Identity-Based Key Management Scheme for Smart Grid over Lattice

Wangke Yu, and Shuhua Wang[*]
School of Information Engineering
Jingdezhen Ceramic University
Jingdezhen 333403, China
[e-mail: ywkyyy@163.com, w614sh@126.com]
[*]Corresponding author: Shuhua Wang

Received December 9, 2021; revised November 3, 2022; accepted December 29, 2022; published January 31, 2023

Abstract

At present, the smart grid has become one of the indispensable infrastructures in people's lives. As a commonly used communication method, wireless communication is gradually, being widely used in smart grid systems due to its convenient deployment and wide range of serious challenges to security. For the insecurity of the schemes based on large integer factorization and discrete logarithm problem in the quantum environment, an identity-based key management scheme for smart grid over lattice is proposed. To assure the communication security, through constructing intra-cluster and inter-cluster multi-hop routing secure mechanism. The time parameter and identity information are introduced in the relying phase. Through using the symmetric cryptography algorithm to encrypt improve communication efficiency. Through output the authentication information with probability, the protocol makes the private key of the certification body no relation with the distribution of authentication information. Theoretic studies and figures show that the efficiency of keys can be authenticated, so the number of attacks, including masquerade, reply and message manipulation attacks can be resisted. The new scheme can not only increase the security, but also decrease the communication energy consumption.

Keywords: Smart grid, identity information, key agreement, lattice; security

http://doi.org/10.3837/tiis.2023.01.005 **ISSN : 1976-7277**

1. Introduction

With the continuous development of information technology, computer technology, artificial intelligence, big data, and industrial automation technology, computer network technology is widely used in the field of industrial control [1-5]. Ordinary smart grid users can view and manage other electric devices at home through the meter, and equipment maintainers upgrade and maintain the grid devices by upgrading them. Depending on the functions of the grid customers in the smart grid, the grid users have different access rights to the smart devices, and in this smart grid system with multiple devices can access these grid devices accordingly according to the needs of the grid customers in different roles and modification operations according to the needs of different roles of grid customers [6-10]. Quantum computing will potentially enable the computational power of ordinary computers to greatly exceed the present computational power, and in 1997, Shor et al. proposed quantum algorithms for solving the decomposition of large integers and discrete logarithms and demonstrated that the time complexity of their algorithmic operations is of polynomial level [11]. With the development of quantum computing and quantum computers, it is gradually found that the difficult problems currently used in traditional asymmetric cryptographic regimes will probably no longer be secure [12-16]. It is essential to study secure asymmetric cryptosystems in the quantum computer environment and has become a key direction and hotspot for research in the current cryptography and information security community. As one of the typical representatives of asymmetric cryptosystems in the post-quantum computer era, the lattice public key cryptosystem occupies an essential position in the field of quantum cryptography [17-25].

In recent years, increasingly scholars have studied security control in smart grid. In 2012, Sankar et al. proposed a signature-based security access scheme using attribute-based public key encryption [26], in which there is only one key distribution center, but the key center must have strong computing power, and with the increase of the number of smart grid node devices, the key center may become the bottleneck of the whole smart grid. In 2014, Zhou et al. proposed a decentralized access control algorithm for the access control problem of smart grid [27], which effectively reduces the generation of grid peaks and can provide automatic demand response. In 2016, Xie et al. proposed to apply cloud computing to the environment of smart grid [28] to reduce the demand for computing power of smart grid devices and use a grid hierarchy with attribute-based encryption scheme to secure information in the smart grid. In 2017, Guan et al. proposed a secure access scheme with delay tolerance using a secret sharing scheme for the unpredictability of sensitive information generated by electricity consumption transactions between smart grid nodes and grid companies [29], in a model of decentralized grid structure, which effectively reduces the computation and communication overhead of smart grid devices.

Currently, key management schemes for smart grids can be classified into two main categories: symmetric cryptographic regime based and asymmetric cryptographic regime based. When a smart grid node is depleted or identified as an illegal node, the smart grid must be cleared and eliminated in time. The key exchange between smart grid nodes is used to ensure the legitimacy of the communicating smart grid nodes, which is a prerequisite for secure smart grid communication. A lot of research work has been done to reduce the computational overhead and energy consumption of asymmetric cryptosystems and to propose a more secure and reasonable key management scheme. A review of smart grid-related security issues can be found in [30-34], among others, for smart grid key management schemes. Using the solid security foundation over lattice and higher computational efficiency, this paper proposes a lattice-based smart grid key management scheme to ensure the security of communication phase by constructing intra and inter-cluster multi-hop routing security algorithms; introducing timestamp parameters and identity-based information to ensure the security of key update phase; using symmetric cryptosystem algorithms for encryption to improve communication efficiency; and using probabilistic output authentication information that makes the distribution of the output authentication information independent of the private key of the authenticated subject.

2. Basic knowledge

Definition 1 Takes *n* ($m \geq n$) linearly independent vectors in the *m*-dimensional vector space, and define the lattice generated by these *n* vectors as

$$\mathcal{L}(b_1, b_2, \ldots b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

Where the vector $b_1, b_2, \ldots b_n$ is called the basis of the lattice. If the dimensional $m \times n$ matrices B , whose column vectors are $b_1, b_2, \ldots b_n$, are defined, then the lattice generated by the matrix B can be defined as

$$\mathcal{L}(\mathrm{B}) = (b_1, b_2, \ldots b_n) = \left\{ \mathrm{B}X \mid X \in \mathbb{Z}^n \right\}.$$

where *n* is the rank of the lattice; *m* is the dimension of the lattice; and the lattice of $m = n$ is a full-rank lattice.

Definition 2 Assume *q* is a prime number, $\mathrm{A} \in \mathbb{Z}_q^{n \times m}$, define:

$$\Lambda_q(\mathrm{A}) = \{\mathrm{e} \in \mathbb{Z}^m : \exists \mathrm{s} \in \mathbb{Z}_q^n, \mathrm{A}^T \mathrm{s} = \mathrm{e} (\bmod q)\}$$

$$\Lambda_q^{\perp}(\mathrm{A}) = \{\mathrm{e} \in \mathbb{Z}^m : \mathrm{Ae} = 0 (\bmod q)\}$$

$$\Lambda_q^{u}(\mathrm{A}) = \{\mathrm{e} \in \mathbb{Z}^m : \mathrm{Ae} = \mathrm{u} (\bmod q)\}$$

If $\mathrm{t} \in \Lambda_q^u(\mathrm{A})$, then $\Lambda_q^u(\mathrm{A}) = \Lambda_q^{\perp}(\mathrm{A}) + \mathrm{t}$, so $\Lambda_q^u(\mathrm{A})$ is the result of the translation of $\Lambda_q^{\perp}(\mathrm{A})$.

Definition 3 Assumes Λ is a lattice whose dual lattice Λ^* is the set of all vectors whose inner products with all lattice vectors in the lattice Λ are integers, that is.

$$\Lambda^* = \{\mathrm{x} \in \mathbb{R}^n : \mathrm{v} \in \Lambda, \langle \mathrm{x}, \mathrm{v} \rangle \in \mathbb{Z}\}$$

The dual of the dual of the lattice Λ is itself.

$$(\Lambda^*)^* = \Lambda$$

The lattice and in Definition 2 are dual.

$$\Lambda_q^{\perp} = q.(\Lambda_q)^*, \quad \Lambda_q = q.(\Lambda_q^{\perp})^*$$

Definition 4： For any vector *c* [22], positive real numbers $\sigma > 0$, the discrete Gaussian distribution over the lattice $\Lambda_q^{\perp}$ is defined as:

$$D_{\Lambda_q^{\perp}(\mathrm{A}),\sigma,\mathrm{c}}(\mathrm{x}) = \frac{\rho_{\sigma,\mathrm{c}}(\mathrm{x})}{\rho_{\sigma,\mathrm{c}}(\Lambda_q^{\perp}(\mathrm{A}))}$$

Where $\rho_{\sigma,\mathrm{c}}(\mathrm{x})$ is.

$$\rho_{\sigma,\mathrm{c}}(\mathrm{x}) = \exp(\pi \| \mathrm{x} - \mathrm{c} \|^2 / \sigma^2)$$

Theorem 1 Let n, m are the integer, that $q \geq 3$ is an odd number, for any real number δ : $\delta > 0$ [13]. If $m \geq (5+3\delta)n\log q$, then there exists a probabilistic polynomial time algorithm $\mathrm{TrapGen}(q,n)$ out-put matrix pair.

$$(\mathrm{A}, \mathrm{T}_{\mathrm{A}}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}^{m\times m}$$

Where the distribution of A is statistically close to the uniform distribution on $\mathbb{Z}_q^{n\times m}$, T_{A} is a set of short bases on the lattice $q-\mathrm{ary}$ $\Lambda_q^{\perp}(\mathrm{A})$, while the following two equations hold with overwhelming probability:

$$\left\| \tilde{\mathrm{T}}_{\mathrm{A}} \right\| \leq O(\sqrt{n\log q})$$

$$\left\| \mathrm{T}_{\mathrm{A}} \right\| \leq O(n\log q)$$

The specific algorithm is described as follows:

Input: $\mathrm{A}_1 \in \mathbb{Z}_q^{n\times m_1}$ and positive integer $m_2 : m_2 = m - m_1$.

Output: $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$ and S ∶ $\mathrm{S} \in \mathbb{Z}^{m\times m}$ the group of bases on the lattice $\Lambda^{\perp}(\mathrm{A})$.

(a) Generate the matrices $\mathrm{U} \in \mathbb{Z}^{m_2\times m_2}$; $\mathrm{G}, \mathrm{R} \in \mathbb{Z}^{m_1\times m_2}$; $\mathrm{P} \in \mathbb{Z}^{m_2\times m_1}$ and $\mathrm{C} \in \mathbb{Z}^{m_1\times m_1}$, satisfying the following equations:

$$(\mathrm{GP} + \mathrm{C}) \subset \Lambda^{\perp}(\mathrm{A}_1)$$

Where U is a nonsingular matrix.

(b) Calculate A_2 ∶ $\mathrm{A}_2 = -\mathrm{A}_1.(\mathrm{R} + \mathrm{G}) \in \mathbb{Z}^{n\times m_2}$.

(c) Calculate S ∶

$$\mathrm{S} = \begin{pmatrix} (\mathrm{R}+\mathrm{G})\mathrm{U} & \mathrm{RP} \text{-} \mathrm{C} \\ \mathrm{U} & \mathrm{P} \end{pmatrix} \in \mathbb{Z}^{m\times m}.$$

(d) Calculate A ∶ $\mathrm{A} = [\mathrm{A}_1 \,|\, \mathrm{A}_2]$.

(e) Final output A and S .

Theorem 2 Assume $m > n$ is the integer, q is the prime number. The input matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$, the trapdoor T_{A} on the lattice $\Lambda^{\perp}(\mathrm{A})$, the vector $\mathrm{y} \in \mathbb{Z}_q^n$ and the real number $s > \left\| \tilde{\mathrm{T}}_{\mathrm{A}} \right\| \omega(\sqrt{\log(m)})$, and the original image sampling algorithm $\mathrm{SamplePre}(\mathrm{A}, \mathrm{T}_{\mathrm{A}}, \mathrm{y}, s)$ can output *y* in one polynomial time, an original image of $\mathrm{x} \in \mathbb{Z}^m$, for a vector *x* on the lattice $\Lambda^{\perp}(\mathrm{A})$, and the distribution of *x* obedience is statistically close to the distribution of $D_{\Lambda_q^{y}(\mathrm{A}),s}$ [11].

3. Network Model

In the smart grid key management scheme proposed in this paper, to reduce the energy consumption of smart grid nodes, the smart grid ordinary model is used for key pre-distribution management of smart grid nodes; to adapt to the deployment of smart grid nodes in a wider area, this paper uses a clustered smart grid model for node deployment. The smart grid consists of two types of smart grid nodes: base stations, a few cluster head nodes N_i^H and the most common nodes $N_{(i,j)}^C$, and the topology of the smart grid is shown in **Fig. 1**.

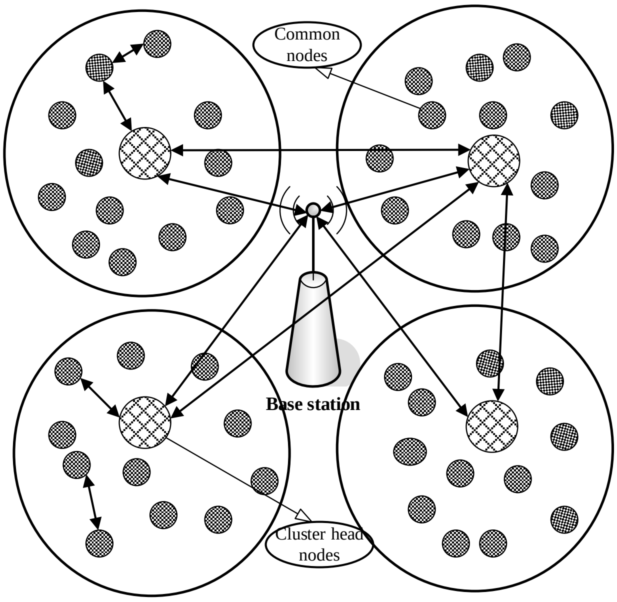

Fig. 1. Network Model

In **Fig. 1**, the base station is characterized by unlimited energy, high computing power, and sufficient storage space, and is honest and reliable. The function of the cluster head smart grid node is to collect information and send it to the base station; the ordinary smart grid node is responsible for sensing the relevant data and sending the collected data to the cluster head smart grid node of this cluster. The ordinary smart grid node has limited energy, computational power, and storage space and is the most deployed type of sensor in the whole network.

In this paper, the following assumptions are made for the base station and smart grid nodes:

(1). The key pairs of smart grid nodes are pre-generated by the base station and pre-distributed to all smart grid nodes.

(2). Each smart grid node has its own unique identity $ID_i^H, ID_{(i,j)}^C \in \mathbb{Z}_q^n$ 。

(3). The processing capacity and storage space of the cluster head node is much larger than that of the ordinary smart grid nodes, and the cluster head smart grid node is indebted to forward the information collected by all ordinary smart grid nodes in this cluster to the base station, and to generate and manage the symmetric communication keys shared by all smart grid nodes in this cluster.

(4). The communication keys between the sensors in each cluster are different.

(5). Ordinary smart grid nodes are the most restricted smart grid nodes in the network in terms of processing power and storage space.

(6). If nodes in different clusters need to communicate, they must go through the cluster head smart grid node in their own cluster for forwarding.

(7). The base station storage space in the proposed protocol in this paper is only large enough and is honest and reliable.

4. Key Management Scheme

In this paper, a lattice-based smart grid key management scheme is proposed, which uses the smart grid common model for key pre-distribution management of smart grid nodes; a clustered smart grid model is used for deployment of smart grid nodes. The base station first generates the system parameters and public-private key pairs of all smart grid nodes and assigns the key pairs to the corresponding smart grid nodes. The smart grid nodes in different clusters establish the corresponding key pairs only when they need to communicate. After establishing the shared key, the smart grid nodes in different clusters can use the shared key to communicate securely through the cluster head of this cluster, which is based on the symmetric cryptosystem. Since the symmetric cryptosystem is more efficient than the asymmetric cryptosystem in cryptographic operations, it can effectively reduce the communication energy consumption of smart grid nodes. Smart grid nodes in the same cluster can communicate with the communication key shared by all nodes in this cluster, and this shared communication key is managed and updated by the cluster head liability. The proposed scheme assumes that the base station can effectively detect the captured nodes, and when the base station detects a captured smart grid node, it immediately sends it to the cluster head node of its cluster to prevent them from continuing communication with the captured smart grid node, and adds the node to the blacklist list, and the *ID* corresponding cluster head node immediately updates the shared key used for communication of all nodes in the cluster.

To make better use of the original image sampling algorithm, this paper proposes a method to generate the corresponding matrix from a vector, denoted as $\mathrm{Gen}_{\mathrm{u}\to\mathrm{U}}(\mathrm{u},k)$, where the positive integers $k>0$ denotes the dimension of the generated matrix.

The steps of the matrix generation algorithm are as follows:

Input vector *u* and positive integers *k*; output matrix U.

(a) Suppose the vector $\mathrm{u}=\{u_1,u_2,\ldots,u_n\}$, first take out the last bit u_n; then shift the other $n-1$ bits to the right; fill u_n in the first bit to get u_1:

$$\mathrm{u}_1=\{u_n,u_1,\ldots,u_{n-1}\}.$$

(b) Repeat step (a) to obtain:

$$\mathrm{u}_2=\{u_{n-1},u_n,\ldots,u_{n-2}\}$$
$$\mathrm{u}_3=\{u_{n-2},u_{n-1},\ldots,u_{n-3}\}$$
$$\vdots \quad \vdots$$

(c) The last vector is output：

$$\mathrm{u}_{k-1}=\{u_{n-k+2},u_{n-k+3},\ldots,u_{n-k+1}\}.$$

(d) Final output matrix $\mathrm{U}\in\mathbb{Z}^{n\times k}$ ：

$$\mathrm{U} = \begin{Bmatrix} u_1 & u_n & \cdots & u_{n-k+2} \\ u_2 & u_1 & \cdots & u_{n-k+3} \\ \vdots & \vdots & \vdots & \vdots \\ u_n & u_{n-1} & \cdots & u_{n-k+1} \end{Bmatrix}.$$

4.1 System parameters and keys

The system parameters and key pairs are generated as follows:

(1) Let the system security parameter is 1^n。

(2) First, choose the prime number q ：$q = poly(n)$, positive integers d, m, k, λ, l, where m the following inequalities must be satisfied:

$$m \geq (5+3\delta)n \log q \text{ ；}$$

Select real numbers σ, s , satisfy the following two equations:

$$\sigma \geq 12 d \lambda \sqrt{m}$$

$$s > O(\sqrt{n \log q}).\omega(\sqrt{\log(m)}).$$

(3) Run the trapdoor generation algorithm $\mathrm{TrapGen}(q,n)$ in Theorem 1, and output a matrix $\mathrm{A} \in \mathbb{Z}_q^{n \times m}$ and a set of bases $\mathrm{T_A} \in \mathbb{Z}^{m \times m}$ on the lattice $\Lambda_q^{\perp}(\mathrm{A})$, Satisfaction:

$$\left\| \tilde{\mathrm{T}}_{\mathrm{A}} \right\| \leq O(\sqrt{n \log q}).$$

(4) Select four secure hash functions：

$$H_1 : \{0,1\}^* \to \left\{ \mathrm{v} : \mathrm{v} \in \{-1,0,1\}^k, \|\mathrm{v}\|_1 \leq k \right\}$$

$$H_2 : \mathbb{Z}_q^n \to \{0,1\}^l$$

$$F_1 : \{0,1\}^l \to \{0,1\}^{l_1}$$

$$F_2 : \{0,1\}^{l_1} \to \{0,1\}^l.$$

(5) To generate the key pairs of cluster head smart grid nodes: first, run the vector generation matrix algorithm $\mathrm{Gen}_{\mathrm{u}\to\mathrm{U}}(ID_i^H, k)$ can be proposed in this paper to output an identity-based $ID_i^H \in \mathbb{Z}_q^n$ matrix $\mathrm{U}_i^H \in \mathbb{Z}_q^{n \times k}$ for each cluster-head smart grid node N_i^H; run the original image sampling algorithm $\mathrm{SamplePre}(\mathrm{A}, \mathrm{T_A}, \mathrm{u}_i^H, s)$ to output the number k identity-based vectors $\mathrm{s}_i^H \in \mathbb{Z}^m$ for each vector in the matrix U_i^H , and form a matrix $\mathrm{S}_i^H \in \mathbb{Z}^{m \times k}$ from this number k vectors, where each column vector in the k columns of the matrix S_i^H is the original image each column vector in the column of the matrix is the number k vectors corresponding to the output of the original image sampling algorithm. Finally, the base station generates a public-private key pair $(\mathrm{U}_i^H, \mathrm{S}_i^H)$ for the cluster head smart grid node with identity information ID_i^H that satisfies $\mathrm{U}_i^H = \mathrm{A}\mathrm{S}_i^H$.

(6) Generate key pairs for common smart grid nodes: As (5), run the matrix algorithm $\mathrm{Gen}_{\mathrm{u}\to\mathrm{U}}(ID_{i,j}^{C},k)$ and original image sampling algorithm $\mathrm{SamplePre}(\mathrm{A},\mathrm{T}_{\mathrm{A}},\mathrm{u}_{i,j}^{C},s)$ to output public-private key pairs $(\mathrm{U}_{i,j}^{C},\mathrm{S}_{i,j}^{C})$ based on identity information $ID_{i,j}^{C}\in\mathbb{Z}_{q}^{n}$ for each common smart grid node $N_{i,j}^{C}$ respectively.

Finally, the base station outputs the system common parameters:

$$PP=\{\mathrm{A},F_1,F_2,H_1,H_2\}$$

Key pairs of cluster heads and common smart grid nodes:

$$(\mathrm{U}_{i}^{H},\mathrm{S}_{i}^{H}),(\mathrm{U}_{i,j}^{C},\mathrm{S}_{i,j}^{C}).$$

4.2 Generate intra-cluster key

All smart grid nodes in the same cluster share the same communication key, which is produced, managed, updated, etc. By the cluster head smart grid node. The communication key is based on a symmetric cryptographic system, so that the communication efficiency will be higher. The specific process of intra-cluster key generation is as follows: first, the cluster head smart grid node randomly generates the communication key shared within the cluster and then forwards the generated key message to all smart grid nodes within the cluster. This scheme assumes that the public key of the smart grid nodes in the cluster is known only to the smart grid nodes in this cluster and the base station, and is not known to the smart grid nodes in other clusters. When the normal smart grid nodes in this cluster receive the message with the key, they first verify it, and if it passes the verification, they receive the corresponding intra-cluster key message, otherwise they reject it. The detailed process of generating the intra-cluster key is as follows.

Take the number *i* cluster as an example, the number *i* cluster head smart grid node N_i^H first randomly generates a symmetric communication key K_i for intra-cluster communication: $K_i\in\{0,1\}^l$, which is a key in the symmetric cryptosystem, using the symmetric cryptosystem for encryption and decryption is more efficient, the specific validity time of the key depends on the specific situation, if the network environment security is relatively good, and no smart grid node is captured the key The validity time of the key K_i can be extended appropriately if the security condition of the network environment is good and no smart grid node is captured. The specific process is as follows:

(1) Select a random y_i : $y_i\leftarrow D_{\sigma}^{m}$ and a timestamp t_i : $t_i\in\{0,1\}^*$, where t_i indicate that the message was generated by the number *i* cluster head smart grid node N_i^H at time *t*.

(2) Calculate u_y and u_K :

$$u_y=H_2(\mathrm{A}y_i)$$

$$u_K=K_i\oplus u_y$$

(3) Calculate $u_K^{'}$:

$$u_K^{'} = F_1(u_K) \| (F_2(F_1(u_K)) \oplus u_K)$$

(4) Calculate the validation message (z,c) ：

$$c = H_1(\mathrm{A}y_i, t_i)$$
$$z = \mathrm{S}_i c + y_i$$

(5) With probability $\min(1, \frac{D_\sigma^m(z)}{MD_{\sigma,\mathrm{S}_i c}^m(z)})$ Output (z,c), the number *i* cluster head smart grid node N_i^H sends the message $(z,c,u_K^{'},t_i)$ containing the symmetric communication key to all normal smart grid nodes and base stations in the cluster.

The timestamp t_i is used to determine the timeliness of the message; (z,c) is used for authentication; and $u_K^{'}$ is used to extract the symmetric communication key after authentication.

4.3 Verify and recover the intra-cluster key

When all common smart grid nodes and the base station in the cluster receive the message $(z,c,u_K^{'},t_i)$ from the number *i* cluster head smart grid node, first verify the validity of the message with the public key U_i^H of the number *i* cluster head smart grid node, and if the verification passes, extract and receive the symmetric communication key sent by the number *i* cluster head smart grid node, all smart grid nodes in the number *i* cluster can use the symmetric key for All smart grid nodes in the number *i* cluster can use this symmetric key for secure communication, and the base station can also use this symmetric key to communicate with the first cluster head smart grid node, and if the verification fails, the packet is discarded. The specific process is as follows.

(1) Verify that both following equations hold：

$$c = H_1(\mathrm{A}z - \mathrm{U}_i^H c, t_i)$$
$$\|z\| \le 2\sigma\sqrt{m}$$

If both of the above equations hold, it means that the verification passes and will continue to the next operation; otherwise, the verification fails and the packet is discarded.

(2) Calculate：

$$u_y = H_2(\mathrm{A}z - \mathrm{U}_i^H c)$$

(3) Recovered message u_K ：

$$u_K = [u_K^{'}]_l \oplus F_2([u_K^{'}]^{l_1})$$

(4) Verify that the equation $[u_K^{'}]^{l_1} = F_1(u_K)$ holds, and if it does, recover the symmetric communication key $K_i = u_K \oplus u_y$; if it fails, discard the packet and terminate the operation.

Where $[u_K^{'}]^{l_1}$ denotes the first few l_1 bit of $u_K^{'}$ from high to low; $[u_K^{'}]_l$ denotes: the last few bits of $u_K^{'}$ from low to high.

Finally, all normal smart grid nodes and base stations in the cluster receive the symmetric communication key information from the number *i* cluster head smart grid node and recover the symmetric communication key K_i from the packet if it passes the verification.

If the base station finds that a smart grid node is captured, it should broadcast the *ID* information of the node in time to avoid its malicious attack. If the network security condition is good, the valid time of the symmetric communication key can be extended appropriately to reduce the consumption due to the frequent update of the key.

4.4 Cross-Cluster Communication Key

If the smart grid nodes in different clusters need to communicate with each other, they must go through the cluster head smart grid node of the corresponding cluster for forwarding, because the common smart grid nodes in different clusters do not have a common symmetric communication key and the public key information of the other smart grid nodes, so the common smart grid nodes in different clusters cannot communicate with each other directly. The corresponding symmetric communication key message is generated by one of the cluster head smart grid nodes in the communication, and then the generated symmetric communication key message is sent to the cluster head smart grid node of another cluster. When the cluster head smart grid node of another cluster receives the symmetric communication key message, it first asks for the public key information of the cluster head smart grid node to which the information is sent by the base station and verifies it, and if it passes the verification, it receives the corresponding symmetric communication key message, otherwise it rejects it.

Take the example of the smart grid nodes the number *i* cluster and the number *j* cluster need to communicate, the number *i* cluster head smart grid node N_i^H first generates a random symmetric communication key $K_{i\leftrightarrow j}$: $K_{i\leftrightarrow j} \in \{0,1\}^l$ for communication with the number *j* cluster head smart grid node, which is a key in the symmetric cryptographic regime. Then an authentication message $(z, c, u_K^{'}, t_{i\leftrightarrow j})$ with the symmetric communication key embedded is generated and forwarded to the number *j* cluster head smart grid node N_j^H .

When the number *i* cluster head smart grid node N_j^H receives the authentication message $(z, c, u_K^{'}, t_{i\leftrightarrow j})$, it first asks the base station for the public key U_i^H of the number *i* cluster head smart grid node and uses the public key U_i^H to verify the validity of the message $(z, c, u_K^{'}, t_{i\leftrightarrow j})$, and finally recovers the symmetric communication key $K_{i\leftrightarrow j}$ from the message $(z, c, u_K^{'}, t_{i\leftrightarrow j})$. The cross-cluster symmetric communication key exchange process is similar to the intra-cluster symmetric communication key exchange process.

4.5 Communication using a symmetric key

After the above symmetric communication key exchange process, the symmetric communication keys between the intra-cluster smart grid nodes, between the base station and the cluster head smart grid nodes, and between the cluster head and the cluster head in the smart grid are shown in **Table 1**.

Table 1. Symmetric communication key sharing situation

The body of the shared key	Shared symmetric communication key $K_?$
Between the base station and the cluster head	K_i ：the shared key of number *i* cluster head and the base station
Between cluster head and cluster head	$K_{i\leftrightarrow j}$ ：the shared key of number *i* and number *j* cluster head
Between cluster nodes	K_i ：the shared key of all nodes in the number *i* cluster

The following describes the specific process of communication with symmetric keys in three cases: the communication between smart grid nodes within a cluster, communication between smart grid nodes across a cluster, and communication between a cluster head and a base station, respectively.

(1) Communication between smart grid nodes within a cluster

Assume that the smart grid nodes $N_{(i,1)}^{C}$ and $N_{(i,2)}^{C}$ in the number *i* cluster need to communicate with each other, and since the smart grid nodes in the number *i* cluster share the same key K_i , the two smart grid nodes that need to communicate can communicate directly with the symmetric key K_i, and the roadmap for the communication of the smart grid nodes in the cluster is shown in **Fig. 2**.

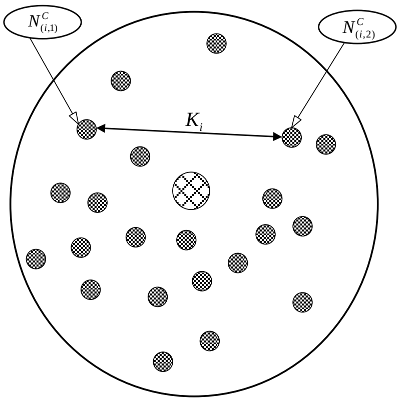

Fig. 2. Intra-cluster node communication line diagram

The specific process is as follows:

The smart grid node of number *i* cluster of $N_{(i,1)}^{C}$ ：

Encrypted message u ：

$$u_{En} = En(K_i, u)$$

Where u denotes the message to be encrypted; K_i denotes: the symmetric communication key shared by the smart grid nodes in the number *i* cluster; $En(K_i, u)$ denotes: the plaintext message u to be encrypted is encrypted with the symmetric communication key K_i, and the algorithm used is the more efficient symmetric cryptosystem algorithm, which is set as $EnSY$; u_{En} denotes: the encrypted ciphertext message; $N_{(i,1)}^{C}$ denotes: the first smart grid node in the number *i* cluster. Then, the smart grid node $N_{(i,1)}^{C}$ sends the encrypted ciphertext u_{En} to the smart grid node $N_{(i,2)}^{C}$.

When the smart grid nodes $N_{(i,2)}^{C}$ receives the cipher text u_{En} can be sent from the smart grid node $N_{(i,1)}^{C}$, then the text u_{En} will be decrypted with the previously generated symmetric communication key pair K_i .

The smart grid nodes of number *i* cluster $N_{(i,2)}^{C}$ ：

Decrypted message ：

$$u_{De} = De(K_i, u_{En}) = u \, .$$

Where $De(K_i, u_{En})$ denotes: decryption of the ciphertext u_{En} with a symmetric communication key K_i using a symmetric cryptosystem algorithm $EnSY$; u_{De} denotes the decrypted ciphertext message. Finally, the smart grid node $N_{(i,2)}^{C}$ obtains the message u ： $u = u_{De}$ sent by the smart grid node $N_{(i,1)}^{C}$.

(2) Communication between cross-cluster smart grid nodes

Assume that the ordinary smart grid node $N_{(i,1)}^{C}$ of the number *i* cluster and the ordinary smart grid node $N_{(j,1)}^{C}$ of the number *j* cluster need to communicate with each other, because the ordinary smart grid node of the number *i* cluster and the ordinary smart grid node of the number *j* cluster do not have a shared key, so the two smart grid nodes of different clusters cannot communicate directly, they must forward through the cluster head node in their own cluster, the smart grid node and the smart grid of the roadmap for communication between smart grid nodes $N_{(i,1)}^{C}$ and smart grid nodes $N_{(j,1)}^{C}$ is shown in **Fig. 3**.

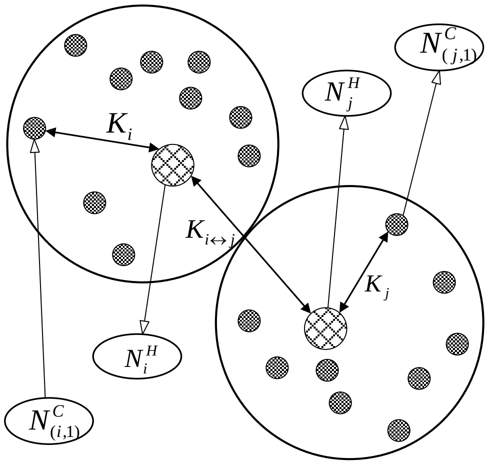

Fig. 3. Cross-cluster node communication line diagram

The specific process is as follows:

(a) The smart grid node of the number *i* cluster $N^C_{(i,1)}$:

Encrypted message u :

$$u^i_{En} = En(K_i, u).$$

Where u^i_{En} denotes: the smart grid node $N^C_{(i,1)}$ of number *i* cluster encrypts the plaintext message using the symmetric communication key K_i shared by the smart grid nodes of the number *i* cluster and encrypts the ciphertext message using the encryption algorithm $EnSY$. Then, the smart grid node $N^C_{(i,1)}$ ciphertext u^i_{En} is sent to the head smart grid node N^H_i of number *i*.

When the head smart grid node of the number *i* cluster receives the cipher text u^i_{En} , which can be sent from the smart grid node $N^C_{(i,1)}$, first decrypts u^i_{En} with the symmetric communication key K_i shared within the cluster.

(b) Number *i* cluster head smart grid node N^H_i :

Decrypted message :

$$u^i_{Dn} = De(K_i, u^i_{En}) = u$$

Where $De(K_i, u^i_{En})$ denotes: decrypting the ciphertext u^i_{En} with a symmetric communication key K_i using an algorithm $EnSY$. Finally, the cluster head smart grid node N^H_i acquires the message *u*, which is sent by the smart grid node $N^C_{(i,1)}$.

After decryption, the number *i* cluster head smart grid node re-encrypts the message *u* with the symmetric key shared with the number *j* cluster head smart grid node and forwards it to the first cluster head smart grid node.

Encrypted message u :

$$u_{En}^{i\to j} = En(K_{i\leftrightarrow j}, u)$$

The number *i* cluster head smart grid nodes N_i^H sends the cipher text $u_{En}^{i\to j}$, which can be encrypted with the symmetric communication key $K_{i\leftrightarrow j}$ to the number *j* cluster head smart grid node N_j^H.

(c) The number *j* cluster head smart grid node N_j^H ：

Decrypted message：

$$u_{De}^{i\to j} = De(K_{i\leftrightarrow j}, u_{En}^{i\to j}) = u$$

The number *j* cluster head smart grid node will decrypt the message with the symmetric communication key shared with the number *i* cluster head smart grid node and re-encrypt it with the shared key within this cluster.

Encrypted message u ：

$$u_{En}^{j} = En(K_j, u)$$

Finally, the number *j* cluster head smart grid node sends the ciphertext u_{En}^{j} encrypted with the intra-cluster symmetric communication key K_j to this cluster smart grid node $N_{(j,1)}^C$

(d) The number *j* cluster smart grid node $N_{(j,1)}^C$ ：

Decrypted message：

$$u_{Dn}^{j} = De(K_j, u_{En}^{j}) = u$$

Finally, the smart grid node $N_{(j,1)}^C$ of the number *j* cluster gets the message u ： $u = u_{Dn}^{j}$ sent by the smart grid node of the number *i* cluster.

(3) Communication between base stations and cluster head smart grid nodes

Assume that communication is required between the number *i* cluster-head smart grid node N_i^H and the base station, and since there is a shared symmetric communication key K_i between the number *i* cluster-head smart grid node and the base station, the communication can be performed directly as follows:

The number *i* cluster head smart grid node N_i^H ：

Encrypted messages u ：

$$u_{En}^{i\to} = En(K_i, u)$$

Decrypted message：

$$u_{Dn}^{i\to} = De(K_i, u_{En}^{i\to}) = u$$

Since the communication between the cluster head smart grid node and the base station is more important, another more secure communication method between the base station and the cluster head smart grid node is described below:

The number *i* cluster head smart grid node N_i^H ：

(a) Decrypted message u ：

$$u_{En}^{a} = En(K_i, u)$$

(b) Compute the message (z_a, c_a) after ciphertext embedding：

$$c_a = H_1(\mathrm{A}y, u_{En}^a)$$

$$z_a = \mathrm{S}_a c + y$$

(c) Output with probability $\min(1, \frac{D_\sigma^m(z_a)}{MD_{\sigma,\mathrm{S}_a c_a}^m(z_a)})$ message (z_a, c_a) with embedded ciphertext.

Then, the number *i* cluster head smart grid node sends the message (z_a, c_a, u_{En}^a) with the embedded ciphertext to the base station.

When the base station receives the message (z_a, c_a, u_{En}^a) embedded in the ciphertext from the number *i* cluster head smart grid node, it verifies the message (z_a, c_a) with the public key U_i^H of the number *i* cluster head smart grid node and decrypts u_{En}^a with the previously generated symmetric communication key K_i.

Base station：

(a) Verify that both following equations hold：

$$c_a = H_1(\mathrm{A}z_a - \mathrm{U}_i^H c_a, u_{En}^a)$$

$$\|z_a\| \le 2\sigma\sqrt{m}$$

If both of the above equations hold, the verification passes and will continue to the next step; otherwise, the verification fails and this packet is discarded.

(b) Decrypted message u_{En}^a ：

$$u_{De}^a = De(K_i, u_{En}^a) = u \, .$$

Finally, the base station acquires the message *u* sent by the number *i* cluster head smart grid node.

The two smart grid communication methods described above have their own advantages and disadvantages, and different smart grid communication methods can be selected according to the importance of the data. If the data to be encrypted is not essential and the security level is not particularly high, you can use the smart grid communication method of using a symmetric secret key to communicate directly, which is more efficient as long as the encryption and decryption operations are carried out by the symmetric cryptographic system algorithm. If the data to be encrypted is more important and the security requirement is higher, you can use the smart grid communication method of embedding the cipher text into the message, which is more secure. Communication method, this communication method is more secure.

5. Protocol Analysis

In this paper, we analyze the new scheme in 3 aspects: consistency, security and efficiency.

5.1 Consistency Analysis

According to the specific process of the above key management scheme, the sampling algorithm consistency, verification process consistency and key recovery consistency is described and analyzed separately in this paper. (1) Sampling algorithm consistency analysis：

According to the original image sampling principle in Theorem 2, there exists a polynomial-time algorithm $\mathrm{SamplePre}(\mathrm{A},\mathrm{T}_{\mathrm{A}},\mathrm{u}_i^H,s)$ for all $\mathrm{u}_i^H\in\mathbb{Z}_q^n$ draw vector S_i^H, such that the following equation holds.

$$\mathrm{u}_i^H=\mathrm{As}_i^H, i=0,1,\ldots,k-1$$

From the principle of the matrix construction algorithm $\mathrm{Gen}_{\mathrm{u}\to\mathrm{U}}(\mathrm{u},k)$ proposed in this paper, we get

$$\mathrm{U}_i^H=\begin{Bmatrix}\mathrm{u}_o^H\\ \mathrm{u}_1^H\\ \vdots\\ \mathrm{u}_{k-1}^H\end{Bmatrix}^T=\begin{Bmatrix}u_1 & u_2 & \cdots & u_n\\ u_n & u_1 & \cdots & u_{n-1}\\ \vdots & \vdots & \vdots & \vdots\\ u_{n-k+2} & u_{n-k+3} & \cdots & u_{n-k+1}\end{Bmatrix}^T$$

$$\mathrm{S}_i^H=\begin{Bmatrix}\mathrm{s}_o^H\\ \mathrm{s}_1^H\\ \vdots\\ \mathrm{s}_{k-1}^H\end{Bmatrix}^T=\begin{Bmatrix}s_{01} & s_{02} & \cdots & s_{0m}\\ s_{11} & s_{12} & \cdots & s_{1m}\\ \vdots & \vdots & \vdots & \vdots\\ s_{(k-1)1} & s_{(k-1)2} & \cdots & s_{(k-1)m}\end{Bmatrix}^T$$

For $\mathrm{u}_i^H=\mathrm{As}_i^H$ to get：

$$\mathrm{U}_i^H=\mathrm{AS}_i^H$$

From the above analysis, we can see that it is correct to use the public-private key pair $(\mathrm{U}_i^H,\mathrm{S}_i^H)$ generated based on the identity information ID_i^H of the smart grid nodes in this paper.

(2) Validation process consistency analysis：

$$\mathrm{Az}-\mathrm{U}_i^Hc=\mathrm{A}(\mathrm{S}_i^Hc+y)-\mathrm{U}_i^Hc=\mathrm{AS}_i^Hc+\mathrm{A}y-\mathrm{U}_i^Hc=\mathrm{AS}_i^Hc+\mathrm{A}y-(\mathrm{AS}_i^H)c=\mathrm{A}y$$

Thus：

$$H_1(\mathrm{Az}-U_i^Hc,t_i)=H_1(\mathrm{A}y,t_i)=c$$

The following two lemmas are introduced before proving that the inequalities holds $\|z\|\le 2\sigma\sqrt{m}$ with overwhelming probability.

Lemma 1 For any real number $\sigma>0$ and positive integer *m*, the following inequality holds [14]

$$\Pr[y\leftarrow D_\sigma^m:\|y\|>2\sigma\sqrt{m}]<2^{-m}$$

Lemma 2 For an arbitrary vector $v\in\mathbb{Z}^m$, if：

$$\sigma=\omega(\|v\|\sqrt{\log m})$$

Then the following equation holds [14]：

$$\Pr[y\leftarrow D_\sigma^m:D_\sigma^m(y)/D_{\sigma,v}^m(x)=O(1)]=1-2^{\omega(\log m)}$$

According to Lemma 2, the distribution characteristics of *z* are very close D_σ^m; from Lemma 2, we can conclude that the inequality $\|z\|\le 2\sigma\sqrt{m}$ will be satisfied with a probability greater z than or equal to $1-2^{-m}$, the inequality will be satisfied with an overwhelming probability.

(2) Recover Keys Consistency Analysis：

(a) Analytical equation $[u_K^{'}]^{l_1} = F_1(u_K)$ ：

$$[u_K^{'}]^{l_1} = [F_1(u_K) \| (F_2(F_1(u_K)) \oplus u_K)]^{l_1} = F_1(u_K)$$

(b) Analyze the correctness of the key K_i:

$$K_i = u_K \oplus u_y = [u_K^{'}]_l \oplus F_2([u_K^{'}]^{l_1}) \oplus u_y = [F_1(u_K) \| (F_2(F_1(u_K)) \oplus u_K)]_l \oplus$$
$$F_2([F_1(u_K) \| (F_2(F_1(u_K)) \oplus u_K)]^{l_1}) \oplus u_y \quad = [F_1(u_K) \| (F_2(F_1(u_K)) \oplus u_K)]_l \oplus$$
$$F_2(F_1(u_K)) \oplus u_y$$
$$= (F_2(F_1(u_K)) \oplus u_K) \oplus F_2(F_1(u_K)) \oplus u_y = u_K \oplus u_y = K_i \oplus u_y \oplus u_y = K_i$$

From the above analysis, it can be concluded that the smart grid nodes in the number i cluster establish a common symmetric communication key K_i, and can use K_i to communicate.

5.2 Security Analysis

This section analyzes that the above smart grid key management scheme is secure under the assumption of a small integer solution problem with parameters $(q, m, (4\sigma + 2d\lambda)\sqrt{m})$ of the following two aspects: key exchange process and smart grid node communication.

(1) Key Management Solution Security Analysis：

Assume that there exists a polynomial-time algorithm ξ to obtain a new forged authentication signature for a message (z^w, c^w) with non-negligible probability, such that:

$$\mathrm{A}z - \mathrm{U}_i^H c = \mathrm{A}z^w - \mathrm{U}_i^H c^w$$

As $\mathrm{U}_i^H = \mathrm{AS}_i^H$, then：

$$\mathrm{A}z - \mathrm{U}_i^H c - \mathrm{A}z^w - \mathrm{U}_i^H c^w = \mathrm{A}z - \mathrm{AS}_i^H c - \mathrm{A}z^w - \mathrm{AS}_i^H c^w$$
$$= \mathrm{A}(z - \mathrm{S}_i^H c - z^w - \mathrm{S}_i^H c^w) = 0$$

Based on the consistency of the authenticated message, we get：

$\|z\|, \|z^w\| \le 2\sigma\sqrt{m}$ and $\|\mathrm{S}_i^H c\|, \|\mathrm{S}_i^H c^w\| \le d\lambda\sqrt{m}$ holds with overwhelming probability, then：

$$z - \mathrm{S}_i^H c - z^w - \mathrm{S}_i^H c^w \le 4\sigma\sqrt{m} + 2d\lambda\sqrt{m}$$

Lemma 3 for any matrix $\mathrm{A} \in \mathbb{Z}_q^{n\times m}$ satisfying the condition $m \ge 64 + n\log q / \log(2d+1)$, randomly chosen s : $\mathrm{s} \overset{\$}{\leftarrow} \{-d, \ldots, 0, \ldots, d\}^m$, then with probability $1-2^{-m}$ there exists another $\mathrm{s}^{'} : \mathrm{s}^{'} \in \{-d, \ldots, 0, \ldots, d\}^m$, satisfying $\mathrm{As} = \mathrm{As}^{'}$ [14]

According to Lemma 3, it can be concluded that a new smart grid node private key S_i^{Hw}

can be generated with greater probability than $1-2^{-m}$, satisfying the equation $\mathrm{AS}_i^H = \mathrm{AS}_i^{Hw}$, then:

$$z-\mathrm{S}_i^H c - z^w +_i^H c^w - z + \mathrm{S}_i^{Hw} c + z^w - \mathrm{S}_i^{Hw} c^w = (\mathrm{S}_i^{Hw} - \mathrm{S}_i^H)(c-c^w) \neq 0$$

then：

$$z-\mathrm{S}_i^H c - z^w + \mathrm{S}_i^H c^w \neq 0$$

Thus, the smart grid key management scheme proposed in this paper is secure under the assumption of a small integer solution problem with parameters $(q, m, (4\sigma + 2d\lambda)\sqrt{m})$.

(3) Smart grid node communication security analysis：

Take the example of the communication between the number *i* cluster head smart grid node and the base station.

If no other malicious, smart grid node eavesdrops during the key exchange and transmission between the number *i* cluster head smart grid node and the base station, then the direct communication with symmetric smart grid communication keys K_i is secure.

If a malicious smart grid node N_e eavesdrops on the packet during the key exchange and transmission between the number *i* cluster head smart grid node and the base station, but the malicious smart grid node N_e does not know the public key U_i^H of the number *i* cluster head smart grid node, the malicious smart grid node N_e cannot recover the corresponding communication key from the eavesdropped symmetric communication key exchange information, so the number *i* cluster head smart grid node and the base station communicate directly with the symmetric communication key in a secure manner. The direct communication between the first cluster smart grid node and the base station with the symmetric communication key K_i is secure.

If the malicious smart grid node N_e has previously obtained the public key U_i^H of the number *i* cluster head smart grid node, the malicious smart grid node N_e can verify and recover the symmetric communication key shared between the number *i* cluster head smart grid node and the base station by using the public key K_i of the number *i* cluster head smart grid node, and this case can be communicated by embedding the ciphertext into the authentication message in a more secure way. The security of the embedded ciphertext communication method is analyzed below.

A malicious, smart grid node N_e can impersonate the number i cluster head smart grid node to encrypt the forged message u^e and generate a forged ciphertext u_{En}^e :

$$u_{En}^e = En(K_i, u^e)$$

Then, a random one $y_e \leftarrow D_\sigma^m$ is generated; the forged authentication message c_a is calculated:

$$c_a = H_1(\mathrm{A}y_a, u_{En}^a)$$

However, since the malicious, smart grid nodes N_e do not know the private key S_i^H of the number i cluster head smart grid node, there is no way to embed the impersonated ciphertext u_{En}^e into the forged authentication message z_e.

$$z_e \neq \mathrm{S}_i^H c_e + y_e$$

From the above analysis, it can be seen that the communication between the first cluster head smart grid node and the base station proposed in this paper is secure. The communication between the intra-cluster smart grid nodes and the cross-cluster smart grid nodes is a similar to the analysis of the communication method between the cluster head smart grid node and the base station.

5.3 Efficiency Analysis

In this section, we mainly focus on the computational costs, storage overhead. First, we make a comparison of storage overhead between our smart grid key management scheme and other related secret key schemes, Li et al. Scheme [23], Wang et al. Scheme [24] and Brakerski et al. Scheme [25]. The specific results of storage comparison of the schemes are shown in **Table 2**.

Table 2. Storage overheads of all schemes

Scheme	Private key size	Public key size
Li et al. Scheme [23]	$nk \log q$	$4nk \log q$
Wang et al. Scheme [24]	$3m^2 \log q$	$(2l+9)m^2 \log q$
Brakerski et al. Scheme [25]	$2ml \log q$	$m^2 \log q$
Our scheme	$mk \log q$	$2n(n-k)\log q$

As depicted in **Table 2**, we make a comparison of storage overhead between our smart grid key management scheme and Li et al. Scheme [23], Wang et al. Scheme [24] and Brakerski et al. Scheme [25]. The public key size is $4nk \log q$ in Li et al. Scheme [23], is $(2l+9)m^2 \log q$ in Wang et al. Scheme [24], is $m^2 \log q$ in Brakerski et al. Scheme [25], and is $2n(n-k)\log q$ in our smart grid key management scheme. The private key size is $nk \log q$ in Li et al. Scheme [23], is $3m^2 \log q$ in Wang et al. Scheme [24], is $2ml \log q$ in Brakerski et al. Scheme [25], and is $mk \log q$ in our smart grid key management scheme. By comparing the results, our proposed the smart grid key management scheme has certain advantages in storage overhead.

Table 3. Comparison with RSA and ECC algorithms

Security level	RSA algorithm	ECC algorithm	Our algorithm
128B	8.072KB	0.256KB	68.968KB
256B	16.144KB	0.512KB	70.623KB
512B	32.288KB	1.024KB	71.567KB

By comparing the results of our smart grid key management scheme and other related secret key schemes base on RSA and ECC algorithm, the costs of our smart grid key management scheme is $m\log(12\sigma)$, which is only related to the message *m* and the parameter σ. The authentication costs corresponding to different security levels (such as 128bits, 256 bits and 512 bits) can be calculated when the selected system parameter is $n = 256, q = 2^{32}$. The results are shown in **Table 3**. The authentication costs of RSA and ECC authentication algorithms corresponding to different security levels are given. As shown in **Table 3**, the authentication costs of the RSA algorithm increase rapidly with the improvement of the security level, but no matter how the security level increases, the size of the authentication remains at a stable level in our smart grid key management scheme. In addition, RSA and ECC algorithms can't resist quantum attacks, so our smart grid key management scheme has good anti-quantum security. With the development of quantum computer and quantum computing, lattice cipher will be a very practical cryptographic algorithm in the quantum era.

The smart grid key management scheme proposed in this paper consumes less energy compared with the standard key management scheme. The smart grid key management scheme proposed in this paper does not require the smart grid nodes to send the key exchange information separately because the symmetric key information has been embedded in the key exchange information, and the smart grid nodes receiving the key exchange information can verify the embedded key information and extract the corresponding symmetric communication key. Since the proposed smart grid key management scheme does not require multiple messages, it can reduce the communication overhead of the smart grid. In addition, the key used for communication between smart grid nodes is based on the symmetric cryptosystem algorithm, so it can effectively improve the efficiency of smart grid communication. In terms of computational complexity, the main operations of the proposed key management scheme are simple hash operations and logical operations, which generally consume more energy to transmit 1 bit of data than to compute 32 bits of data. In summary, the smart grid key management scheme proposed in this paper has certain advantages in storage overhead, costs and high security.

6. Conclusion

In this paper, we propose an identity-based smart grid key management scheme on the grid, whose core idea is to use the solid security foundation and high computational efficiency on the grid, and the keys for communication are based on symmetric cryptosystem algorithm, so it can effectively reduce the communication overhead between smart grid nodes. The private keys of smart grid nodes are generated by identity-based information, so malicious, smart grid nodes are unable to calculate the public-private key pairs of other smart grid nodes. The analysis results show that the smart grid key management scheme proposed in this paper has good security.

Acknowledgement

This work was supported by the Jiangxi Province key S&T cooperation project (no. 20212BDH80021). The authors are grateful to the anonymous reviewers whose comments helped to improve this paper.

References

[1] H. Yang, F. Li, D. Yu, Y. Zou, and J. Yu, "Reliable data storage in heterogeneous wireless sensor networks by jointly optimizing routing and storage node deployment," *Tinshhua Sci. Technol.*, vol. 26, no. 2, pp. 230–238, Apr. 2021. Article (CrossRef Link).

[2] J. Kang et al., "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019. Article (CrossRef Link).

[3] K. Kinoshita, N. Inoue, Y. Tanigawa, H. Tode, and T. Watanabe, "Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks," *IEEE Sensors J.*, vol. 16, no. 10, pp. 3981–3988, May 2016. Article (CrossRef Link).

[4] M. Zhang and W. Cai, "Energy-Efficient Depth Based Probabilistic Routing Within 2-Hop Neighborhood for Underwater Sensor Networks," *IEEE Sens. Lett.*, vol. 4, no. 6, pp. 1–4, Jun. 2020. Article (CrossRef Link).

[5] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019. Article (CrossRef Link).

[6] J. Liu, Z. Zhao, J. Ji, and M. Hu, "Research and application of wireless sensor network technology in power transmission and distribution system," *Intell. and Converged Netw.*, vol. 1, no. 2, pp. 199–220, Sep. 2020. Article (CrossRef Link).

[7] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid," *IEEE Trans. Ind. Inf.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019. Article (CrossRef Link).

[8] K. G. Omeke et al., "DEKCS: A Dynamic Clustering Protocol to Prolong Underwater Sensor Networks," *IEEE Sensors J.*, vol. 21, no. 7, pp. 9457–9464, Apr. 2021. Article (CrossRef Link).

[9] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2019. Article (CrossRef Link).

[10] C. Michaelides and F.-N. Pavlidou, "Mutual Aid Among Sensors: An Emergency Function for Sensor Networks," *IEEE Sens. Lett.*, vol. 4, no. 9, pp. 1–4, Sep. 2020. Article (CrossRef Link).

[11] P. W. Shor, "Polynomial-time Algorithm for Prime Factorizeation and Discrete Logarithm on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1997. Article(CrossRefLink).

[12] J. W. Jiang, D. Wang, G. Y. Zhang, Z. Y. Chen, "Private key management scheme for mobile edge computing," *Chinese Journal of Computers*, vol. 45, no. 6, pp. 1348-1372, 2022. Article(CrossRefLink).

[13] L. Zhu, Y. Wu, K. Gai, K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527-535, 2019. Article (CrossRef Link).

[14] J. Alwen and C. Peikert, "Generating Shorter Bases for Hard Random Lattices," *Theory Comput Syst*, vol. 48, no. 3, pp. 535–553, Apr. 2011. Article (CrossRef Link).

[15] P. Kumar et al., "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021. Article (CrossRef Link).

[16] Y. Jiang, G. Tong, H. Yin, and N. Xiong, “A Pedestrian Detection Method Based on Genetic Algorithm for Optimize XGBoost Training Parameters,” *IEEE Access*, vol. 7, pp. 118310–118321, 2019. Article (CrossRef Link).

[17] Z. Li, D. Wang, and E. Morais, “Quantum-Safe Round-Optimal Password Authentication for Mobile Devices,” *IEEE Trans. Dependable and Secure Comput.*, vol. 19, no. 3, pp. 1885–1899, May 2022. Article (CrossRef Link).

[18] J. J. Gooding and S. M. Liu, “A New Year Period Emphasizing the Need for Better Sensors,” *ACS Sens.*, vol. 5, no. 3, pp. 597–598, Mar. 2020. Article (CrossRef Link).

[19] S. Doss et al., “Memetic Optimization with Cryptographic Encryption for Secure Medical Data Transmission in IoT-based Distributed Systems,” *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1577–1594, 2021. Article (CrossRef Link).

[20] C. Michaelides and F.-N. Pavlidou, “Programmable MAC in Body Area Networks, One Command at a Time,” *IEEE Sens. Lett.*, vol. 3, no. 7, pp. 1–4, Jul. 2019. Article (CrossRef Link).

[21] R. Behnia, M. O. Ozmen, and A. A. Yavuz, “Lattice-Based Public Key Searchable Encryption from Experimental Perspectives,” *IEEE Trans. Dependable and Secure Comput.*, vol. 17, no. 6, pp. 1269–1282, Nov. 2020. Article (CrossRef Link).

[22] D. Micciancio and C. Peikert, “Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller,” in *Proc. of Advances in Cryptology – EUROCRYPT 2012*, pp. 700–718, 2012. Article (CrossRef Link).

[23] D. Li, H. Chen, C. Zhong, T. Li, and F. Wang, “A New Self-Certified Signature Scheme Based on NTRUSing for Smart Mobile Communications,” *Wireless Pers Commun*, vol. 96, no. 3, pp. 4263–4278, Oct. 2017. Article (CrossRef Link).

[24] G. Wang, Z. Liu, D. Gu, “Ciphertext policy attribute-based encryption for circuits from LWE assumption,” in *Proc. of the 21st International Conference on Information and Communications Security (ICICS 2019)*, Beijing, China, 278-396, 2019. Article(CrossRefLink).

[25] Z. Brakerski and V. Vaikuntanathan, “Lattice-Inspired Broadcast Encryption and Succinct Ciphertext-Policy ABE,” in *Proc. of 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, pp. 28:1-28:20, 2022. Article(CrossRefLink).

[26] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, “Practical Lattice-Based Zero-Knowledge Proofs for Integer Relations,” in *Proc. of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event USA, pp. 1051–1070, 2020. Article (CrossRef Link).

[27] K. Zhou and L. Cai, “A decentralized access control algorithm for PHEV charging in smart grid,” *Energy Syst*, vol. 5, no. 4, pp. 607–626, Dec. 2014, Article (CrossRef Link).

[28] Y. Xie et al., “Three-Layers Secure Access Control for Cloud-Based Smart Grids,” in *Proc. of 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Boston, MA, USA, pp. 1–5, 2015. Article (CrossRef Link).

[29] Z. Guan, J. Li, L. Zhu, Z. Zhang, and X. Du, “Towards Delay-Tolerant Flexible Data Access Control for Smart Grid with Renewable Energy Resources,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3216-3225, 2017. Article(CrossRefLink).

[30] E. Hauck, E. Kiltz, J. Loss, and N. K. Nguyen, “Lattice-Based Blind Signatures, Revisited,” in *Proc. of Advances in Cryptology – CRYPTO 2020*, pp. 500–529, 2020. Article (CrossRef Link).

[31] S. H. Seo, J. Won, S. Sultana, E. Bertino, “Effective key management in dynamic wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10 no. 2, pp. 371-383, 2015. Article(CrossRefLink).

[32] R. Tavakoli, M. Nabi, T. Basten, and K. Goossens, “Dependable Interference-Aware Time-Slotted Channel Hopping for Wireless Sensor Networks,” *ACM Trans. Sen. Netw.*, vol. 14, no. 1, pp. 1–35, Feb. 2018. Article (CrossRef Link).

[33] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, “Shorter Lattice-Based Zero-Knowledge Proofs via One-Time Commitments,” in *Proc. of Public-Key Cryptography – PKC 2021*, pp. 215–241, 2021. Article (CrossRef Link).

[34] T. Attema, V. Lyubashevsky, and G. Seiler, “Practical Product Proofs for Lattice Commitments,” in *Proc. of Advances in Cryptology – CRYPTO 2020*, pp. 470–499, 2020. Article (CrossRef Link).

Wangke Yu received his Ph.D. in 2011 from the School of Computer Network and Security, Xidian University, China. His research interests include Information security, computer communication and network security.

Shuhua Wang received her Ph.D. in 2020 from the School of Statistics and Mathematics, Zhejiang Gongshang University, China. Her PhD was on convergence analysis of kernel-based learning algorithms. Her research interests include machine Information security, optimization theory and application.