^t(\text{mod } q)$ can be decrypted to $\boldsymbol{b}^t=\boldsymbol{b}_1{}^t+\boldsymbol{b}_2{}^t$, and then $b = \sum_{i=1}^m \left(b_{1i}+b_{2i}\right) = \sum_{i=1}^m b_{1i} + \sum_{i=1}^m b_{2i} = b_1 + b_2$. And $\boldsymbol{c}^t=\boldsymbol{c}_1{}^t+\boldsymbol{c}_2{}^t(\text{mod } q)=(\boldsymbol{s}_1{}^t+\boldsymbol{s}_2{}^t)A+p(\boldsymbol{e}_1{}^t+\boldsymbol{e}_2{}^t)+(\boldsymbol{b}_1{}^t+\boldsymbol{b}_2{}^t)$ (mod q). Let $\boldsymbol{s}^t=\boldsymbol{s}_1{}^t+\boldsymbol{s}_2{}^t$, $\boldsymbol{e}^t=\boldsymbol{e}_1{}^t+\boldsymbol{e}_2{}^t$ and $\boldsymbol{b}^t=\boldsymbol{b}_1{}^t+\boldsymbol{b}_2{}^t$, then $\boldsymbol{c}^t=\boldsymbol{s}^t\boldsymbol{A}+p\boldsymbol{e}^t+\boldsymbol{b}^t(\text{mod } q)$. Obviously, $\boldsymbol{s}^t \sim U\left(\boldsymbol{Z}_q^n\right), \boldsymbol{e}^t \sim \Psi_\beta(q)$. While the selected parameter q is large enough that each element of $p\boldsymbol{e}^t+\boldsymbol{b}^t$ is less than q, $\boldsymbol{b}^t=\boldsymbol{b}_1{}^t+\boldsymbol{b}_2{}^t$ can be gotten by decryption. In the same way, the additive homomorphism of polynomial times can be proved.

For subtraction, $\boldsymbol{b}^t=\boldsymbol{b}_1{}^t-\boldsymbol{b}_2{}^t$ can be decrypted by $\boldsymbol{c}^t=\boldsymbol{c}_1{}^t-\boldsymbol{c}_2{}^t(\text{mod } q)$. If any elements of $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are not greater than $q/2$, the size of the corresponding element of $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ can be judged according to the value of the element of $\boldsymbol{b}$. if $b_i \le q/2 (i=1,\ldots,m)$ which is the element of $\boldsymbol{b}$, then $b_{1i} \ge b_{2i}$ and $b_{1i} < b_{2i}$ otherwise.

3.2. Electricity Billing

Assume that the period in which the smart meter releases the power data is ΔT, and for the user U, the current power is Q_1, ciphertext is $\boldsymbol{c}_1$, the last power is Q_2, ciphertext is $\boldsymbol{c}_2$, and price is P. According to the encryption homomorphism of the encryption algorithm, for the power of the user U during ΔT, the ciphertext is $\boldsymbol{c}=\boldsymbol{c}_1-\boldsymbol{c}_2$, the plaintext is $\boldsymbol{b} = (b_1, b_2, \cdots, b_m)^t \in \boldsymbol{Z}_p^m$ and the actual electricity is $Q = \sum_{i=1}^m b_i$. The electricity billing formula is $\Delta\boldsymbol{d}=P\boldsymbol{c}=P\boldsymbol{s}^t\boldsymbol{A}+Pp\boldsymbol{e}^t+P\boldsymbol{b}^t(\text{mod } q)$. Decrypted plaintext is $P\boldsymbol{b}^t=(Pb_1,\ldots,Pb_m)^t$. The actual electricity bill is $\sum_{i=1}^m Pb_i = PQ$.

3.3. Value Transfer

Suppose that the ciphertext of the user U's actual electricity bill is $\Delta\boldsymbol{d}=P\boldsymbol{c}$, account balance ciphertext is $\boldsymbol{d}_u$, grid company account balance ciphertext is $\boldsymbol{d}_s$. Update the balance $\boldsymbol{d}_u \leftarrow \boldsymbol{d}_u - \Delta\boldsymbol{d}$ and $\boldsymbol{d}_s \leftarrow \boldsymbol{d}_s - \Delta\boldsymbol{d}$.

KGC decrypts $\boldsymbol{d}_u$ and $\boldsymbol{d}_s$ periodically. Suppose $\boldsymbol{d}_u$ and $\boldsymbol{d}_s$ are decrypted as $\boldsymbol{b}_u=(b_{u1},\ldots,b_{um})^t$ and $\boldsymbol{b}_s=(b_{s1},\ldots,b_{sm})^t$. Calculate the account balance of users $b_u=\sum_{i=1}^m b_{ui} - kq$ in which k is the number of elements greater than $q/2$ in $\boldsymbol{b}_u$. It means that the user's electricity fee is owed if $b_u<0$.

4. Security Proof and Performance Analysis

4.1. Security Proof

The security of the scheme in this paper is based on the difficulty of the DLWE problem[15,16] and meets the IND-CPA security.

Theorem 2. If there is a distinguishable algorithm that can crack the encryption algorithm whose parameters n, m, p, q, β of this paper with a non-negligible advantage ε, a distinguisher $\mathcal{D}$ can be constructed with this distinction algorithm to solve the DLWE problem whose parameters n, m, p, q, β with advantage at least $\varepsilon/2m$ in the same time. Then the algorithm is said to be CPA security.

Proof: Let $\mathcal{A}$ be a CPA-adversary which can distinguish ciphertexts of different plaintexts with a non-negligible probability ε. We first construct a distinguisher $\mathcal{D}$ with advantage at least $\varepsilon/2$ between the two distributions $\left\{\left(\boldsymbol{A}, \boldsymbol{s}^t\boldsymbol{A}+\boldsymbol{e}^t\right): \boldsymbol{A}\in \boldsymbol{Z}_q^{n\times m}, \boldsymbol{s}\in \boldsymbol{Z}_q^n, \boldsymbol{e}\sim \boldsymbol{\Psi}_\beta^m(q)\right\}, \left\{U\left(\boldsymbol{Z}_q^{n\times m}\times \boldsymbol{Z}_q^m\right)\right\}$.

Given the input $\left(\boldsymbol{A}\in \boldsymbol{Z}_q^{n\times m}, \boldsymbol{c}^t\in \boldsymbol{Z}_q^m\right)$, run the adversary $\mathcal{A}$ with $\boldsymbol{A}$ as the public key. Upon receiving the plaintext message $\boldsymbol{b}_0\in \boldsymbol{Z}_p^m$ and $\boldsymbol{b}_1\in \boldsymbol{Z}_p^m$ from $\mathcal{A}$, $\mathcal{D}$ chooses $k\in_R\{0,1\}$ at random, returns the challenge ciphertext $p\boldsymbol{c}^t+\boldsymbol{b}_k{}^t(\text{mod } q)$. And then let $\mathcal{A}$ guess the challenge ciphertext and output k'. If $k'=k$, guess correctly , then output 1 and 0 otherwise.

On the other hand, if the ciphertext vector $\boldsymbol{c}$ is taken from the uniform distribution $U\left(\boldsymbol{Z}_q^m\right)$, the challenge ciphertext is also subject to uniform distribution. The probability that the $\mathcal{D}$ output 1 is 1/2. If $\boldsymbol{c}^t=\boldsymbol{s}^t\boldsymbol{A}+\boldsymbol{e}^t(\text{mod } q)$, challenge ciphertext is $p\boldsymbol{c}^t+\boldsymbol{b}^t=\boldsymbol{s}_1{}^t\boldsymbol{A}+p\boldsymbol{e}^t+\boldsymbol{b}^t(\text{mod } q)$ in which $\boldsymbol{s}_1{}^t=p\boldsymbol{s}^t(\text{mod } q)$ is uniformly randomly distributed because p and q are mutually different prime numbers. So, the probability that $\mathcal{A}$ can correctly guess k is $(1+\varepsilon)/2$ by CPA attack ability of $\mathcal{A}$. Then the probability that $\mathcal{D}$ outputs 1 is $(1+\varepsilon)/2$.

In summary, the probability that $\mathcal{D}$ can correctly distinguish two distributions is at least $\frac{1}{2}\varepsilon/2+\frac{1}{2}(1+\varepsilon)/2=\frac{1}{2}+\varepsilon/2$. That is, the advantage is not less than $\varepsilon/2$. Therefore, the advantage of using the distinguisher $\mathcal{D}$ to solve the DLWE problem with parameters n, m, p, q, β is not less than $\varepsilon/2m$.

4.2. Performance Analysis

Table 1: Space performance analysis table

Algorithm	Plaintext space	Ciphertext space	Public key space	Private key space
The paper[17]	$\boldsymbol{Z}_2^{m\times m}$	$\boldsymbol{Z}_q^{m\times m}$	$\boldsymbol{Z}_q^{m\times n}$	$\boldsymbol{Z}_q^{m\times m}$
The paper[18]	$\boldsymbol{Z}_p^{m\times m}$	$\boldsymbol{Z}_q^{m\times m}$	$\boldsymbol{Z}_q^{m\times n}$	$\boldsymbol{Z}_q^{m\times m}$
This paper	$\boldsymbol{Z}_p^m$	$\boldsymbol{Z}_q^m$	$\boldsymbol{Z}_q^{m\times n}$	$\boldsymbol{Z}_q^{m\times m}$

Table 2: Calculation performance analysis table

Algorithm	Addition		Multiplication		Modular	
	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
The paper[17]	$(n+1)m^2$	$4(m-1)m^2$	$(n+1)m^2$	$4m^3$	m^2	$2m^2$
The paper[18]	$(n+1)m^2$	$2(m-1)m^2$	$(n+1)m^2$	$2m^3$	m^2	$2m^2$
This paper	$(n+1)m$	$2(m-1)m$	$(n+1)m$	$2m^2$	m	$2m$

In the homomorphic encryption algorithm, vectors and matrices participate in the operation including matrix multiplication, matrix addition, and modulo operations, no exponential operation.

Therefore, the algorithm has less computational complexity and higher efficiency. Software and hardware implementation is easier. Compared with the algorithms in the paper [17] and [18], the results are shown in Table 1 and Table 2.

5. Conclusion

In this paper, the decentralization idea is introduced into the grid electricity billing, and the electricity blockchain based on smart contract is designed. Since blockchain data is transparent and the electricity data may disclose the privacy of the user, this paper proposes a privacy protection scheme based on additive homomorphic encryption. The scheme can protect the privacy of users while realizing electricity billing. Finally, the security of the encryption algorithm is proved and its performance is analyzed. In this scheme, the encryption, decryption and storage of data are in the form of a matrix which consumes a large amount of storage space in spite of less calculation and high efficiency. Therefore, the next step is to reduce the space consumption of the encryption algorithm.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] WANG Anping, FAN Jingang, GUO Yanlai. Application of Blockchain in Energy Interconnection [J]. Electric Power Information and Communication Technology,2016(9): 1-6(in Chinese).

[3] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain application development techniques. Ruan Jian Xue Bao/ Journal of Software, 2017,28(6):1474−1487 (in Chinese).

[4] WANG Hao, SONG Xiangfu, KE Junming,et al. Blockchain and Privacy Preserving Mechanisms in Cryptocurrency [J]. Netinfo Security, 2017(7):32-39(in Chinese).

[5] Liao K, Zhao Z, Doupe A, et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin[C]// Electronic Crime Research. IEEE, 2016:1-13.

[6] Zhu Liehuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. Survey on Privacy Preserving Techniques for Blockchain Technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.

[7] Bergan T, Anderson O, Devietti J, et al. CryptoNote v 2.0 [J]. 2013.

[8] Monero. About monero [EB/OL]. [2017-11-08]. https://getmonero.org/resources/about/

[9] Miller A, Moeser M, Lee K, et al. An Empirical Analysis of Linkability in the Monero Blockchain[J]. 2017.

[10] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin [J]. IEEE Symposium on Security & Privacy, 2013:397-411.

[11] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2014:459-474.

[12] Ben-Sasson E, Chiesa A, Genkin D, et al. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge[M]// Advances in Cryptology – CRYPTO 2013. Springer Berlin Heidelberg, 2013:90-108.

[13] Guo Xiaoli, Zhang Jiajia, Wang XiuLei.The research and application of information privacy protection method for smart grid users [J]. Electrical Measurement & Instrumentation, 2016, 53(24):94-99.

[14] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain Application Development Techniques[J]. Journal of Software, 2017, 28(6): 1474-1487(in Chinese).

[15] C. Peikert. Publi-key Cryptosystems from the worst-case shortest vector problem: extended abstract[C]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, 2009, 333-342.

[16] O. Regev. On lattices, learning with errors, random linear codes, and cryptography[C]. Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005, Baltimore, MD, USA, 2005, 84-93.

[17] Gentry C,Halevi S,Vaikuntanathan V.A Simple BGN-type Cryptosystem from LWE [C] //Proceedings of the29th Annual International Conference on the Theory andApplications of Cryptographic Techniques. Berlin,Germany: Springer,2010: 506-522.

[18] WU Guangxian, LIU Nianyi, LIU Boya. Design and Application of BGN-type CPA Secure Encryption Scheme Based on LWE. Computer Engineering, 2016, 42(12): 118-123(in Chinese).