# Fine-grained Access Control Method for Blockchain Data Sharing based on Cloud Platform Big Data

Yu Qiu*, Biying Sun, Qian Dang, Chunhui Du, Na Li
State Grid Gansu Electric Power Company Internet Division, Lanzhou, China

***Abstract*—Blockchain technology has the advantages of decentralization, de-trust, and non-tampering, which breaks through the limitations of traditional centralized technology, so it has gradually become the key technology of power data security storage and privacy protection. In the existing smart grid framework, the grid operator is a centralized key distribution organization, which is responsible for sending all the secret credentials, so it is easy to have a single point of failure, resulting in a large number of personal information losses. To solve the problems of inflexible access control in smart grid data-sharing framework and considering the limitation of multi-party cooperation among grid operators and efficiency, an attribute-based access control scheme supporting privacy preservation in smart grid is constructed in this paper. A fine-grained access control scheme supporting privacy protection is designed and extended to the smart grid system, which enables the system to achieve fine-grained access control of power data. A decryption test algorithm is added before the decryption algorithm. Finally, through performance analysis and comparison with other schemes, it is verified that the performance of this system is 7% higher than the traditional method, and the storage cost is 9.5% lower, which reflects the superiority of the system. Full optimization of the access policy is achieved. It is proved that the scheme is more efficient to implement the coordination and cooperation of multiple authorized agencies in the system initialization.**

***Keywords*—Power grid data; blockchain technology; data sharing; fine-grained access control; game strategy; ciphertext key***

## I. INTRODUCTION

With the wide application of big data, fog computing, and Internet of Things technology, more and more applications store a large number of users' private data in the near-end fog node for computing. This solves the problem of insufficient storage space or limited computing resources of most mobile terminals in the current Internet of Things environment. At the same time, with the rise of new network architectures such as SDN, the computing, and storage capabilities of edge network devices and core gateway devices are continuously enhanced [1]. However, because the private data of users can bring commercial value to criminals, Internet of Things devices with weak performance have become the main target of hackers [2]. To prevent the user's data from being stolen, it is necessary to authenticate all unknown devices in the environment through identity authentication and other technical means, and then grant the corresponding device access to data after passing the identity authentication. However, most of the existing identity authentication schemes ignore the user's privacy disclosure in the authentication process, including the user's functional attributes, real identity privacy and geographical location privacy.

Power data can be used by other organizations outside the grid system, for example, to calculate costs, monitor unexpected behavior, and predict future conditions. However, the power data of a single smart meter contains private information such as household habits, which needs to be protected. Therefore, how to balance the availability and privacy of power data is a problem faced by the smart grid [3]. In addition, RTUs and power consumers want to control access from users. Users want to get different power information depending on their specific tasks. For example, maintainers and system engineers monitor the network, while costing and analysis will be performed by auditors [4]. Therefore, in the smart grid system, it is particularly important to achieve fine-grained access control of power data [5]. However, most of the existing smart grid schemes focus on information aggregation but ignore the privacy protection and access control in the process of power data sharing.

Blockchain technology is a trusted storage network composed of distributed equal nodes, consisting of tamper-proof block data and automatically executable smart contract code, which has the characteristics of tamper-proof, coordination autonomy, high security, and trust of decentralized decision-making [6]. In the research of data sharing mechanisms based on blockchain, Dai Mingjun et al. [7] promoted the storage space of blockchain through distributed storage (DS) based on network coding (NC). Yang Jiachen et al. [8] introduced encryption algorithms to solve the problem of distributed secure storage of big data. Wang Zuan et al. [9] separated the original data storage and data transactions by using a double-chain structure and combined with proxy re-encryption technology to achieve secure and reliable data sharing. In 2016, Alharbi et al. [10] proposed an efficient privacy-preserving identity-based signature (IBS) scheme for smart grid communication. In 2017, a smart grid communication model [11] was proposed by Sedaghat et al., in which the cloud proxy service center, as a trusted third party with powerful computing power, is responsible for partially decrypting the shared ciphertext to reduce the burden of authorized users. In 2019, a privacy-preserving power data aggregation scheme [12] was proposed by Liu et al., but this scheme does not consider the access control of shared data.

This paper aims to design a fine-grained access control scheme supporting privacy preservation in the cloud environment. Firstly, a fine-grained access control scheme for data sharing with a completely hidden access policy is constructed. Then, based on this, extended research on

application scenarios is carried out, and an attribute-based access control scheme supporting privacy preservation in a smart grid is constructed.

The main innovations of this paper are:

*1)* The access policy and attribute set are transformed into vectors, and the access policy is completely hidden.

*2)* An attribute-based access control scheme supporting privacy preservation in a smart grid is constructed. Combine blockchain technology to control data sharing and access.

*3)* The scheme in this paper can realize the independent work of multiple distribution network operators, realize lightweight encryption, and improve decryption efficiency.

Content and structure of this paper are as follows:

*1)* Elaborate the research direction, introduce the research background and content;

*2)* Introduce the theoretical content of the relevant basic content;

*3)* Design the security game strategy of power grid big data access control system;

*4)* Establish a shared data access scheme for power grid block chain;

*5)* Realize the attribute-based access control scheme for the power grid privacy protection;

*6)* Summarize the paper and look forward to the next step.

## II. Related Work

### A. Access Control Security Model

With the rapid development of the ubiquitous power Internet of Things (IoT), various IoT intelligent terminal devices deployed in the smart grid generate a large amount of data. Although the application of cloud Internet of Things technology has effectively solved the problem of massive data collection, storage and sharing, the smart grid is faced with a huge number of intelligent terminal devices deployed in all aspects of the grid, users with a sharp increase in data and mixed personnel. Therefore, the data privacy security issues that involve posing a serious security threat [13]. These security threats are mainly manifested in:

Data security risk: the combination of smart grid and Internet of Things technology, and the application of various emerging technologies in the smart grid makes the system complexity of the smart grid become higher. The security risk of various types of data is increased [14]. The application of cloud Internet of Things technology effectively realizes the collection, storage, and management of terminal data, but when it interacts with users, business systems, and power grid researchers, the misoperation and illegal access will cause data leakage.

User privacy risk: In the smart grid, while protecting the privacy data of ordinary users, it is also necessary to prevent the leakage of grid system data. Users' personal information and power consumption data belong to users' privacy; and the important operation data of each link of the smart grid system also need to be protected [15]. In the face of distributed attacks by illegal elements, illegal access by malicious users and illegal operations by staff, the privacy data of power grid users and systems will be threatened.

### B. Safety Requirements

According to the security threat analysis of data privacy protection in the smart grid cloud Internet of Things, effective access control methods are adopted to achieve the goal of data privacy security, and the following security requirements are considered:

*1) Authentication:* The identity of the user connected to the smart grid control center needs to be authenticated to prevent the user from stealing private data under false names. Data visitors must be authenticated with the control center in both directions [16].

*2) Data confidentiality:* When a visitor in the smart grid needs to decrypt and obtain encrypted data, its attribute set needs to meet the access policy requirements defined by the data owner, and unauthorized visitors cannot access user data.

*3) Anti-collision attack:* Unauthorized users cannot combine their key information to decrypt the ciphertext through the collusion of multiple users.

*4) Forward-backward confidentiality:* The newly authorized visitor cannot decrypt the previous ciphertext data with his own private key; the unauthorized visitor cannot decrypt the decrypted ciphertext data [17].

*5) Data integrity:* All kinds of private data must be encrypted before they can be transmitted between entities to avoid illegal tampering, damage and plagiarism during transmission and storage [18].

## III. Power Grid Big Data Access Control System

The system consists of five main bodies, as shown in Fig. 1.

Grid Operator (GO): As a certification center, the GO is responsible for setting up the smart grid system, distributing GIDs to users, and granting access to users. In addition, GO distributes identity keys for legitimate users.

Multiple Distribution Operators (DGOs): As multiple attribute authorities, each DGO is responsible for establishing its own domain, managing attributes, and distributing attribute keys to users according to the attribute set.

Cloud storage server: It is responsible for storing power data in the form of ciphertext. The cloud storage server does not participate in the access control and data decryption process.

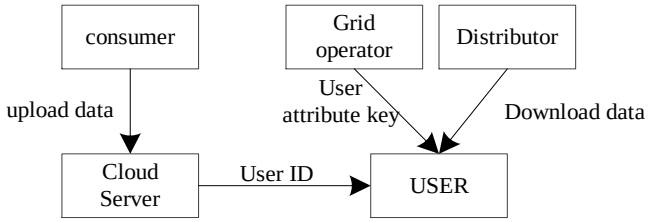


Fig. 1. Access Control System Model of Smart Grid.

Power data owners: Power data owners include RTUs and power consumers. The owner of the power data can define an access policy, use it to encrypt the power data, and upload it to the cloud storage server.

Users: Users may be maintainers, system engineers, researchers, policymakers, and auditors of power systems [19]. After the user downloads the encrypted power data from the cloud storage server, if the user wants to decrypt it, he needs to prove his identity to GO and initiate a key request to DGOs.

### A. Fine-grained Shared Security Game Strategy

This section will elaborate the security model of the scheme based on the security game between the attacker $A$ and the simulator $B$. Among them, the security game will have the following stages:

Initialization: attacker $A$ sends fine-grained authority $DGO_k^*$ to emulator $B$, and d gets the public parameter $pp$ of the system.

Authority establishment: for each fine-grain authority, that simulator $B$ runs an authority establishment algorithm. The public key $PK_k$ and the private key $SK_k$ are obtained, and then the public key $PK_k$ is published to $A$ [20].

Stage 1: Attacker $A$ submits attribute vector $\vec{y}$ and GID and initiates a user key challenge to impersonator $B$. Wherein the vector $\vec{y}$ is generated by encoding the attribute set $S'$ randomly selected by $A$. $B$ runs the user key generation algorithm and replies the corresponding $SK_{k,j}$ and $SK_{gid}$ to $A$. In phase 1, $A$ may interrogate the key within the PPT.

Challenge: $A$ submits two messages $M_0$. $M_1$ of equal length and two policy vectors $\vec{x_0}$, $\vec{x_1}$ to $B$. Wherein, the vectors $\vec{x_0}$ and $\vec{x_1}$ are respectively encoded and generated by the access strategies $W_0^{'}$ and $W_1^{'}$ selected by $A$ [21]. But it must be satisfy that neither that vector $\vec{x_0}$ nor the vector $\vec{x_1}$ is orthogonal $\vec{y}$, that is, $(<\vec{x_0},\vec{y}>\neq 0)\wedge(<\vec{x_1},\vec{y}>\neq 0)$. Simulator $B$ tosses a coin to generate a random bit $\xi\in\{0,1\}$, and then runs the encryption algorithm to generate the corresponding ciphertext $CT_\xi$ and sends it to attacker $A$.

Stage 2: As in stage 1, $A$ then makes a user key challenge to $B$. But must satisfy that vector $\vec{x_0}$. Neither $\vec{x_1}$ nor the vector $\vec{y}$ is orthogonal.

Guess: $A$ guesses $\xi$ and gives $\xi'$. If $\xi'=\xi$, then $A$ wins and the winning margin is $Adv_A=\left|\Pr[\xi'=\xi]-\frac{1}{2}\right|$.

### B. Threshold Access Policy

The key technologies of threshold access policy encoding are divided into the following two parts:

*1) The access policy W is transformed into a vector $\vec{x}$:*

First, the power data owner defines an access policy $W=\left\{t_{1,n_1},t_{2,n_2},\cdots,t_{j,n_j}\right\}$, selects t random coefficients $a_i\in Z_p$, and sets a polynomial $f(x)$ of order $t-1$ as follows:

$$f(x)=a_{t-1}x^{t-1}+\cdots+a_1x+a_0 \pmod p \tag{1}$$

Then, for each element $t_{i,j}$ in the access policy W, the component elements of the corresponding vector $\vec{x}$ are generated:

$$\begin{cases} x_i=\begin{cases} f(t_{i,j}) & t_{i,j}\in W \\ 0 & t_{i,j}\notin W \end{cases}:\forall i=1,\cdots,L-1 \\ x_L=-f(0)=-a_0 \end{cases} \tag{2}$$

*2) Convert the attribute set $S_k$ to a vector $\vec{y}$:*

Let $S=\left\{v_{1,n_1},v_{2,n_2},\cdots,v_{j,n_j}\right\}$ and $U_k=\left\{w_{1,n_1},w_{2,n_2},\cdots,w_{j,n_j}\right\}$ be two attribute sets of the same length, where S represents the attribute set of the user in the system, and $U_k$ represents the attribute set managed by the authority $DGO_k$. For a corresponding location that is not an attribute managed by $U_k$, let $w_{i,j}=0$. Define $S_k=S\cap U_k=\begin{cases} v_{i,j} & v_{i,j}=w_{i,j} \\ 0 & v_{i,j}\neq w_{i,j} \end{cases}$. Then, calculate the value of the Lagrange polynomial $\Delta_{v_{i,j},S}(x)$ at $x=0$, where $\Delta_{v_{i,j},S}(x)=\prod_{k\in S,i\neq k}\frac{x-v_{k,j}}{v_{i,j}-v_{k,j}}$. For each element $v_{i,j}$ in the attribute set $S_k$, a component element of the corresponding vector $\vec{y}$ is generated:

$$\begin{cases} y_i=\begin{cases} \Delta_{v_{i,j},S}(0) & v_{i,j}\in S_k \\ 0 & v_{i,j}\notin S_k \end{cases}:\forall i=1,\cdots,L-1 \\ y_L=1 \end{cases} \tag{3}$$

Attention:

$$< \vec{x}, \vec{y} >= f(0) \Leftrightarrow t_{i,j} = v_{i,j} (i \geq t) \Leftrightarrow S \perp W \quad (4)$$

The above calculations only appear in the exponential part of the decryption phase.

## IV. Blockchain Shared Data Access Scheme

$u = \{att_1, \cdots, att_L\}$ is defined as the global attribute set of the system and $H : \{0,1\}^{\lambda} \times Z_p^{l+1} \to Z_p^{k+1}$ is a collision-resistant hash function. The specific construction of the attribute-based access control scheme supporting privacy protection in the smart grid is as follows:

System initialization: This phase consists of the following two algorithms. GO generates the whole system by running the system establishment algorithm, and DGOs generates its own domain by running the authority establishment algorithm.

GO-Setup: Run the group generator g to generate the bilinear group $(p, g_1, g_2, e, G_1, G_2, G_T)$. GO builds N authorities for the system, respectively: $DGO_1, DGO_2, \cdots, DGO_N$, where each $DGO_k$ manages a mutually exclusive set of attributes $U_k = \{Att_1, Att_2, \cdots, Att_{n_k}\}$, and $|U_k| = n_k$. Let $\sum_{sign} = (keygen, Sign, Verify)$ be a signature scheme. Select the random matrix $A, B \in Z_p^{(k+1)\times k}$, $P \in Z_p^{(k+1)\times(k+1)}$, calculate $P_1 = g_1^A, P_2 = g_2^B, X = g_1^{P^{\mathrm{T}}A}$, and return the common parameter $pp$ as follows:

$$pp = \{G_1, G_2, G_T, e, p, g_1, g_2, P_1, P_2, X, Verify\} \quad (5)$$

DGOS-Setup: For any authority $DGO_k$ in the system, select two random matrices $U_k, W_k \in Z_p^{(k+1)\times(k+1)}$ and a random vector $\overrightarrow{a_k} \in Z_p^{k+1}$, calculate $V_{1,k} = g_1^{U_k^{\mathrm{T}}A}, V_{2,k} = g_1^{W_k^{\mathrm{T}}A}, Y_k = e(g_1, g_2)^{\overrightarrow{a_k}^{\mathrm{T}}A}$, and then publish the public key $PK_k$ of $DGO_k$ and keep the private key $SK_k$.

$$PK_k = \{V_{1,k}, V_{2,k}, Y_k\}, SK_k = \{U_k, W_k, \overrightarrow{\alpha_k}\} \quad (6)$$

Authentication and key distribution: When a user joins the system, GO assigns a unique GID to the user. If the user wants to decrypt the ciphertext, first, the user needs to convert the attribute set S into a vector $\vec{y} = \{y_j \mid j \in [1, L]\}$, the user needs to submit the attribute set S and the attribute vector $\vec{y}$ to request the key from GO. For the legal user who has completed the registration, GO will distribute the identity key $SK_{gid}$ with the signature to the legal user by running the identity key generation algorithm. Next, the user needs to submit the attribute set S, the attribute vector $\vec{y}$, and the identity key $SK_{gid}$ with the GO signature to request the attribute key from the DGOs. Each $DGO_k$ then uses Verify to verify the signature. Once the verification is passed, each $DGO_k$ generates attribute keys $SK_{k,j}$ by running the attribute key generation algorithm and sends them to the user. This process involves the following two algorithms:

Identity key generation (GO-KeyGen): For the authentication center GO in the system, randomly select two vectors $\vec{\gamma} \in Z_p^{(k+1)}, \vec{r} \in Z_p^k$ and calculate the user identity key:

$$SK_{gid} = P_2^{\frac{\vec{r}}{u+\vec{\gamma}}} \quad (7)$$

Where, $u = H(GID, \vec{y})$.

Attribute key generation (DGOS-KeyGen): For each authority $DGO_k$ in the system, it is first necessary to convert the attribute set $S_k$ into a vector $\vec{y} = \{y_j \mid j \in [1, n_k], \sum_{k=1}^{N} n_k = L\}$, where $S_k = S \cap U_k$, according to Section 4.1.5, and then calculate the user attribute key:

$$SK_{k,j} = g_2^{\overrightarrow{\alpha_k}} [(SK_{gid}{}^{\mathrm{T}})^{y_j U_k{}^{\mathrm{T}} + W_k{}^{\mathrm{T}}}]^{\mathrm{T}} \quad (8)$$

Data release: The power data owner defines an access policy W, and converts it into a vector $\vec{x}$; then, the power data $M_p$ is encrypted by the following encryption algorithm, and the ciphertext $CT_p$ is uploaded.

Encrypt: For the power data owner in the system, randomly select two vectors $\vec{s}, \overrightarrow{s^*} \in Z_p^k$ and calculate the ciphertext $CT_p = \{C_0, C_1, C_k, C_j^*, C_{k,j}\}$ as follows:

$$\begin{cases} C_0 = M_p \cdot \prod_{k=1}^{N} Y_k^{\vec{s}} = M_p \cdot e(g_1, g_2)^{\sum_{k=1}^{N} \overrightarrow{\alpha_k}^{\mathrm{T}} \cdot A\vec{s}} \\ C_1 = P_1^{\vec{s}} \\ C_k = V_{2,k}{}^{\vec{s}} = g_1^{W_k^{\mathrm{T}} A\vec{s}} \\ C_{k,j} = [X^{x_j} \cdot V_{1,k}]^{\vec{s}} = g_1^{(x_j P^{\mathrm{T}} + U_k^{\mathrm{T}}) A\vec{s}} \\ C_j^* = P_1^{\overrightarrow{s^*} x_j} (k \in [1, N], j \in [1, L]) \end{cases} \quad (9)$$

Data recovery: Any user can access the power data encrypted in the cloud, but only when $S \perp W$, the authorized user can successfully decrypt it. In order to reduce the cost of decryption, the decryption process is divided into two stages: decryption test and complete decryption. The user first runs the test algorithm to verify $S \perp W$ or $S \forall W$. If $F(W,S)=1$ is output, the user runs the full decryption algorithm; otherwise, the decryption is terminated. Details are as follows:

Decryption Test Phase: User calculation:

$$F(W,S)=\sum_{j=1}^{l+1} C_j^{*y_j} \tag{10}$$

Attention: $F(W,S)=1 \Leftrightarrow \sum_{j=1}^{L} x_j y_j = 0 \Leftrightarrow S \perp W$. If output $F(W,S)=1$, so, it represents $S \perp W$, then the user will proceed to the next stage for full decryption; otherwise, the user will terminate decryption.

Dec-Phase: Once the above test Phase is passed, it indicates $S \perp W$, and the user has performed the following calculations:

$$C_0 \cdot \frac{e(\prod_{k=1}^{N}\prod_{j=1}^{L} C_{k,j}^{\ y_j} \cdot C_k, SK_{gid})}{e(C_1, \prod_{k=1}^{N}\prod_{j=1}^{L} SK_{k,j})} = M_p \tag{11}$$

## V. Attribute-based Access Control Scheme for Privacy Protection in Power Grid

System initialization Setup1 (PK, MSK):

Enter the security parameters to obtain the public key PK and the master key MSK.

Encrypt (M, PK, W) CT: Input message M, public key PK, and access policy W to get ciphertext CT.

Key GenPK, MSK, S SK: Input public key PK, master key MSK and attribute set S to get user key SK.

Decrypt CT, SK, PK M or: input ciphertext CT, user key SK and public key PK, if S W, output message M; otherwise, the algorithm aborts and outputs.

System Setup (GO-Setup): This phase is executed by GO, which inputs security parameters $1^{\lambda}$ and obtains system public parameters $pp$, as well as a pair of signature and authentication keys (Sign, Verify).

DGOS-Setup: This algorithm is executed by DGOs, which inputs the subscript k of DGOk and outputs the public and private keys.

User key generation (KeyGen): includes two stages of identity key generation and attribute key generation, as follows:

*1)* Identity key generation phase (GO-KeyGen): This phase is executed by GO. Input the global identity GID of the user to get the identity key $SK_{gid}$ of the user.

*2)* Attribute key generation phase (DGOS-KeyGen): This phase is performed by DGOs, inputting the private key $SK_k$ and the encoding vector $\vec{y}$ of the attribute set S, and then outputting the attribute key $SK_{k,j}$ of the user.

Encrypt: The algorithm is run by the owner of the power data, inputting the public key $PK_k$, power data $M_p$, and the encoding vector $\vec{x}$ of the access policy W, and outputting the power data in encrypted form $SK_{k,j}$.

Decrypt: This algorithm includes two phases: decryption test and full decryption, as follows:

*1)* Decryption Test Phase: Input the power data $CT_p$ in encrypted form and the encoding vector $\vec{y}$. If $F(W,S)=1$, proceed to the next phase; otherwise, the algorithm is aborted.

*2)* Complete Decryption Phase (Dec-Phase): Input the power data $CT_p$ in encrypted form, the encoding vector $\vec{y}$, the user's attribute key $SK_{k,j}$ and the user's identity key $SK_{gid}$, and output the power data $M_p$ or $\perp$.

## VI. Experimental Analysis

### A. Experimental Platform

The experimental environment builds a micro-cloud environment to simulate the big data service under the cloud platform. The server-side and client-side configurations are shown in Table I.

This paper is based on the Pairwise Cryptography Laboratory (PBC) and uses 160-bit elliptic curve groups over a 512-bit finite field, which are used to calculate the cost of the test operation and the decryption operation.

### B. Performance Analysis

In the simulation test, $E_{G_1}$, $E_{G_2}$ and $E_{G_T}$ respectively represent the time cost of an index operation in $G_1$, $G_2$ and $G_T$. $N_W$ and $N_S$ represent the number of attributes in the access policy and user attribute set, respectively. The $\hat{e}$ represents the time cost required to compute a bilinear function. The $O(H)$ represents the time required to compute a hash function. The $p_i$ indicates the number of possible values for a multivalued attribute.

*1) Theoretical analysis:* In Table II, this scheme is further compared with scheme [22-25] from four aspects of key generation cost, encryption cost, test cost and decryption cost.

TABLE I. EXPERIMENTAL PLATFORM CONFIGURATION PARAMETERS

| Configurations | Type | |
|---|---|---|
| | Server side | Client side |
| CPU | Core(TM) i7-10900k4.6GHz | Core(TM) i5-10400f 4.3GHz |
| Memory | 128G | 16G |
| System | Windows Server LTSC Preview | Windows 11 |

TABLE II. PERFORMANCE COMPARISON OF SMART GRID ACCESS CONTROL SCHEMES

| Plan | Types | Independent authorized agency | Decryption test | Full hiding strategy | IPE | Adaptive safety |
|---|---|---|---|---|---|---|
| [22] | MA-ABE | √ | × | × | × | × |
| [23] | MA-ABE | √ | × | × | × | × |
| [24] | MA-ABE | √ | × | × | × | × |
| [25] | D-MA-ABE | × | × | √ | √ | √ |
| The plan | MA-ABE | √ | √ | √ | √ | √ |

TABLE III. COMPARISON OF COMPUTATIONAL COMPLEXITY OF SMART GRID ACCESS CONTROL SCHEMES IN DIFFERENT STAGES

| Plan | User key generation | | Encryption | | | Decryption test | | | Fully decrypted | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | $E_{G2}$ | O(H) | e | $E_{G1}$ | $E_{GT}$ | e | $E_{G1}$ | $E_{GT}$ | e | $E_{G2}$ | $E_{GT}$ |
| [25] | $N_S$ | $N_S$ | 1 | $1 + N_W$ | 1 | - | - | - | 2 | 2 | $2p_iN_S$ |
| The plan | $N_S$ | 0 | 1 | $1+3N_W$ | 1 | 0 | $p_iN_S$ | 0 | 1 | $3p_iN_S$ | 3 |

It can be seen from Table III that this scheme is more efficient than the scheme [25] in the key generation and decryption stages because of the calculation of the hash function in the scheme [25].

*2) Simulation test:* The actual performance of the present protocol and the protocol [25] will be tested. The results show that, compared with the scheme [25], the present scheme has obvious advantages in both the key distribution phase and the decryption phase. Fig. 2 shows the comparison of the storage cost of this scheme and the scheme [25] in each stage of the algorithm. In the simulation, the lengths of the elements in the bilinear groups $G_1$, $G_2$, and $G_T$ are set to 512 bits. Assume that there are 10 authorities in the system, that is, $N=10$, and specify that each authority manages five attributes.

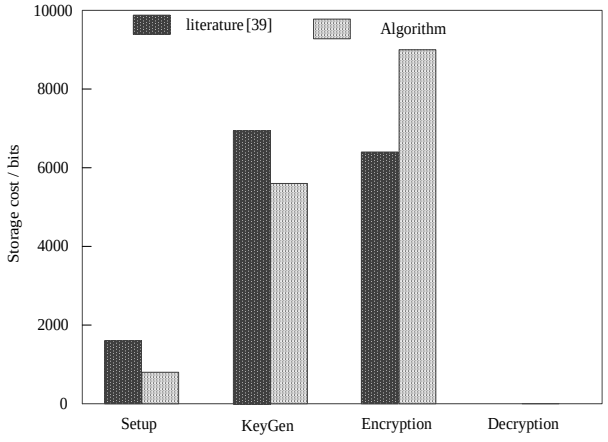


Fig. 2. Storage Cost Comparison.

It can be seen from Fig. 2 that, compared with the scheme [25], the construction of this scheme requires less space to store the public key and the secret key of the user. Fig. 3, Fig. 4 and Fig. 5 respectively show the running time comparison of the user key distribution algorithm, the encryption algorithm and the decryption algorithm in this scheme and the scheme [25].

Fig. 3 shows that the running time of the user key distribution algorithm of the two schemes increases linearly with the number of attribute sets.

As can be seen from Fig. 4, the efficiency of the encryption algorithm in this scheme is obviously low, which is a compromise for security performance.

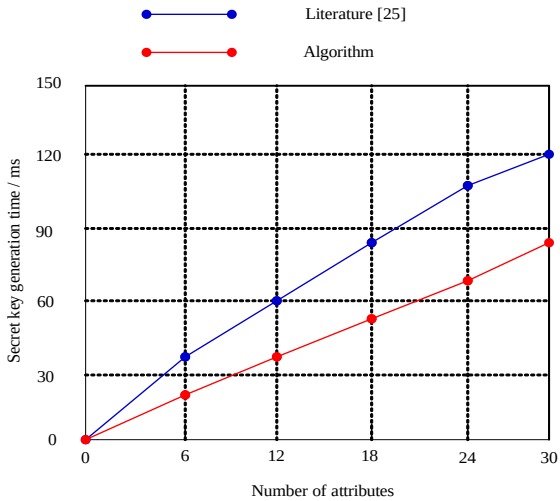


Fig. 3. Comparison of Secret Key Generation Time.

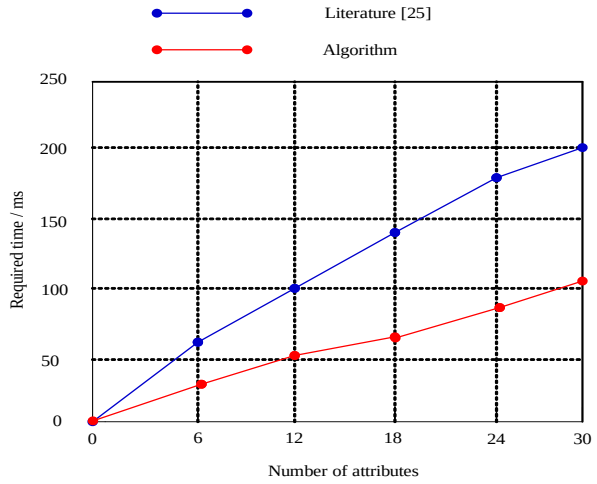


Fig. 4. Time Comparison of Encryption Algorithms.

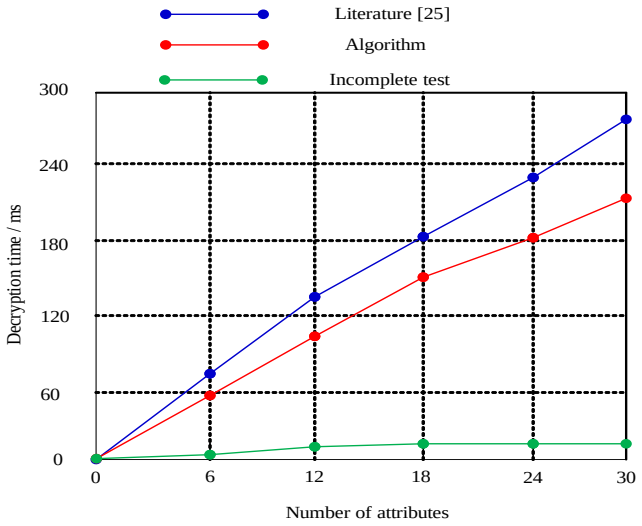


Fig. 5. Time Comparison of Decryption Algorithms.

As shown in Fig. 5, the decryption test algorithm in this scheme takes significantly less time than the full decryption algorithm. If the attribute set of the user does not satisfy the access policy, the scheme only executes the decryption test algorithm and does not need to execute the complete decryption operation. Due to the decryption test operation, the time required for successful decryption of the present scheme is much shorter than that of the scheme [25].

### C. Discussion

If the distributions of encryption and decryption are statistically similar, there is no one simulator B that can distinguish the two strategies by any advantage.

Proof: In the challenge phase, simulator B randomly selects A, to satisfy.

Then generate:

$$C_{k,j} = g_1^{(x_{b,j}P^{\mathrm{T}}+U_k^{\mathrm{T}})(A\vec{s}+b^{\perp}\hat{s})} = g_1^{x_{b,j}P^{\mathrm{T}}(A\vec{s}+b^{\perp}\hat{s})} \cdot g_1^{U_k^{\mathrm{T}}(A\vec{s}+b^{\perp}\hat{s})} \quad (12)$$

Given $g_1^A, g_1^{A\vec{s}+b^{\perp}\hat{s}}, g_1^{U_k^{\mathrm{T}}A}, g_2^B$, this term $g_1^{U_k^{\mathrm{T}}(A\vec{s}+b^{\perp}\hat{s})}$ is uniformly distributed in the group. Therefore, there is no adversary that can distinguish strategies $Game_3$ and $Game_4$ with any advantage.

In the strategy $Game_4$, in the opponent's view, the choice of $b$ by the simulator $B$ is statistically independent, and the opponent cannot win the strategy by any advantage.

If the K-Linear assumption holds, the privacy-preserving power data access control scheme is IND-CPA secure.

It is proved that under the k-Linear assumption, based on the proof of the above lemma, the attacker's advantage in winning the real security strategy is negligible. Therefore, the attacker cannot break the scheme in the PPT.

## VII. Conclusion

In this paper, a fine-grained access control scheme is proposed to support data sharing in the smart grid. The main work includes:

*1)* The decentralized attribute-based encryption scheme is extended to the smart grid system, which is based on a more flexible threshold access structure.

*2)* In order to improve the efficiency, a test phase is added before the data is completely decrypted, which avoids many unnecessary decryption operations.

*3)* Based on the k-Linear assumption, it is proved that the scheme achieves adaptive security.

Performance analysis shows that this scheme has obvious advantages compared with similar schemes.

The content of this paper can protect the privacy information of the trajectory data, and improve the availability of the data. Finally, through the experimental verification, it is proved that the proposed method not only protects the privacy information of trajectory data but also improves the availability of data.

In the next step, when the privacy budget is allocated by the special series method. Although infinitely many points can be protected, if there are too many position points in trajectory data, the smaller the privacy budget allocated to the later position points is, the larger the corresponding added random noise is. Then, the availability of the data will be reduced.

## References

[1] Zhang P, Song J. Research progress on performance optimization of blockchain consensus algorithm. Computer Science, 2020, 47(12): 296-303.

[2] Lu G, Xie L, Li X. A comparative study of blockchain consensus algorithms. Computer Science, 2020, 47(6A): 332-339.

[3] Bamakana S, Motavali A, Bondarti A. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 2020, 154: 1-21.

[4] W. Sun, L. Wang, P. Wang, and Y. Zhang. Collaborative blockchain for space-air-ground integrated network. IEEE Wireless Communications, 2020, 27(6): 82-89.

[5] Sel D, Zhang K, Jacobsen H. Towards solving the data availability problem for sharded Ethereum. SERIAL 2018-Proceedings of the 2018

Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, 2018, 1: 25-30.

[6] Liu X, Feng J. Trusted blockchain oracle scheme based on aggregate signature. Journal of Computer and Communications, 2021: 95-109.

[7] Fan H, Liu Y, Zeng Z, Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain. Sensors, 2020, 20(18): 1-14.

[8] Xue Z, Pan X, Lv Z, et al. Application of blockchain in energy and power business. Journal of Physics: Conference Conference Series, 2020, 1626(1): 1-7.

[9] Zeng Z, Li Y, Cao Y, et al. Blockchain technology for information security of the energy internet: fundamentals, features, strategy and application. Energies, 2020, 13(4): 1-24.

[10] J. Huang, C. Lin, H. Zhou, Z. Xu, and C. Lin. Research on key technologies of deduction of multinational power trading in the context of Global Energy Interconnection. Global Energy Interconnection, 2019, 2(6): 560-566.

[11] Y. Jiang, C. Wang, Y. Wang, and L. Gao. A cross-chain solution to integrating multiple blockchains for IoT data management. Sensors (Switzerland), 2019, 19(9): 1-18.

[12] G. van Leeuwen, T. AlSkaif, M. Gibescu, and W. van Sark. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. Applied Energy, 2020, 263(1): 114613.

[13] M. Kim, et al. A secure charging system for electric vehicles based on blockchain. Sensors (Switzerland), 2019, 19(13): 1-22.

[14] E. Mengelkamp, J. Gärttner, K. Rock. Designing microgrid energy markets A case study: The Brooklyn Microgrid. Applied Energy, 2018, 210: 870–880.

[15] Z. Ji, X. Wang, C. Cai, and H. Sun. Power entity recognition based on bidirectional long short-term memory and conditional random fields. Global Energy Interconnection, 2020, 3(2): 186-192.

[16] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov. Blockchain in smart grids: A review on different use cases. Sensors (Switzerland), 2019, 19(22): 1-25.

[17] J. Zhang, et al. Design scheme for fast charging station for electric vehicles with distributed photovoltaic power generation. Global Energy Interconnection, 2019, 2(2): 150-159.

[18] P. Liu, W. Jiang, X. Wang, H. Li, H. Sun. Research and application of artificial intelligence service platform for the power field. Global Energy Interconnection, 2020, 3(2): 175-185.

[19] B. Hong, Q. Li, W. Chen, B. Huang, H. Yan, K. Feng. Supply modes for renewable-based distributed energy systems and their applications: case studies in China. Global Energy Interconnection, 2020, 3(3): 259-271.

[20] N. Saxena, B. J. Choi. Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks. IEEE Transactions on Information Forensics & Security, 2017, 11(7): 1438-1452.

[21] M. S. Rahman, A. Basu, S. Kiyomoto, M. Z. A. Bhuiyan. Privacy-friendly secure bidding for smart grid demand-response. Information Sciences, 2017, 379: 229-240.

[22] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. L. Wei, P. Hong. RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967.

[23] Aitzhan N Z, Svetinovic D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840-852.

[24] Fan, T.; He, Q.; Nie, E.; Chen, S. A study of pricing and trading model of Blockchain & Big data-based Energy-Internet electricity. In Proceedings of the 3rd International Conference on Environmental Science and Material Application (ESMA 2018), Chongqing, China, 25 – 26 November 2018: 1 – 12.

[25] POP, Claudia, et al. Blockchain based decentralized management of demand response programs in smart energy grids. Sensors, 2018, 18(1): 162.