ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0012

Attribute Homomorphic Encryption Scheme Based Lattice on AMI

Baoyi Wang*, Zichen Tian, Shaomin Zhang

North China Electric Power University, Hebei 071000, China.

Abstract

With the development of smart grid, the Advanced Meter Infrastructure (AMI) is faced with the problems such increasing data collection and more frequency collection. Meanwhile, in order to improve user's participation and save power resources, the reliability and security of network communication are further challenged. The 5G network has the characteristics of large bandwidth, low power consumption and low delay, so it is imperative to build a network structure to meet the needs of AMI communication. The 5G network slicing takes full advantage of network virtualization and general API programming to allocate various hardware resources. With the further implementation of 5g network and the increase of information data collection, the risk of user privacy data exposure increases. In order to deal with the traditional problem of user privacy protection under the new network slice architecture, we need to further strengthen the protection of user privacy while building the corresponding slice network and slice resource management.

Keywords

DLWE based-on Shortest Lattice; Attribute Fully Homomorphic Encryption; Privacy Protection.

1. Introduction

With the recent technology trending such as communication, big data, cloud compute, smart infrastructure and internet of thing (IoT),the connectedness between the people ,processes, data and things is revolutionizing the usage about control , monitor and acquisition of electricity information over the electrical grid[1]. Therefore, traditional power grid is gradually replaced by smart grid, which can satisfied the two-way communication between public utilities and users, demand response, electri-city theft detection and other functions.

The advanced meter infrastructure (AMI) which plays an important role in smart grid provides periodic and high-frequency data collection to monitor various states of entities, such as power consumption, load balancing, resource allocation, etc. this kind of fine-grained energy related data can support intelligent distribution, energy consumption regulation and energy management. However, this large amount of data interaction brings higher privacy exposure risk, so that there are many articles on this problem. At present, the privacy protection methods of smart grid can be divided into non-password and password-based methods.

However, the existing research on privacy protection seldom considers quantum security, and quantum computing technology is developing rapidly [2]. Lattice based cryptography is a kind of classical post quantum cryptography, which is recognized as the most powerful competitor of post quantum cryptography algorithm standard [3]. Combined with the current situation and related network topology, based on the current AMI data aggregation scheme, this paper proposes an attribute based fully homomorphic encryption algorithm to achieve privacy protection in AMI communication network.

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0012

2. Methodology

The communication network in AMI is composed of smart meter, data concentrator, communication carrying network and data monitoring management system, and its structure is as follows:

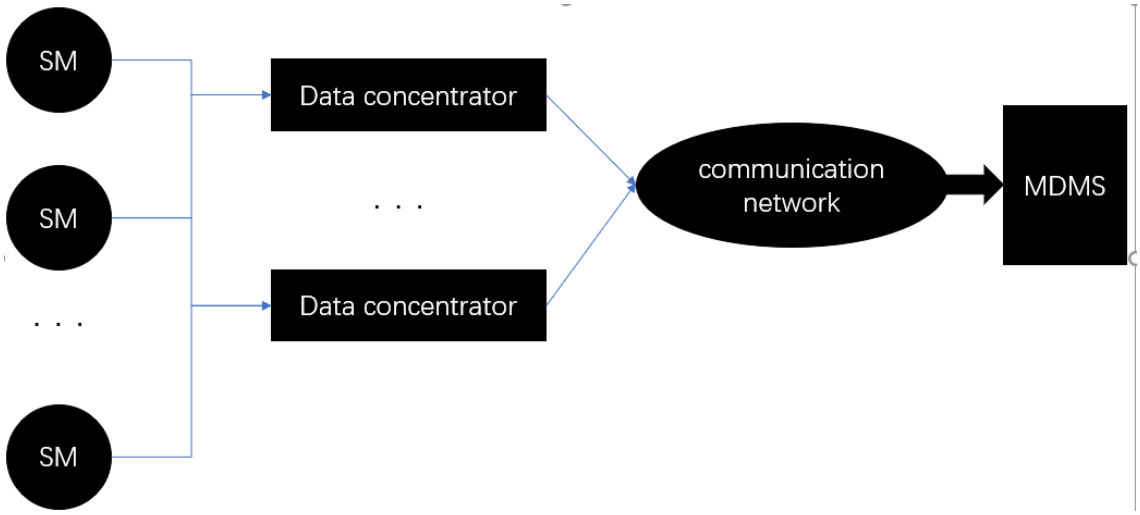

Figure 1. AMI communucation network

As shown in Figure 1, the data exchange in AMI network is that multiple smart meters are uploaded to the data concentrator. The data concentrator obtains and integrates the corresponding meter data, and then packages and sends the data to the measurement data management system by the com-munucation network which is generally attached to the wireless network provided by the communication service provider, thus we can call the network slice to use the communication resources in the wireless network, to reduce the system overhead and improve the reliability of the communication network.

2.1. System initialization algorithm

In the initial algorithm of the system, the power grid company generates a security parameter (1^n) for a specific data concentrator and sends it to the communication network with the identity information DH of the corresponding concentrator, and generates a public parameter Pp and master key Mk:

(1) The network slice transforms the concentrator identity information DH into a label matrix H and makes h equal to an identity matrix. The auxiliary matrix G_n is called and a random uniform distribution matrix $A=[A'|G_n-A'T_A] \in \mathbb{Z}_q^{n\times m}$ is generated randomly, where T_A is a access policy function of a joint H. Generate a matrix pair (a, T_A)

(2) Then, K random uniform matrices $B_i \in \mathbb{Z}_q^{n\times n}$ are generated as the common class of corresponding attribute values of each meter.

(3) Select a uniform random vector $u \epsilon \mathbb{Z}_q^n$.

(4) Output public parameter $Pp= \{A,B_{i(1\le i\le k)},u\}$ and public key Mk = (T_A) and transfer them to the corresponding data concentrator

2.2. Meter private key generation

A meter registers with the corresponding gateway, sends a registration request, and the concentrator sends the obtained public parameter Pp, main public key Mk, and security

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0012

parameter (1^n) of the corresponding power grid to the corresponding meter. The meter generates the corresponding private key Sk.

(1) For the security parameter (1^n), the corresponding attribute u = PUF (1^n) is generated by physical non clonable function and sent to the data concentrator to generate the threshold value W, and an attribute column L = {Li} (Li ∈ Si) is generated.

(2) The label H = $\sum_{\forall v_{i,j} \in L} B_i H(v_{i,j})$ is obtained by calculating each attribute value on L, where H (x) is a full rank hash function $\mathbb{Z}_q^n \rightarrow \mathbb{Z}_q^{n \times n}$ that can be calculated in polynomial time (nLogq).

(3) Let H' be H minus an identity matrix, and calculate A_L=A+[0|$B_L G_n$]=[A'|H'G_n-A'T_A]

(4) Add a Gaussian parameter σ to H', G_n, T_A, Uand σ The output vector $r_L \in \mathbb{Z}_q^{\overline{m}+\overline{n}}$ satisfies H'r_L=u.

(5) Output Sk = {r_L} as the private key for the meter.

2.3. Electricity information encryption

When the meter needs to send data to the data concentrator, it needs to match the threshold value first, and then obtain the corresponding access rights to encrypt the user data and send the ciphertext to the data concentrator.

(1) For each attribute in the threshold value W, H_w' = $\sum_{\forall v_{i,j} \in W} B_i H\left(v_{i,j}\right)$, H_W is calculated as H_W' minus an identity matrix, and A_W=A+[0|$B_w G_n$]=[A'| $B_w G_n$-A'T_A]

(2) Select a random uniform matrix $S \in \mathbb{Z}_q^{n \times M}$.

(3) An error matrix E = (e_1,..., e_M) and an error term e_0 are generated from a distribution $\mathfrak{X}^M$,and send it to the corresponding meter.

(4) The meter calculates the ciphertext of power consumption information

$$C=\begin{bmatrix} \mathbf{u}^T \\ \mathbf{A}_W^T \end{bmatrix} s+\begin{bmatrix} e_0^T \\ E \end{bmatrix}+plmesG \in \mathbb{Z}_q^{(1+m)\times M} \pmod q$$

2.4. Data aggregation encryption

The data concentrator obtains the ciphertext data C sent by the meter, and outputs a new ciphertext data cmesf by combining with the ciphertext data {C_1,...,C_i} sent by other k-1 meters, and satisfies decrypt (Pp, C_f, SK_L) = f (M_1, M_2,..., M_i). The ciphertext satisfies the

1.additive homomorphism: $C_f^+ = C_1 + C_2$

2.multiplicative homomorphism: $C_f^{\times}=C_1 \cdot G^{-1}(C2)$

Then the multiplication result of K ciphertext homomorphisms is:

$$C_f= C_1 \cdot G^{-1}(C_2 \cdot G^{-1}(\cdots C_{k-1} \cdot G^{-1}(C_k)))$$

2.5. Decryption

The data concentrator uploads the collected data to the communication network, and the network slice detects it. After calculation, it matches the corresponding information and confirms that the information is uploaded by the correct gateway or data concentrator. Then, the corresponding public parameter Pp, ciphertext C and the corresponding master keyMk are aggregated to decrypt the data, so as to obtain the corresponding power consumption data plmes

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0012

(1) Corresponding to the attribute value in the attribute list and the master key, a matrix v=(1;-Mk) $\in \mathbb{Z}_q^{l+m}$

(2) g_i is defined as the i-th column of G, C_i is the i-th column of C. At the same time, according to the i-th element e_i of error matrix E, it is calculated:

$$x_i=v^T Cimes_i=plmes_i\, v^T g_i+v^T\begin{bmatrix} e_i \\ e_0 \end{bmatrix}.$$

(3) The plaintext data $M_i=[x_{i-1}/g_{i-1}]$ is obtained.

3. Security Analysis

3.1. Accuracy of encryption algorithm

According to the homomorphism of the above encryption algorithm, we can calculate the following:

$$v^T(C_1+C_2) = (M_2+M_1)v^T G+ v^T(\overline{E_1}+\overline{E_2})$$
$$v^T(C_1\cdot G^{-1}(C_2))= M_1 v^T M_2 v^T G+ v^T(M_1\overline{E_2}+\overline{E_1}\cdot G^{-1}(C_2))$$

At the same time, we can see that the error term after calculation depends on the original error term, M_1 and G^{-1}, where G^{-1} is a matrix of $M\{0,1\}^{M\times M}$, so the growth value depends significantly on M_1.Thus the increase and change of error mainly depends on homomorphic multiplication. In order to ensure the accuracy of encryption, we carry out homomorphic multiplication of multiple ciphertexts:

$$v^T C_1\cdot G^{-1}(C_2\cdot G^{-1}(\cdots C_{k-1}\cdot G^{-1}(C_k)))=P_1P_2\cdots P_k v^T G+v^T\overline{E_f},$$

Then we set $\overline{E_{f,i}}$ is the i-th column of $\overline{E_f}$, $\overline{E_i}=\begin{bmatrix} e_{0,i} \\ e_i \end{bmatrix}$ is the i-th column of $\overline{E}$, and based on the Electricity information encryption we can calculate the following:

$$P_f=\left[\frac{v^T C_{f,t-1}}{g_{t-1,1}}\right]=\left[\frac{P_f g_{t-1,1}+v^T\overline{E_{f,t-1}}}{g_{t-1,1}}\right]=\left[P_f+\frac{v^T\overline{E_{f,t-1}}}{g_{t-1,1}}\right]$$

Therefore, in order to ensure the accuracy of the encryption algorithm, it must be $\frac{v^T\overline{E_{f,t-1}}}{g_{t-1,1}}$ less than 1/2, as the error $v^T\overline{E_{f,t-1}}$ must be less than q/8.

Then we calculate the error term: $v^T\overline{E_{f,t-1}}\le|vT(O(1)\cdot\sqrt{M}+1)\,\overline{E_{t-1}}|= B(O(1)\cdot\sqrt{M}+1)(1+\sigma m)$.

When the $\sigma\ge\sqrt{m}\omega(\sqrt{\log q})||\widetilde{G_n}||$, it must be that $(O(1)\cdot\sqrt{M}+1)(1+\sigma m)<q/8$, so the accuracy of encryption algorithm is guaranteed.

3.2. Security of encryption algorithm

First, according to the problem $DLWE_{n,q,\chi}$,let's make such an extension: let S = (s1,s2,⋯,sm) $\in \mathbb{Z}_q^{n\times M}$ and A=(a1,a2,⋯,am) $\in\mathbb{Z}_q^{n\times m}$, χ Is a distribution on ℤ, $e_j=(e_{1,j},e_{2,j},\cdots,e_{m,j})^T$ is an error term on χ^m. If problem $DLWE_{n,q,\chi}$ it is true, then(A,A^TS+E) and (A, $\mathbb{Z}_q^{n\times M}$) are indistinguishable in distri- bution.

Proof: Let M =2,if there is a PPT algorithm $\mathscr{F}1$ can easily distinguish the (A,ATS+E) and (A, $\mathbb{Z}_q^{n\times M}$), then we build a PPT algorithm $\mathscr{F}2$ based on $\mathscr{F}1$ to solve the problem DLWEn, q,χ. Samples(A,b1) were extracted from (A, ATs1+e1)and(A, $\mathbb{Z}_q^m$) to form the $\mathcal{A}2$ distribution. $\mathcal{A}2$ random sampling r ∈ {0,1}. When r = 1, $\mathscr{F}2$ random sampling S2 ∈ and error term E2 ⟵ χ m. After calculation, ATs2+e2 is added to the original sample to form a new distribution (A, ATs1+e1, ATs2+e2) When r = 0, then a random uniform vector b2 $\in\mathbb{Z}_q^m$ is selected, and the samples are placed to form (A,b1,b2). Finally, the new element in $\mathcal{A}2$ is input into $\mathscr{F}1$. If $\mathscr{F}1$ determines that the sample comes from (A, $\mathbb{Z}_q^m$, $\mathbb{Z}_q^m$), then $\mathscr{F}2$ can also determine that the same sample comes

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0012

from (A, $\mathbb{Z}_q^m$), similarly, $\mathscr{F}1$ determines that the sample belongs to (a, ATS + e), then $\mathscr{F}2$ can also determine that the sample is distributed in (A,ATs1+e1). If $\mathscr{F}1$ has 1/2 probability to obtain samples, then $\mathscr{F}2$ can solve dlwen, Q, χ The probability is 1/2. According to the above conclusion, the lattice based attribute homomorphism encryption algorithm can resist the chosen plaintext attack

4. Conclusion

As the context shows, the homomorphic encryption algorithm used in this paper has less time cost. The selection of network slice structure makes part of the calculation transferred to the cloud, thus reducing the calculation cost of the meter itself.

Advanced measurement system is an important part of smart grid. The previous network slicing design for power business is based on its power business requirements. Therefore, this AMI network slicing only considers the real-time and accuracy required by its collection business, and does not respond to the challenges in the transmission process. However, this paper only considers the core network slicing to provide certain computing service support and fault handling guarantee for AMI network, and the rest, such as access network slicing and bearer network slicing, are not included in the network structure, so the network structure is immature. In the future research, we need to consider the characteristics of a variety of network slicing to better serve the AMI communication network. At the same time, homomorphic encryption based on immature network also needs to be further optimized when the new chip is added or the network structure is updated, so as to better use network resources and reduce the cost of electricity meter. Increase security.

References

[1] Ji, Z., Li, H., Liu, X., Luo, Y., Chen, F., & Hua, W., et al. (2017). On efficient and robust anonymization for privacy protection on massive streaming categorical information. IEEE Transactions on Dependable & Secure Computing, 14(5), 507-520.

[2] Langlois, A., & D Stehlé. (2015). Worst-case to average-case reductions for module lattices. Designs Codes & Cryptography, 75(3), 565-599.

[3] Sharma, A., & Ojha, V.. (2010). Implementation of cryptography for privacy preserving data mining. International Journal of Database Management Systems, 2(3).

[4] Zhang, P., Jiang, H., Cai, J., Wang, C., & Xu, Q.. (2017). Recent Advances in Lattice-Based Cryptography.

[5] Chen, L., Jordan, S. P., Liu, Y. K., Moody, D., Peralta, R. C., & Perlner, R. A., et al. (2016). Report on Post-Quantum Cryptography.

[6] Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K.. (2017). Survey of security advances in smart grid: a data driven approach. IEEE Communications Surveys & Tutorials.