





Research Article

SACS-ABE&B: Supervised Access Control Scheme Based on Attribute-Based Encryption and Blockchain

Guo Kaiyang ^{1,2} Han Yiliang ^{1,2} Wu Riming ^{1,2} and Liu Kai ^{1,2}

¹Engineering University of the PAP, Xi'an 710086, China

²Key Laboratory for Network and Information Security of the PAP, Xi'an 710086, China

Correspondence should be addressed to Han Yiliang; hanyil@163.com

Received 29 December 2021; Revised 17 June 2022; Accepted 3 August 2022; Published 23 September 2022

Academic Editor: Zhili Zhou

Copyright © 2022 Guo Kaiyang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Aiming at the problem of illegal data sharing of malicious users in the access control scheme based on attribute-based encryption, an access control scheme that can restrict the sending ability of data owners is proposed. By adding a sanitizer to sanitize the ciphertext, it can ensure that parties who do not adhere to the system control policy cannot share information effectively. The scheme is constructed based on blockchain, and the traceability of access process can be realized. Off-chain storage can also lower the blockchain storage load. The scheme meets the No-Read and No-Write rules, achieves chosen-plaintext attack security under the random oracle model, and can against quantum attacks. As a result of theoretical analysis and experimental simulation, the scheme has certain feasibility and practical significance.

1. Introduction

For the increasing needs of information security, cryptography and information security technology have attracted more and more attention. Access control can protect data resources from unauthorized access, which is an important component of information security technology [1]. The rapid growth of data in cyberspace poses a new challenge to the research of access control: how to develop the traditional access control technology to solve the new cloud data security problem. As a public key encryption technology, attribute-based encryption (ABE) can not only encrypt data, but also realize fine-grained access control of data, which provides a method to solve problems [2, 3]. As a powerful advanced cryptographic primitive, compared with traditional public key encryption, one of its biggest features is that ABE can realize “one to many” secure data sharing and can improve data sharing efficiency [4].

Although the ABE has certain advantages in access control, there are still some problems that cannot be ignored from the real practical application. These problems include the inherent problems of ABE, such as attribute revocation [5–7], preserve privacy [8–10] and traceable [11–13]. In

addition, there are other potential security issues that need to be attended. For example, in ciphertext policy attribute-based encryption (CP-ABE), the data owner determines the access object of the data, and in this case once a malicious user carries out illegal data sharing in the public channel, the system will not be able to intervene effectively. In addition to security issues, efficiency issues also deserve attention. Most of the existing attribute encryption schemes are based on bilinear pairing, but bilinear pairing has been criticized for its high cost. With the increase of data volume and attributes, the performance of the scheme based on bilinear pairing will inevitably decline. In addition, with the development of quantum computing technology, the security of schemes based on traditional number theory will also be threatened.

At present, cryptography has been widely used in data access control, such as digital signature [14, 15], secret sharing [16, 17], ABE [18], access control encryption (ACE) [19] and so on. The following briefly introduces some schemes combining cryptography and access control. The first attribute-based encryption scheme was proposed by Sahai and Waters on the basis of identity-based encryption at the Eurocrypt in 2005 [20]. CP-ABE is the data access

object determined by the data owner's policy, and compared with Key-policy attribute-based encryption (KP-ABE), CP-ABE has a broader application prospect in data access control. In 2010, Yu et al. proposed a secure, scalable and fine-grained data access control scheme in cloud environment based on ABE and proxy re-encryption [21]. In 2015, Zhou et al. proposed a multi-agency attribute-based encryption scheme with white-box traceable and revocable properties [22], which realized multi-level privacy protection in the electronic medical cloud computing system. In 2017, Yang et al. embedded the hierarchical attribute hierarchy dominance relationship into the ABE [23], realizing the Hierarchical Authorization feature of access control and storage data isolation, but the system has high complexity. In 2019, Li and Sato proposed a blockchain access control scheme based on MACP-ABE [24], and data users can combine secret keys from different sources to match ciphertext policies. In 2019, Wu et al. proposed an efficient traceable key scheme in blockchain to solve the problem of key abuse [25], so that the blockchain has publicly verifiable traceability to the key. The signature attribute of the user and the master key of the authorization centre are embedded into the user's key through CP-ABE. In 2021, Yu and Ma designed a model of Attribute and Trust-Based RBAC [26]. On the basis of RBAC, attribute/trust management module is added to grant users a set of attribute sets and embed access structure for roles. In 2021, Zhang and Yu proposed a blockchain data sharing model based on ABE [27], focusing on privacy protection and data security in the current blockchain data sharing mechanism.

In 2016, as a new cryptographic primitive, access control encryption was first proposed by Damgård et al. [19]. Different from other access control schemes, ACE focuses on the sending authority of the data owner, considers the security of the whole access process from another perspective, and expands the security research of access control schemes. In 2017, Kim and Yu proposed the first ACE scheme for arbitrary policies from standard assumptions [28], and they concluded by introducing several extensions to the ACE framework to support dynamic and more fine-grained access control policies. In 2020, Wang et al. constructed a basic ACE scheme based on DBDH assumption to achieve information flow control in Internet of Energy [29], and this scheme can control not only what users can read but also what they can write.

1.1. Security and Function Requirements. A complete access control system should provide corresponding functions and security services to ensure data sharing among entities. In some units and places with high security requirements, stricter measures should be taken to ensure the high security of information.

1.1.1. Fine-Grained Access Control. It should ensure fine-grained access control between user entities in the system. Users can freely decide who can access the data they own, and can also access the data shared by other users as needed.

1.1.2. Data Security and User Privacy Protection. The system should provide strong security protection for the data shared by users, and no one can get any valid information from the data except the users who can access the data specified by the data owner. Users' privacy should be protected. Except for trusted entities, other entities cannot obtain users' personal information during data sharing and access.

1.1.3. Supervision and Mandatory Control. When corrupt users are found in the system, the system should be able to deal with this situation in a timely manner. At the same time, for units with high security requirements, in order to ensure the security of information, the system should have a set of controls that override the user access policies to eliminate the harmful data sharing behaviour of the unit.

1.1.4. Tailored Forensics. The system shall provide certain evidence collection mechanism to ensure that the transaction has certain integrity and traceability. This is also to ensure that the data can be monitored during the sharing process, prevent controversial situations, and play a positive role in protecting specific units.

1.2. Contribution. Based on the idea of access control encryption, the security of sending authority of the data owner in attribute-based encryption is concerned, and an access control scheme based on blockchain is designed. The main contributions of this paper are listed as follows.

- (1) On the basis of the data owner's free decision on the access object, the system supervision function is added. While controlling the user's right to receive data, it can also provide restrictions on its sending permission, to prevent malicious users in the system from illegal data sharing through the public channel.
- (2) Based on blockchain, the traceability of the access process is realized, and the access records cannot be tampered with. At the same time, off-chain storage is adopted to reduce the storage burden on the chain and improve the efficiency of the system.
- (3) The scheme is constructed based on the learning with error over the ring (RLWE) on lattice and has the characteristics of anti-quantum attack. Compared with the scheme constructed by the learning with error (LWE), the ciphertext size and key size are shorter and the efficiency is higher.

1.3. Paper Structure. The remainder of this paper is organized as follows. In Section 2, we review some mathematical knowledge. In Section 3, we give the system model and security model, definition of scheme and construction. The scheme is analysed in Section 4, mainly including security analysis, performance analysis and experimental analysis. Finally, we conclude our paper in Section 5.

2. Preliminaries

2.1. Lattice

Definition 1 (Lattice). Λ is called lattice if there are m linearly independent n -dimensional vectors in Λ , such that any vector in Λ is an integer linear combination of $B = \{b_1, b_2, \dots, b_m\}$, that is $\Lambda = \Lambda(b_1, b_2, \dots, b_m) = \{\sum_{i=1}^m s_i b_i, \quad s_i \in \mathbb{Z}\}$, n is the dimension of lattice Λ , m is the rank of lattice Λ , and B is a set of bases of lattice Λ .

Definition 2 (Ideal Lattice). There is a ring $R = [x]/\langle f \rangle$ and an ideal $I \subseteq R$, A lattice $\Lambda \in \mathbb{Z}^n$ is an ideal lattice if Λ is associated with I .

Definition 3 (Decision $RLWE_{d,q,\chi}$ Problem [30]). Given the security parameter λ , select the integer d, q based on λ , let $R = \mathbb{Z}[x]/f(x)$, where $f(x) = x^d + 1$ and $R_q = R/q$. Given discrete distribution $\chi \subset R_q$ based on λ , there is an unspecified challenge model O in the Decision $RLWE_{d,q,\chi}$ Problem, that is to determine whether the challenge model is a noisy pseudo-random sampler O_s or a real random sampler O'_s for random secret key, $K \in R_q$, which perform respectively as follows:

O_s : outputs $(\omega, \nu) = (\omega, \omega K + e) \in R_q \times R_q$. The element ω is uniformly random from R_q , where $\omega \leftarrow R_q$ and the $K \leftarrow R_q$ fixed for all samples. The element $e \leftarrow R_q$ is a small error term that generated with a distribution χ .

O'_s : outputs truly random samples $(\omega, \nu) \in R_q \times R_q$.

2.2. Access Control Structure

Definition 4 (Monotone Access Structure). Let $U = \{u_1, u_2, \dots, u_n\}$ be a set of attributes. A collection $D \subseteq U$ is monotone if $\forall B, \quad C: B \in D, \quad B \subseteq C \Rightarrow C \in D$. The sets in A are called as authorized sets, and the sets not in D are called as unauthorized sets.

Definition 5 (Linear Secret Sharing Scheme (LSSS) [31]). The Π is a secret sharing scheme over a set of attributes U if the following properties are met:

- (1) All sharers have a secret sharing vector based on R_q ;
- (2) There is a share-generating matrix $F \in R_q^{n \times m}$ for Π , with row labels $\rho(i) \in U, \quad \forall i \in [n]$. Given a column vector, $\vec{v} = (s, r_2, \dots, r_m)$, where $s \in R_q$ is the secret to be shared and $r_2, \dots, r_m \leftarrow R_q$ are randomly chosen. Let $\delta_i = F_i \times \nu \in R_q, \quad i \in (1, n)$ represent attribute $\rho(i)$, where $\rho(i)$ is a function from i to U .

Linear secret sharing scheme has linear reconstruction characteristics. Suppose that Π is an LSSS that represents the access structure A . Let $A \in A$ be an authorized set, and $I \subset \{1, \dots, n\}, \quad I = \{i: \rho(i) \in D\}$. There exist constants $\{\omega_i \in R_q\}_{i \in I}$ then $\sum_{i \in I} \delta_i \omega_i = s$ such that of δ_i are valid shares of a secret s according to Π . Furthermore, these constants ω_i can be calculated through the share-generating matrix F in polynomial time. For unauthorized sets, it cannot be

calculated, that is, any information of secret sharing value cannot be obtained.

3. Supervised Access Control Scheme Based on Attribute-Based Encryption and Blockchain

3.1. System Model. The proposed system includes six entities: Authority, Data Owner (DO), Inter-Planetary File System (IPFS), Sanitizer, Data User (DU) and Blockchain. The relationship among the entities is shown in Figure 1.

- (1) *Authority.* The authority generates the system's public parameters PP and master private key MSK , manages the users in the system, and constructs the secret key for each user according to the user's identity and authority, then the authority generates a sanitizer key sk according to the system control policy when accessing data. We assume that authority is completely trusted, it always correctly implements the requirements put forward by all entities in the scheme, and will not disclose any information or attempt to obtain user information. Generally speaking, the authority of the system, as a separate trusted entity, can also be deployed separately in this scheme. However, in combination with the characteristics of the private chain, in order to facilitate data processing, it is expanded and deployed on the nodes of the blockchain.
- (2) *Data Owner (DO).* The data owner generates ciphertext tag based on data and encrypts data with a symmetric key k , then uploads encrypted data into the Inter-Planetary File System (IPFS). After that, DO sets the access policy of the data, and encrypts the symmetric key and address, then DO uploads this ciphertext CT and tag S_c to blockchain.
- (3) *Inter-Planetary File System (IPFS).* The IPFS is responsible for storing data and returning an address. IPFS is honest but curious, always correctly implement the requirements put forward by all entities in the scheme, but attempts to decrypt the ciphertext content.
- (4) *Sanitizer.* The sanitizer encrypts the ciphertext CT according to the sanitizer key sk . For sanitizer, it is equivalent to re encrypting the ciphertext. Its input and output are in the form of ciphertext without much effective information. Therefore, it is implemented in the form of smart contract. The sanitizer is honest but curious, always correctly implement the requirements put forward by all entities in the scheme, but attempts to decrypt the ciphertext content.
- (5) *Data User (DU).* The data user can access data according to their needs after registration. Generally, when the user's identity is normal, his access right to certain data is determined by the data owner, but the system has the ability to change the user's access right when the system suspects that the communication is abnormal.

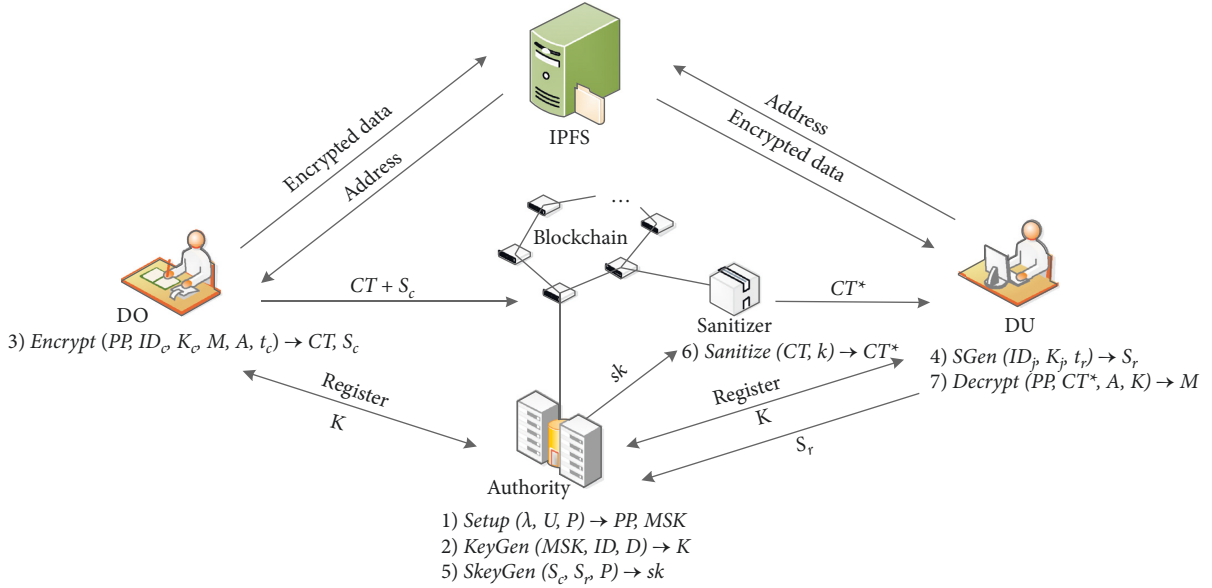


FIGURE 1: System model.

(6) *Blockchain*. The blockchain is used to store CT and tag S_c . Records of key distribution and data access can be formed into transactions and recorded on the blockchain. Since this scheme provides a powerful system supervision for a small range of organizations and institutions, the private chain technology is mainly used here to strengthen the system supervision through certain control, and provide faster response and tamper proof recording services.

3.2. Overview of the SACS-ABE ϕ B Scheme. The priority in the system is, user identity permission > system control policy > user access policy. The user identity permission is granted by the system according to user registration information. System control policies are generated by the system as needed and can be adjusted in time. User access policies are generated by the data owner.

When a user registers, the authority generates a unique ID for each user. In order to protect the privacy and security of users, only the user and the authority can obtain the ID. The identity permission of each user is $ui \in \{0, 1\}$, 0 means that the user is illegal and does not have any read and write permissions; 1 means that the user is normal, which means that data can be read or write. The default permission of the user is 1. System control policy refers to a representation of whether users can communicate with each other. An access control matrix can be set to determine whether users can communicate through the values in the matrix, where the value 1 indicates that communication is allowed and the value 0 indicates that communication is rejected. For example, in the example given in Table 1, we can know that the system prohibits communication between $u1$ and $u3$ through the matrix.

TABLE 1: Example of access control matrix.

| | $u1$ | $u2$ | $u3$ | \dots | ui |
|----------|----------|----------|----------|---------|----------|
| $u1$ | 1 | 1 | 0 | \dots | 1 |
| $u2$ | 1 | 1 | 1 | \dots | 1 |
| $u3$ | 0 | 1 | 1 | \dots | 1 |
| \vdots | \vdots | \vdots | \vdots | \dots | \vdots |
| ui | 1 | 1 | 1 | \dots | 1 |

When the user needs to share data, the DO first generates a ciphertext tag. The ciphertext tag is the unique identification symbol generated by the timestamp and the user's ID encrypted. The timestamp is to ensure that the identification generated after each encryption is different, to prevent the enemy from obtaining the user's privacy information by analysing the identification. In the second step, the DO needs to encrypt the data with a symmetric key, send it to IPFS and return an address, then encrypt the symmetric key and address according to access policy, and send the ciphertext and tag to the blockchain.

DU first obtains the ciphertext tag of the data and sends an access request to the blockchain when accessing data. The access request includes the ciphertext tag and access tag. The access tag is also encrypted by the timestamp and the user's ID. After receiving the request, the authority obtains the ID of both the DO and the DU through decryption tags, then judges whether they meet the system control policy, then generates sanitizer key sk and send it to sanitizer. Sanitizer uses the sk to encrypt the ciphertext, and then forwards the re-encrypted ciphertext to the DU. Finally, the DU decrypts the ciphertext according to his key. If both parties meet the requirements of identity permission, system control policy and user access policy, the DU can successfully obtain the data.

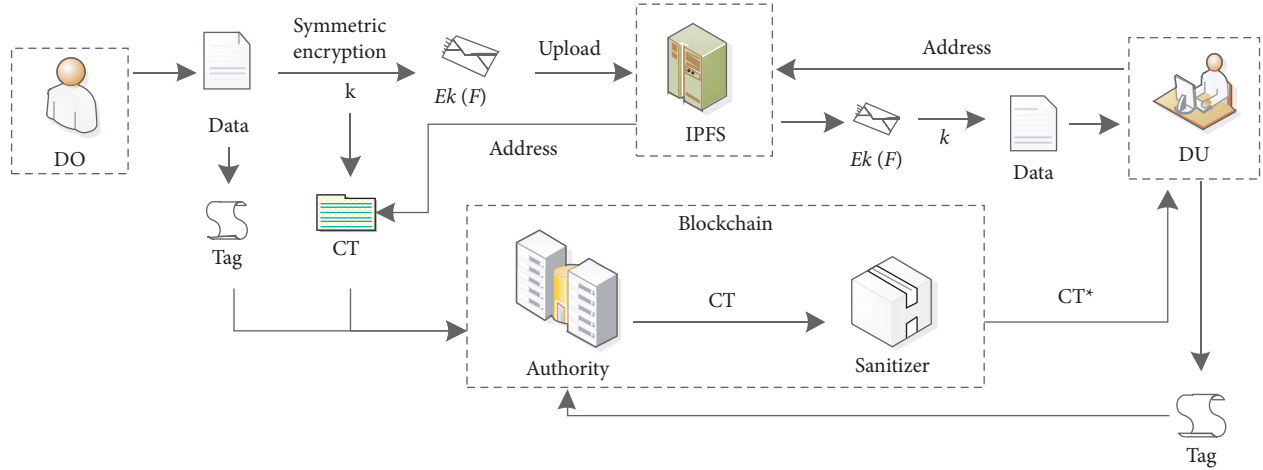


FIGURE 2: Access flow chart.

The process is shown in Figure 2.

The scheme consists of the following eight algorithms.

$\text{Setup}(\lambda, U) \rightarrow PP, MSK$. The algorithm is executed by authority. Given the security parameter λ , and the collection of all attributes U in the system, This algorithm outputs public parameters PP and master secret key MSK .

$\text{KeyGen}(MSK, D, ID) \rightarrow K$. The algorithm is executed by authority. Input master secret key MSK , user's attribute set D . This algorithm outputs the secret key K for the user.

$\text{SymEnc}(DT, k) \rightarrow ED$. The algorithm is executed by DO. The DO randomly generates a symmetric key k and encrypts the data DT with this key to obtain the ciphertext ED , then upload the ciphertext ED to IPFS and return an address T , let $M = T||k$.

$\text{Enc}(PP, ID_c, K_c, M, A, t_c) \rightarrow CT, S_c$. The algorithm is executed by DO. Input public parameters PP , master key MSK , user's secret key K_c , the message M about $T||k$, user's access policy A and timestamp t_c . This algorithm outputs the ciphertext CT and tag S_c .

$\text{SGen}(ID_r, K_r, t_r) \rightarrow S_r$. The algorithm is executed by DU. Input public parameters PP , user's ID_r and timestamp t_c . This algorithm outputs the access tag S_r .

$\text{SkeyGen}(S_c, S_r, P) \rightarrow sk$. The algorithm is executed by authority. Input ciphertext tag S_c , access tag S_r and system control policy P . This algorithm outputs the sanitizer key sk .

$\text{San}(CT, sk) \rightarrow CT^*$. The algorithm is executed by sanitizer. Input ciphertext CT and sanitizer key sk . This algorithm outputs the ciphertext CT^* .

$\text{Dec}(PP, CT^*, K) \rightarrow M$. The algorithm is executed by DU. Input public parameters PP , ciphertext CT^* , user's secret key K . This algorithm outputs $M = T||k$, then the DU can download the data through the address T and decrypt it with the key sk to obtain DT .

3.3. Security Model. We define three security models: No-Read Rule, No-Write Rule and Chosen-plaintext attack Security. No-Read Rule means that DU cannot obtain any valid data without the permission of system control policy. No-Write Rule means that the DO cannot send any valid data without the permission of the system control policy. $P(ui, uj) = 1$ indicates that

communication between the data owner ui and the data user uj is allowed, and $P(ui, uj) = 0$ indicates that communication between the data owner ui and the data user uj is prohibited. Three models are defined as follows.

Definition 6. (Correctness [32]). Given attribute universe U and all message $M \in M$, for all $(i, j) \in [n] \times [n]$ such that $P(ui, uj) = 1$ and D satisfied with A :

$$\Pr[\text{Dec}(PP, \text{San}(\text{Enc}(M), sk), K) \neq M] \leq \text{negl}(\lambda), \quad (1)$$

where $\text{Setup}(\lambda, U) \rightarrow PP, MSK$, $\text{KeyGen}(MSK, D, ID) \rightarrow K$, $\text{SkeyGen}(S_c, S_r, P) \rightarrow sk$.

Correctness captures the feature that DO with K_c can deliver a message to DU for which DU's attribute set D satisfied with DO's policy A and $P(DO, DU) = 1$. In this case, the sanitizer should pass the message to DU smoothly, and DU should be able to decrypt CT^* by K .

Definition 7. (No-Read Rule [32]). Consider the following game between a challenger and an adversary over the attribute universe U , message space M , and it is assumed that for a challenge access structure A^* , the adversary cannot request the key that meets A^* . The game is as shown in Table 2.

If \mathcal{A} wins the game, it must meet $b = b'$, $|M_0| = |M_1|$, $u_0, u_1 \in \{0, 1\}$, and comply with Payload Privacy or Sender Anonymity.

Payload Privacy. For all queries q to O_G about uj , it holds that $P(u_0, uj) = P(u_1, uj) = 0$.

Sender Anonymity. For all queries q to O_G about uj , it holds that $P(u_0, uj) = P(u_1, uj)$ and $M_0 = M_1$.

The formal definition of No-Read Rule is $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\mathcal{A} \text{ win the No-Read game}] - 1/2| \leq \text{negl}(\lambda)$.

That is the probability of \mathcal{A} winning the No-Read game is negligible, which ensures that when DO sends the message, the probability of successfully decrypting the message for all users with $P(ui, uj) = 0$ or $uj = 0$ is negligible. Only the intended recipients who meet the conditions can obtain valid information (Payload Privacy) and no one can learn about the identity of DO (Sender Anonymity).

TABLE 2: No-read rule.

| No-read rule | Oracle definition |
|--|--|
| Game definition | |
| 1.Setup(λ, U) $\longrightarrow PP, MSK$ | $O_G(uj)$: |
| 2. $\mathcal{A}^{O_G(\cdot), O_S(\cdot)}(PP) \longrightarrow (M_0, M_1, u0, u1)$ | KeyGen(MSK, D, ID) $\longrightarrow K$ |
| 3. $\{0, 1\} \longrightarrow$ | $O_E(ui, M)$: |
| 4.Enc(PP, K_{ui_b}, M_b, A^*) $\longrightarrow CT$ | KeyGen(MSK, D, ID) $\longrightarrow K$ |
| 5. $\mathcal{A}^{O_G(\cdot), O_E(\cdot)}(CT) \longrightarrow b'$ | KeyGen(MSK, D, ID) $\longrightarrow K$ |

TABLE 3: No-write rule.

| No-write rule | Oracle definition |
|---|--|
| Game definition | |
| 1.Setup(λ, U) $\longrightarrow PP, MSK$ | $O_S(uj)$: |
| 2. $\mathcal{A}^{O_E(\cdot), O_S(\cdot)}(PP) \longrightarrow (CT, ui')$ | KeyGen(MSK, D, ID) $\longrightarrow K$ |
| 3.KeyGen(MSK, ID, D) $\longrightarrow K_{ui'}$ | SkeyGen(S_c, S_r, P) $\longrightarrow sk$ |
| 4.SkeyGen(S_c, S_r, P) $\longrightarrow sk$ | $O_R(uj)$: |
| 5. $M \longrightarrow rM$ | KeyGen(MSK, D, ID) $\longrightarrow K$ |
| § | |
| 6. $\{0, 1\} \longrightarrow$ | |
| -if $b = 0$ | SkeyGen(S_c, S_r, P) $\longrightarrow sk$ |
| San(CT, sk) $\longrightarrow CT^*$ | $O_E(ui, M)$: |
| -if $b = 1$ | |
| San(Enc($PP, K_{ui'}, rM, A^*$), sk) $\longrightarrow CT^*$ | KeyGen(MSK, D, ID) $\longrightarrow K_{ui}$ |
| 7. $\mathcal{A}^{O_E(\cdot), O_R(\cdot)}(CT^*) \longrightarrow b'$ | Enc(PP, K_{ui}, M, A^*) $\longrightarrow CT$ |
| | San(CT, sk) $\longrightarrow CT^*$ |

Definition 8. (No-Write Rule [32]). Consider the following game between a challenger and an adversary over the attribute universe U , message space M , and it is assumed that for a challenge access structure A^* , the adversary cannot request the key that meets A^* . The game is as shown in Table 3.

Let I_S be the set of identify about all queries for key. \mathcal{A} wins the game if $ui' \in I_S \cup \{0\}$ and $P(ui, uj) = 0, \forall ui, uj \in I_S$ when $b = b'$. The formal definition of No-Write Rule is $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\mathcal{A} \text{ win the No - Write game}] - 1/2| \leq \text{negl}(\lambda)$.

That is, the probability of the \mathcal{A} winning the No-Write game is negligible, which ensures that the probability of successfully information exchange with other users is negligible when $P(ui, uj) = 0$ or $uj = 0$. There are two other explanations about No-Write Rule as follows.

Note 1. The target ciphertext CT in (CT, ui') is obtained only in two cases, one is generated by legal encryption key queried, and the other is chosen uniformly from ciphertext space.

Note 2. The sanitizer should be honest, and it is required that the adversary does not corrupt the sanitizer as an unavoidable condition.

Definition 9 (Chosen-plaintext attack Security [33]). The definition is given by describing the game between adversary \mathcal{A} and simulator \mathcal{B} . The scheme satisfies the security of chosen-plaintext attack if all polynomial algorithm

adversaries' advantage is negligible in the game. The specific process of the game is as follows.

Initialization. The adversary \mathcal{A} selects an access structure A^* and sends it to \mathcal{B} .

Setup. The simulator \mathcal{B} generates public parameters PP and master keys MSK and sends them to \mathcal{A} .

Inquiry Phase 1. The adversary \mathcal{A} asks the simulator \mathcal{B} for the secret key, but \mathcal{A} 's attribute set does not meet the access structure. The simulator runs the *KeyGen* algorithm to generate the secret key and send it to \mathcal{A} .

Challenge. The adversary \mathcal{A} chooses two messages $M_0, M_1 \in \{0, 1\}$ and send them to simulator \mathcal{B} , then \mathcal{B} randomly select $b \in \{0, 1\}$ to calculate the challenge ciphertext and send it to \mathcal{A} .

Inquiry Phase 2. \mathcal{A} asks for the key as in phase 1.

Guess. Adversary \mathcal{A} outputs his guess b' about b . The advantage of \mathcal{A} in this game is defined as $\text{adv}^{\mathcal{A}} = \Pr[b' = b] - 1/2$.

3.4. Construction of the SACS-ABE&B Scheme. Setup(λ, U) $\longrightarrow PP, MSK$. Given the security parameter λ , and the collection of all attributes U in the system, randomly select a large prime number $q = 1 \text{ mod } (2\lambda)$ and a small positive integer p , where $p \ll q$ and $\text{gcd}(p, q) = 1$. Let

$f(x) = (x^d + 1)$, where d is a power of 2. Let $R_q = Z_q[x]/\langle f(x) \rangle$ be the ring of integer polynomials modulo both $f(x)$ and q . Let $\chi = \chi(\lambda)$ be an error distribution over R_q . Select a uniformly random $SK_0 \leftarrow R_q$ and random element $a \leftarrow R_q$, then choose a small noise term $e_0 \leftarrow \chi$. Compute $PK_0 = aSK_0 + pe_0 \in R_q$. Next, select a pair of uniformly random $(SK_i, SK_i^{-1}) \leftarrow R_q$ for each attribute in U , where SK_i^{-1} is the inverse of SK_i in R_q , and select a small noise term $e_i \leftarrow \chi$, then compute $PK_i = SK_i + pe_i \in R_q$. Lastly, outputs the public parameters $PP = \{a, PK_0, \{PK_i\}_{i=1}^n\}$ and the master secret key $MSK = \{SK_0, \{SK_i\}_{i=1}^n, \{SK_i^{-1}\}_{i=1}^n\}$.

$KeyGen(MSK, D, ID) \rightarrow K$. Input master key MSK , user's attribute set D , then choose a small noise term $e'' \leftarrow \chi$, select a pair of uniformly random $(t_i, t_i^{-1}) \leftarrow R_q$ and choose small noise term $e_i \leftarrow \chi$ for each attribute in D . Compute $K_0 = SK_0 t^{-1} + pe'' \in R_q$, $K_i = SK_i^{-1} t + pe_i'' \in R_q$, $\forall i \in D$, outputs the secret key $K = (K_0, K_i)$. If the user's identity permission is 0, $K_0' \leftarrow R_q$, $K_i' \leftarrow R_q$, $\forall i \in D$ outputs the secret key $K = (K_0', K_i')$.

$SymEnc(DT, k) \rightarrow ED$. Input the DO's data DT and symmetric key k , output the ciphertext data ED , then upload the ciphertext ED to IPFS and return an address T , let $M = T \parallel k$.

$Enc(PP, ID_c, K_c, M, A, t_c) \rightarrow CT, S_c$. Input public parameters PP , user's ID_c , the secret key K_c , the message M about $T \parallel k$, user's access policy A and timestamp t_c . Set access policy $A = (F, \rho)$, $F \in R_q^{n \times m}$ with row labels $\rho(j) \in H$, $\forall j \in [n]$, $H \in A$. Generate a vector $v = (s, r_2, \dots, r_m)$, where $r_2, \dots, r_m \leftarrow R_q$ and $s \in R_q$ is the secret to be shared. $\delta_j = F_j \times v \in R_q$ where F_j is the vector corresponding to j th row

of F , then choose a uniformly random element $r \leftarrow R_q$, and noise terms $e', e_j' \leftarrow \chi$, Compute $C_0 = PK_0 r s + M + pe' \in R_q$, $C_j = arPK_j \delta_j + p_j' \in R_q$, $S_c = K_{c0} + ID_c \parallel t_c$, output $CT = (C_0, C_j)$ and S_c .

$SGen(ID_r, K_r, t_r) \rightarrow S_r$. Input user's ID_r , the secret key $K_r = (K_{r0}, K_{ri})$ and timestamp t_c , then compute $S_r = K_{r0} + ID_r \parallel t_r$.

$KeyGen(S_c, S_r, P) \rightarrow sk$. Input ciphertext tag S_c , access tag S_r and system control policy P , compute $ID_c \parallel t_c = S_c - K_{c0}$ and $ID_r \parallel t_r = S_r - K_{r0}$, then judge whether ID_c and ID_r meet the communication requirements according to the system control policy P . If the identities of both parties are legal and meet the requirements of access control policy, then let $sk' = 1$, otherwise select a uniformly random $sk' \leftarrow R_q$, output the sanitizer key $sk = sk'$.

$San(CT, sk) \rightarrow CT^*$. Input ciphertext CT and sanitizer key sk , compute $C_0' = sk C_0 \in R_q$, $C_j' = C_j \in R_q$, output $CT^* = (C_0', C_j')$.

$Dec(PP, CT^*, K) \rightarrow M$. Input public parameters PP , ciphertext CT^* , user's secret key K . If the DU meets the access control policy P , the ciphertext CT^* is equivalent to the original ciphertext CT , as long as the DU's attribute meets the access structure A , $I \subset \{1, \dots, n\}$, $I = \{i: \rho(i) \in A\}$, compute a set of constants $\{\omega_i \in R_q\}_{i \in I}$ with a linear reconstruction algorithm of LSSS, then $\sum_{i \in I} \delta_i \omega_i = s$, compute $M' = C_0' - K_0 \sum_{i \in I} C_i \omega_i K_i$, $M = M' \bmod p$, the DU can download the data through the address T and decrypt it with the key sk to obtain DT .

The correctness of the successful decryption of the scheme is explained as follows.

$$\begin{aligned}
M' &= C_0' - K_0 \sum_{i \in I} C_i \omega_i K_i \\
&= 1 \cdot C_0 - K_0 \sum_{i \in I} (aPK_i r \delta_i + pe_i') \omega_i K_i \\
&= C_0 - K_0 \sum_{i \in I} (aPK_i r s K_i) - p \cdot K_0 \sum_{i \in I} (e_i' \omega_i K_i) \\
&= C_0 - K_0 \sum_{i \in I} ar s (SK_i + pe_i) (SK_i^{-1} t + pe_j'') - p \cdot K_0 \sum_{i \in I} (e_i' \omega_i K_i) \\
&= M + PK_0 r s + pe' - (SK_0 t^{-1} + pe'') ar s t - p ar s K_0 \sum_{i \in I} (SK_i e_i'' + e_i SK_i^{-1} + e_i pe_i'') - p \cdot K_0 \sum_{i \in I} (e_i' \omega_i K_i) \\
&= M + pe_0 r s + pe' - pe'' tars - p ar s K_0 \sum_{i \in I} (SK_i \cdot e_i'' + e_i \cdot SK_i^{-1} + e_i \cdot p \cdot e_i'') - p \cdot K_0 \sum_{i \in I} (e_i' \cdot \omega_i \cdot K_i).
\end{aligned} \tag{2}$$

Then $M = M' \bmod p$, and in order to ensure the correctness of the scheme, the noise term in the scheme must meet be small enough compared to the ratio of q to p .

4. Analysis

4.1. Security Analysis

4.1.1. Security Assumptions

The underlying data of the blockchain and the data on the IPFS are secure, and there will be no leakage or physical attack.

All underlying crypto primitives used are secure, including symmetric encryption, public key encryption and other encryption operations.

All relevant keys that are externally managed have not been compromised.

It should be noted that legitimate users, illegal users and external attackers are allowed to collude to attack, and it is assumed that all algorithms can calculate accurately and there are no attack and destruction of physical conditions.

The adversary has polynomially bounded computer resources.

4.1.2. Security Proof. This section examines the security of the SACS-ABE&B scheme through three theorems. Before proving, it should be noted that these three theorems prove the different properties of the scheme through the indistinguishability of the ciphertext, and there is no strict progressive relationship between them. Theorems 1 and 2 mainly prove the no read and no write rules, and Theorem 3 mainly proves the part of attribute-based encryption in the scheme. Assuming that in all games, the answers to all legitimate queries are correct.

Theorem 1. *If there is no a Probabilistic Polynomial Time (PPT) algorithm adversary \mathcal{A} can win the game in Definition 7, the SACS-ABE&B scheme satisfies the No-Read Rule.*

Proof. According to the Definition 7, the Payload Privacy and Sender Anonymity of the scheme are proved as follows.

Payload Privacy. According to the definition, access control policy $P(ui_0, u_j) = P(ui_1, u_j) = 0$ must be met for u_j who query the decryption key to O_G . According to the identity permission of the ui_0 and the ui_1 , three situations are discussed below.

- (a) $ui_0 = ui_1 = 0$, that means ui_0 and ui_1 have no right to read and write, their secret key $K \leftarrow R_q$ is randomly generated in $\text{Enc}(PP, K, M, A) \rightarrow CT$, and CT is randomly generated and independent of M_b , where $b = 0$ or $b = 1$. So \mathcal{A} has no special advantage to distinguish M_b , then $\Pr[\mathcal{A} \text{ win the No-Read game}] = \Pr[b = b']$, we can conclude $\text{adv}^{\mathcal{A}} =$

$$2 \cdot |\Pr[\mathcal{A} \text{ win the No - Read game}] - 1/2| = 2 \cdot |\Pr[b = b'] - 1/2| \leq \text{negl}(\lambda).$$

- (b) $ui_0 = ui_1 = 1$, that means ui_0 and ui_1 are legal and they can obtain valid secret key K , the CT are indistinguishable because of the difficulty of the decision $RLWE_{d,q,\chi}$ problem (Theorem 3), we attain $\text{adv}^{\mathcal{A}} = \varepsilon/2 \leq \text{negl}(\lambda)$.
- (c) $ui_0 = 0, ui_1 = 1$ or $ui_0 = 1, ui_1 = 0$. When $ui_0 = 0, ui_1 = 1, ui_1$ can get valid secret key K , and compute normal CT , and $C_0, C_j \in R_q$ are uniformly distributed in the ciphertext space in the CT ; ui_0 cannot get K , his CT is randomly generated in the ciphertext space. It can be seen from case b) that the two CT are indistinguishable, then $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\mathcal{A} \text{ win the No - Read game}] - 1/2| = 2 \cdot |\Pr[b = b'] - 1/2| \leq \text{negl}(\lambda)$. When $ui_0 = 1, ui_1 = 0$, the situation is consistent with $ui_0 = 0, ui_1 = 1$.

Sender Anonymity. According to the definition, access control policy $P(ui_0, u_j) = P(ui_1, u_j)$ and $M_0 = M_1$ must be met for all users u_j who query the decryption key to O_G . According to the identity permission of the ui_0 and the ui_1 , three situations are discussed below.

- (a) $ui_0 = ui_1 = 0$. This case is same as a) in Payload Privacy. So $\text{adv}^{\mathcal{A}} \leq \text{negl}(\lambda)$.
- (b) $ui_0 = ui_1 = 1$. If $u_j = 1$ and $P(ui_0, u_j) = P(ui_1, u_j) = 1$, \mathcal{A} can decrypt the challenge ciphertexts. However, the encryption key and the message in the challenge ciphertexts are completely identical. So $\text{Enc}(PP, K_c, M_b, A) \rightarrow CT$ for $b = 0$ or $b = 1$ are identical, obviously $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\text{win the No - Read game}] - 1/2| \leq \text{negl}(\lambda)$.
- (c) $ui_0 = 0, ui_1 = 1$ or $ui_0 = 1, ui_1 = 0$. This case is same as c) in Payload Privacy. So $\text{adv}^{\mathcal{A}} \leq \text{negl}(\lambda)$.

Now we complete the proof of Theorem 1. \square

Theorem 2. *If there is no a PPT algorithm adversary \mathcal{A} can win the game in Definition 8, the SACS-ABE&B scheme satisfies the No-Write Rule.*

Proof. According to the Definition 8, the identities of the sender are just 0 or 1, so $I_S = \emptyset$ or $I_S = \{1\}$ in the secret key query before giving the attack target. That is, the sender's secret key is queried or the sender's secret key is not queried, two situations are discussed below.

- (a) $I_S = \{1\}$. Because $ui' \in I_S \cup \{0\}$ in definition, so $ui' \in (0, 1)$ and $P(ui, u_j) = 0, \forall ui, u_j \in I_S$. Because $P(ui, u_j) = 0, sk \leftarrow R_q$ are randomly selected. When $b = 0, \text{San}(CT, sk) \rightarrow CT^*$ and CT is the originally specified plaintext encrypted by the encryption algorithm $\text{Enc}(PP, K_c, M, A) \rightarrow CT$; When $b = 1, \text{San}(\text{Enc}(PP, K_c, rM, A), sk) \rightarrow CT^*$ and rM is a random plaintext. Obviously, both of CT^* are all uniform distribution in R_q and all ciphertexts are indistinguishable. \mathcal{A} has no special advantage to

distinguish which situation, so $\Pr[\mathcal{A} \text{ win the No - Write game}] = \Pr[b = b']$, then $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\mathcal{A} \text{ win the No - Write game}] - 1/2| = 2 \cdot |\Pr[b = b'] - 1/2| \leq \text{negl}(\lambda)$.

- (b) $I_S = \emptyset$. We can get $ui' = 0$, so the adversary can query the key before or after generating the attack target according $P(ui, uj) = 0, \forall ui, uj \in I_S$. It is necessary to prove that even if the adversary has keys, it still cannot distinguish the challenge ciphertext. At this time, it is only necessary to prove that in this case, except for the negligible probability, the output and input of Sanitizer are independent. $C_0 = PK_0rs + M + pe' \in R_q$ is uniform distribution in R_q over Enc algorithm and $C'_0 = skC_0 \in R_q$ is uniform distribution in R_q over San algorithm, where $sk \leftarrow R_q$. In this case, the C_0 and C'_0 are independent. So, it still cannot distinguish the challenge ciphertext, then we can conclude that $\text{adv}^{\mathcal{A}} = 2 \cdot |\Pr[\mathcal{A} \text{ win the No - Write game}] - 1/2| = 2 \cdot |\Pr[b = b'] - 1/2| \leq \text{negl}(\lambda)$.

Now we complete the proof of Theorem 2. \square

Theorem 3. *If there exists a PPT algorithm adversary \mathcal{A} with the advantage ε to win the game in Definition 8, then there exists a PPT simulator \mathcal{B} can decide Decision $R - \text{LWE}_{d,q,\chi}$ Problem with advantage $\varepsilon/2$.*

Proof. The Decision $\text{RLWE}_{d,q,\chi}$ Problem is to determine whether the oracle O is a noisy pseudo-random O_s or a truly random O'_s , then the simulator \mathcal{B} differentiate O by adversary \mathcal{A} . First, \mathcal{B} queries the oracle and receives $(t+1)$ samples $(\omega_k, v_k) \in R_q \times R_q$, where $k \in \{0, 1, 2, \dots, t\}$, then proceed as follows.

Initialization Phase. Given a set of attributes U . The adversary \mathcal{A} selects an access structure A^* that wishes to be challenged and sends it to \mathcal{B} .

Setup. \mathcal{B} runs $\text{Setup}(\lambda, U) \rightarrow PP, MSK$, let $PK_0 = p\omega_0 \in R_q$, select a pair of uniformly random $(SK_i, SK_i^{-1}) \leftarrow R_q$ for each attribute in U . Let $PK_i = p\omega_i \in R_q$ if $i \in A^*$; otherwise, let $PK_i = SK_i + pe_i \in R_q$. Then \mathcal{B} send $PP = \{a, PK_0, \{PK_i\}_{i=1}^n\}$ to \mathcal{A} .

Inquiry Phase 1. \mathcal{A} sends secret key queries for $D^* = \{D_1^*, D_2^*, \dots, D_j^*\}$, where D^* does not meet the access policy A^* . \mathcal{B} runs $KeyGen$, computes $K_0 = SK_0t^{-1} + pe'' \in R_q$, $K_i = SK_i^{-1}t + pe''_i \in R_q$, $\forall i \in D^*$, and send $K = (K_0, K_i)$ to \mathcal{A} .

Challenge. \mathcal{A} chooses two messages $M_0, M_1 \in \{0, 1\}$ and send them to simulator \mathcal{B} , then \mathcal{B} randomly select $b \in \{0, 1\}$, if $b = 0$, \mathcal{B} randomly choose $x \leftarrow R_q$ and let $C_0 = px_0 \in R_q$, $C_j = px_j \in R_q$; if $b = 1$, let $C_0 = pv_0 + M \in R_q$, $C_j = pv_j \in R_q$ for $j \in A^*$.

Inquiry Phase 2. \mathcal{A} asks for the key as in phase 1.

Guess. Adversary \mathcal{A} outputs his guess b' about b to \mathcal{B} . If $b' = b$, output $O' = O_s$, otherwise, output $O' = O'_s$. The advantage of \mathcal{A} in this game is defined as $\text{adv}^{\mathcal{A}} = P[rb' = b] - 1/2$, so the oracle O is:

A noisy pseudo-random O_s : the advantage of \mathcal{A} is ε , then $|\Pr[b' = b | O = O_s] - 1/2| \leq \varepsilon$ and

$$\Pr[O' = O | O = O_s] = 1/2 + \varepsilon. \quad (3)$$

A truly random O'_s : \mathcal{A} has no advantage ε and unable to get information about b , then $|\Pr[b' \neq b | O = O'_s]| = 1/2$, $|\Pr[O' = O | O = O'_s]| = 1/2$.

Then the advantage of simulator \mathcal{B} is as follows.

$$\begin{aligned} \frac{1}{2} |\Pr[O' = O | O = O_s]| + \frac{1}{2} |\Pr[O' = O | O = O'_s]| - \frac{1}{2} \\ = \frac{1}{2} \left(\frac{1}{2} + \varepsilon \right) + \frac{1}{2} \left(\frac{1}{2} \right) - \frac{1}{2} \\ = \frac{\varepsilon}{2}. \end{aligned} \quad (4)$$

Now we complete the proof of Theorem 3. \square

4.1.3. Security and Privacy Evaluation

- (1) Fine-grained access control. The system implements fine-grained access control by CP-ABE. Within the scope allowed by the system policy, legitimate users in the system can formulate their own access policies to determine the users who can access data.
- (2) Data security. All data are encrypted before uploading to the cyberspace. The data stored in IPFS is symmetrically encrypted. Even if it is stolen, it will not cause the leakage of effective information. The symmetric key is encrypted through CP-ABE. The security of the encryption scheme is also proved in the previous section.
- (3) Privacy protection. In addition to trusted entities, users will not expose personally identifiable information or get other users' personally identifiable information during access.
- (4) Supervision and mandatory control. The system ensures that the data will strictly comply with the access policy formulated by the system through the sanitizer before sharing, and can effectively prevent the communication between corrupt users. Even after the data is uploaded, it can also play an immediate control. Such behaviour can strictly prevent any data sharing that violates the system control policy.
- (5) Tailored forensics. The system saves the user's access process on the private chain in the form of transactions through the private chain, and uses the tamper proof nature of the blockchain to realize the

TABLE 4: Comparison with other attribute-based encryption schemes.

| Scheme | Access structure | Problem | Secret key size | Ciphertext size | Encryption byte |
|--------|------------------|---------|------------------------|-------------------------------|-----------------|
| [34] | AND | LWE | $2m_1A_u\log q$ | $(2m_1A_c + 1)\log q$ | 1 |
| [35] | Shamir | RLWE | $(nA_u + n)\log q$ | $(nA_c + 1)\log q$ | n |
| [36] | LSSS | RLWE | $(1 + n\eta)A_u\log q$ | $n\eta + (1 + m_2n)A_c\log q$ | n |
| Our | LSSS | RLWE | $(nA_u + n)\log q$ | $(nA_c + 1)\log q$ | n |

TABLE 5: Comparison with other access control schemes on blockchain.

| Scheme | Confidentiality | Fine-grained access control | Privacy protection | Off chain storage | Anti- quantum attack | System control |
|--------|-----------------|-----------------------------|--------------------|-------------------|----------------------|----------------|
| [37] | √ | √ | √ | × | × | × |
| [38] | √ | √ | √ | √ | × | × |
| [39] | √ | √ | √ | √ | × | × |
| [40] | √ | √ | √ | √ | × | × |
| [41] | √ | √ | √ | × | × | × |
| Our | √ | √ | √ | √ | √ | √ |

traceability of the process, so as to facilitate the evidence collection in case of disputes in the future.

4.2. Performance Analysis. The core of this scheme is constructed based on the ciphertext policy attribute-based encryption, which will be analysed first. Some ciphertext policy attribute-based encryption schemes on lattice are selected and compared from the aspects of access structure, problem, user secret key size, ciphertext size and encryption byte. Let A_c is the number of attributes in ciphertext, and A_u is the number of user's attribute. m_1, m_2 and n are the parameters from lattice, η means the columns of matrix in scheme. The comparison is listed in Table 4.

It adopts threshold access structure in scheme [34], which is not flexible enough, and the scheme does not support privacy protection and system control. The schemes of [35, 36] are similar to our scheme in the function and flexibility of the access structure, but they do not support system control, and scheme [35] does not support privacy protection. Scheme [34] is based on the LWE problem on the standard lattice, the encryption byte of the scheme is 1, and the other three schemes are based on the RLWE, and the encryption byte is n . We can know from scheme [34, 36], that $m_1 \geq 5n\log q$ and $m_2 \geq 6n\log q$, the size of the user secret key and ciphertext in our scheme are smaller than scheme [34, 36], which are consistent with scheme [35].

It is an interesting research direction to use the combination of attribute-based encryption and blockchain to achieve better performance in data access control. In order to better explain the characteristics of this scheme, some schemes based on blockchain and attribute-based encryption are selected to analyse from the function and characteristics. The comparison of some functions is listed in Table 5.

It proposed a new trustworthy secure and attribute hiding access control scheme based on blockchain in [37], the scheme can reduce the trust cost, reduce the single point of failure, and realize distributed and trusted access control management. ElGamal homomorphic encryption was used

to ensure the attribute privacy during authorization validation. The scheme takes advantage of the decentralization of blockchain and pays attention to the security risks caused by the transparency of blockchain.

It proposed a blockchain-based security sharing scheme for personal data named BSSPD in [38], and the feature of this scheme is user-centric. There is no other entity between the data owner and the data user. The data owner can fully control its shared data, ensuring privacy and security, and it can provide ciphertext keyword search. Although this improves the security of the data, the data owner needs to process the requests from the data users, which will sacrifice the time and energy of the data owner.

In order to solve the problems of access control in the medical industry, SHDPCPC-CP-ABE scheme was proposed in [39]. The scheme focuses on the data storage and policy optimization in medical treatment, and ensures the privacy of users in the claim process through homomorphic encryption. The scheme makes use of the immutability of blockchain to realize the user's medical record.

In scheme [40], the medical data problem is also concerned, especially how to solve the data sharing problem caused by remote devices. This scheme combines blockchain and other technologies to propose an architecture, which realizes data exchange between different fields without strong trust assumption, and can also provide the inherent forensics mechanism tailored.

In order to solve the security and efficiency problems of cloud data, the scheme of user-centric block level attribute-based encryption is proposed based on the traditional blockchain in [41], and Data Level Access Trust is used to provide certain privacy services.

All of the above schemes are based on the decentralization of blockchain to reduce the trust cost. They focus more on avoiding single point of failure and implementing distributed management, which is a wide range of data sharing and access control between different fields. The difference is that the scheme proposed in this paper is aimed at those units and organizations with high security requirements, such as the military and government

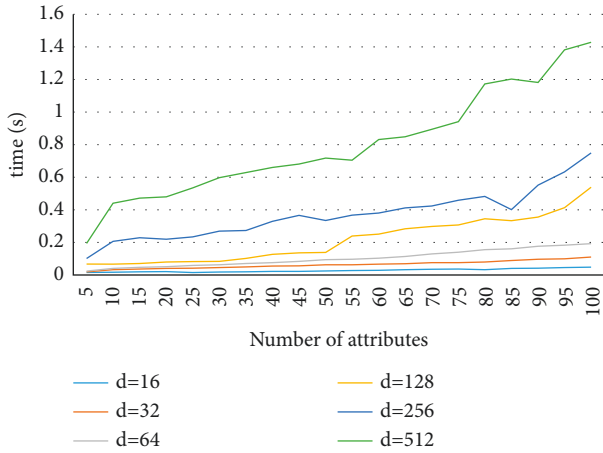


FIGURE 3: Run time of system initialization.

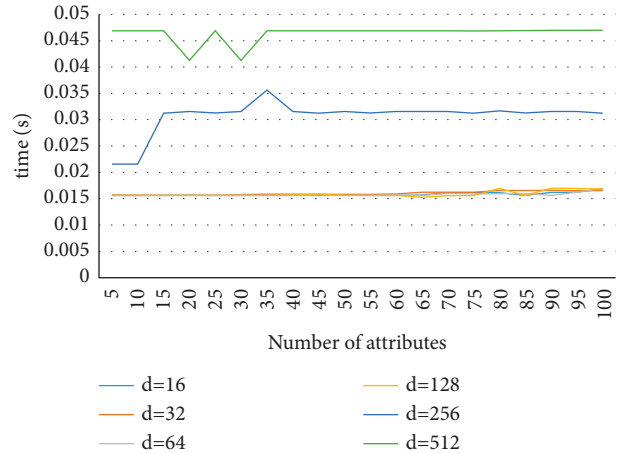


FIGURE 6: Run time of tag generation.

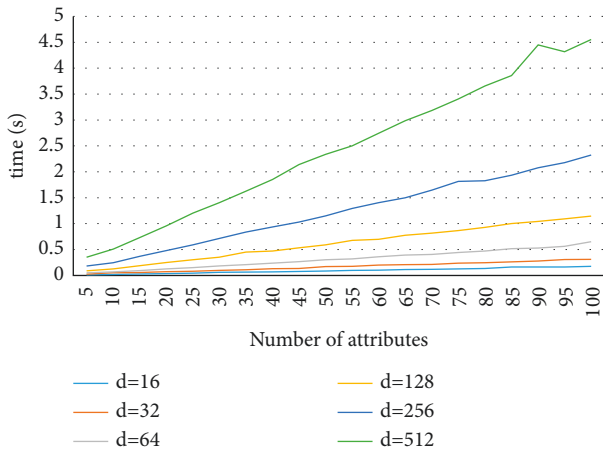


FIGURE 4: Run time of key generation.

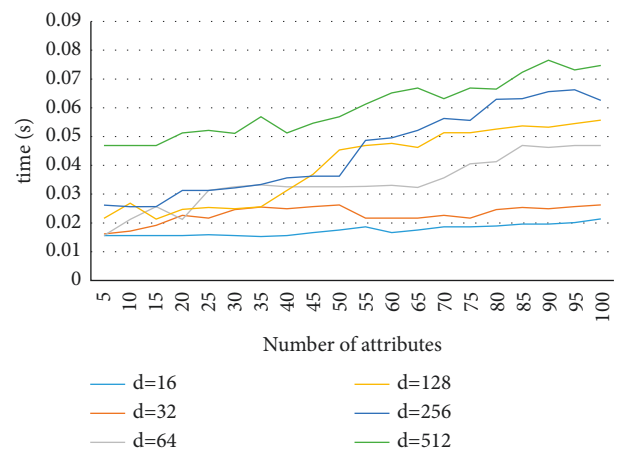


FIGURE 7: Run time of sanitizing.

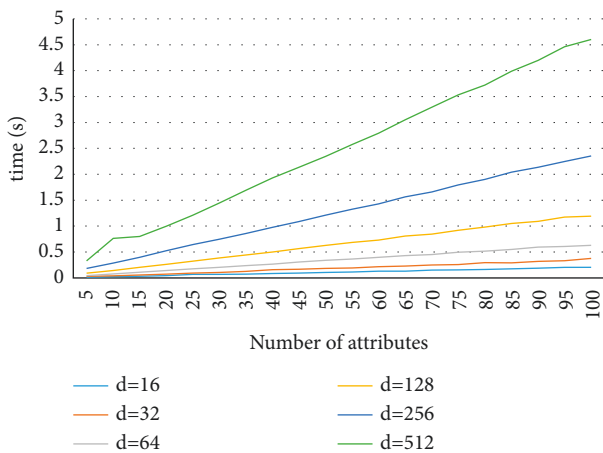


FIGURE 5: Run time of ciphertext generation.

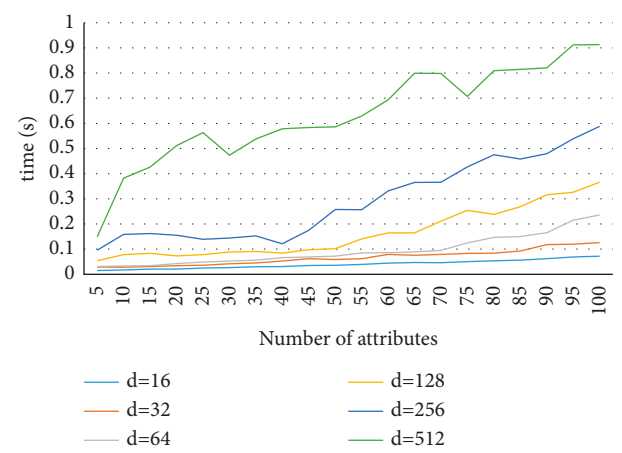


FIGURE 8: Run time of decryption.

departments with high level of confidentiality. These units need to be under certain supervision and control, but also need data sharing and access control. At present, there are few papers focusing on this aspect, so we cannot make a similar comparison. To solve this problem, we give a

specific scheme based on private chain and ABE, which can resist quantum attacks. Although fully trusted entities are required, which increases the trust cost, these sacrifices are necessary for scenarios with high security requirements.

4.3. Experimental Analysis. This section analyses the operation efficiency of this scheme in different stages, including six algorithms: system initialization, key generation, tag generation, sanitizer key generation, sanitize and decryption, and simulates the operation time of these algorithms when the number of attributes ranges from 5 to 100.

The experiment is performed on a 64 bit Windows 10 operating system with inter (R) core™ i7-6700HQ CPU @ 2.60 GHz processor and 16 GB of memory. The parameters selected in this experiment are $q = 67108289$, $p = 3$. In order to better analyse the performance of the scheme, the degrees of polynomials are 16, 32, 64, 128, 256, 512 respectively.

As shown in Figure 3, the system initialization time of our scheme is linear with the number of attributes. As the degree increases, the running time increases with the number of attributes, and the change trend is more and more obvious. Like Figure 3, Figures 4 and 5 show a linear relationship between running time and the number of attributes. Because the key generation stage and encryption stage need multiple multiplication operations, it takes a long time. The specific number of multiplications is related to the number of attributes. However, in general, there are not so many attributes in the policy and in the attribute set of a single user. Figures 6 and 7 show that the running time of the algorithm has nothing to do with the number of attributes, and the algorithm takes a short time and does not bring too much burden to the system, which is also consistent with the theoretical analysis. Figure 8 shows a linear relationship between running time of the decryption and the number of attributes, and there is little difference in the performance of the algorithms below $d = 128$.

5. Conclusion

This paper focuses on how to carry out data sharing and access control in the case of high security requirements. Based on the combination of private chain and attribute-based encryption, a sanitizer is set up to supervise the shared data, avoiding data sharing that violates the system control policy. Although higher trust assumptions are required, higher security and reliability can be obtained, which is of certain significance in specific situations. Through analysis, the scheme meets the No-Read and No-Write rules and the security under chosen-plaintext attack. In terms of performance, the scheme is constructed based on RLWE problem, and its efficiency is better than the scheme based on LWE. In terms of function, it focuses on providing system control and resisting quantum attacks compared with other schemes. Of course, other schemes also have many features that this scheme does not have, such as the problem of updating attributes and policies, the problem of searching ciphertext and so on. In addition, the paper also carries out experimental simulation on the attribute-based encryption and decryption part of the scheme. Unfortunately, the paper does not simulate the whole access process in combination with the blockchain platform. These are the work we need to do in the next step.

Data Availability

All data used during the study are available from the corresponding author upon request.

Conflicts of Interest

The authors state that there is no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61572521), Engineering University of the PAP Innovation Team Science Foundation (No. KYTD201805), Natural Science Basic Research Plan in Shaanxi Province of China (2021JM252).

References

- [1] J. Shen, T. Zhou, and Z. Cao, "Protection methods for cloud data security," *Journal of Computer Research and Development*, vol. 58, no. 10, pp. 2079–2098, 2021.
- [2] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Public Key Cryptography—Pkc2011*, pp. 53–70, Springer, Cham, Switzerland, 2011.
- [3] S. Chawla, "A review on attribute based encryption techniques of access control in cloud computing," *International Journal of Distributed and Cloud Computing*, vol. 6, no. 2, pp. 24–27, 2018.
- [4] V. Goyal, O. Pandey, and A. Sahai, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security—CCS*, vol. 6, p. 89, Alexandria, VA, USA, Virginia USA, October 2006.
- [5] V. Umadevi and E. K. Girisan, "Integrity checking in cloud storage and policy based user revocation using attribute based encryption," *International Journal of Recent Technology and Engineering*, vol. 8, pp. 6905–6911, 2019.
- [6] X. Zhang, F. Wu, W. Yao, Z. Wang, and W. Wang, "Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 21, Article ID e4678, 2019.
- [7] S. Senthilkumar and V. M. Viswanatham, "ERAC-MAC efficient revocable access control for multi-authority cloud storage system," *International Journal of Internet Technology and Secured Transactions*, vol. 9, no. 3, pp. 221–241, 2019.
- [8] L. Zhang, L. Li, E. Medwedeff, H. Huang, X. Fu, and R. Wang, "Privacy protection of social Networks based on classified attribute encryption," *Security and Communication Networks*, vol. 2019, pp. 1–14, Article ID 9108759, 2019.
- [9] X. Li, Y. Chen, and H. Zhu, "An access control scheme supporting privacy protection based on blockchain and attribute," *Journal of Physics: Conference Series*, vol. 1966, no. 1, Article ID 012048, 2021.
- [10] M. Wang, Z. Zhang, and C. Chen, "Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 4, pp. 1237–1245, 2016.
- [11] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any

- monotone access structures,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 76–88, 2013.
- [12] J. Ning, X. Dong, Z. Cao, Lifei Wei, and Xiaodong Lin, “White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.
- [13] Z. Liu, Q. Huang, and D. S. Wong, “On enabling attribute-based encryption to Be traceable against traitors,” *The Computer Journal*, vol. 64, no. 4, pp. 575–598, 2020.
- [14] L. Qiu, F. Cai, and G. Xu, “Quantum digital signature for the access control of sensitive data in the big data era,” *Future Generation Computer Systems*, vol. 86, pp. 372–379, 2018.
- [15] A. Rahmani, A. Amine, and M. Reda, “A mathematical model of access control in big data using confidence interval and digital signature,” *Computer Science & Information Technology (CS & IT)*, vol. 5, no. 15, pp. 183–198, 2015.
- [16] M. Naor and A. Wool, “Access control and signatures via quorum secret sharing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 9, no. 9, pp. 909–922, 1998.
- [17] S. Chhabra and A. Kumar Singh, “Security enhancement in cloud environment using secure secret key sharing,” *Journal of Communications Software and Systems*, vol. 16, no. 4, pp. 296–307, 2020.
- [18] X. Liu, J. Ma, and J. Xiong, “Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,” *International Journal on Network Security*, vol. 16, no. 6, pp. 437–443, 2014.
- [19] I. Damgård, H. Haagh, and C. Orlandi, “Access control Encryption Enforcing information flow with cryptography,” *Cryptography and Information Security Series*, vol. 106, 2016.
- [20] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Aarhus, Denmark, June 2005.
- [21] S. Yu, W. Cong, and K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in *Proceedings of the 2010 Proceedings IEEE INFOCOM*, pp. 1–9, St. Petersburg Russia, May 2010.
- [22] J. Zhou, Z. Cao, and X. Dong, “TR-MABE: white-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems,” in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2398–2406, Hong Kong, China, April 2015.
- [23] T. Yang, P. Shen, and X. Tian, “Access control mechanism for classified and graded object storage in cloud computing,” *Journal of Software*, vol. 28, no. 9, pp. 2334–2353, 2017.
- [24] G. Li and H. Sato, “A privacy-preserving and fully decentralized storage and sharing system on blockchain,” in *Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, pp. 694–699, WI, USA, July 2019.
- [25] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, “Efficient and privacy-preserving traceable attribute-based encryption in blockchain,” *Annals of Telecommunications*, vol. 74, no. 7-8, pp. 401–411, 2019.
- [26] B. Yu and Z. Ma, “The study on attribute and trust-based RBAC model in cloud computing,” *Computer Engineering and Applications*, vol. 9, pp. 84–92, 2020.
- [27] X. Zhang and Y. Yu, “Blockchain data sharing model based on attribute-based encryption,” *Application Research of Computers*, vol. 38, no. 8, pp. 2278–2283, Apr. 2021.
- [28] S. Kim and D. Wu, “Access control encryption for general policies from standard assumptions,” *International Conference on the Theory and Application of Cryptology and Information Security*, vol. 10624, pp. 471–501, 2017.
- [29] P. Wang, T. Xiang, X. Li, and H. Xiang, “Access control encryption without sanitizers for Internet of Energy,” *Information Sciences*, vol. 546, pp. 924–942, 2021.
- [30] V. Lyubashevsky, C. Peikert, and O. Regev, “A toolkit for ring-LWE cryptography,” *EUROCRYPT*, vol. 7881, pp. 35–54, 2013.
- [31] S. Tan and S. Azman, “Lattice ciphertext-policy attribute-based encryption from ring-LWE,” in *Proceedings of the 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET)*, pp. 258–262, Langkawi, Malaysia, August 2015.
- [32] G. Tan, R. Zhang, and H. Ma, “Access control encryption based on LWE,” in *Proceedings of the 4th ACM International Workshop on ASIA Public-Key Cryptography*, pp. 43–50, UAE, April 2017.
- [33] K. Guo, Y. Han, and L. Kai, “Traceable attribute-based encryption on OBDD access structure from lattice,” in *Proceedings of the 2022 11th International Conference on Communications, Circuits and Systems (ICCCAS)*, pp. 210–215, Singapore, May 2022.
- [34] Y. Wang, “Lattice ciphertext policy attribute-based encryption in the standard model,” *International Journal on Network Security*, vol. 16, no. 6, pp. 444–451, 2014.
- [35] X. Yan, Y. Liu, and Z. Li, “Privacy-preserving attribute-based encryption scheme on ideal lattices,” *Journal on Communications*, vol. 39, no. 03, pp. 128–135, 2018.
- [36] S. Zhao, R. Jiang, and B. Bhargava, “RL-ABE: a revocable lattice attribute based encryption scheme based on R-LWE problem in cloud storage,” *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 1026–1035, 2022.
- [37] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, “TrustAccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.
- [38] H. Gao, Z. Ma, S. Luo, Y. Xu, and Z. Wu, “BSSPD: a blockchain-based security sharing scheme for personal data with fine-grained access control,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6658920, 20 pages, 2021.
- [39] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, “EHRChain: a blockchain-based ehr system using attribute-based and homomorphic cryptosystem,” *IEEE Transactions on Services Computing*, vol. 38, p. 1, 2021.
- [40] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, “A hierarchical multi blockchain for fine grained access to medical data,” *IEEE Access*, vol. 8, pp. 134393–134412, 2020.
- [41] S. Godfrey Winster, A. Siva Kumar, and R. Ramesh, “User centric block-level attribute based encryption in cloud using blockchains,” *Computer Systems Science and Engineering*, vol. 42, no. 2, pp. 605–618, 2022.