Logistics Privacy Protection Scheme Based on Multi-Authority Attribute-Based Encryption

Sinan Zhao

Beijing University of Technology, Beijing, China

Corresponding Author:sinan_zhao@126.com

Abstract.- In response to the issues of easy leakage of user privacy data and chaotic permission management in the logistics industry, this paper proposes a privacy protection scheme for logistics users based on multi-authority attribute-based encryption. The scheme improves the attribute-based encryption algorithm of multi-authority, designs an AR-MA-ABE algorithm that supports attribute revocation, and achieves fine-grained access control over logistics data. By utilizing multi-authority attribute-based encryption, the computational burden on a single authority is reduced. By incorporating a revocation mechanism, the computational overhead resulting from attribute revocation issues is mitigated. Through security analysis, it is demonstrated that this scheme is secure against plaintext attacks.

Keywords: Multi-Authority; Attribute-Based Encryption; Logistics; Privacy Protection;

1 Introduction

In the logistics industry, there are numerous personnel involved, and to protect user privacy and ensure that certain private data can only be accessed by relevant personnel, it is necessary to prevent situations such as information resale and privacy breaches [1]. At the same time, it is crucial to ensure that the permissions of personnel involved in work shifts are promptly updated. Therefore, safeguarding user privacy information and preventing personal data leakage in the logistics process has become an urgent issue in the industry.

In 2019, Gao Qi proposed the application of attribute-based encryption (ABE) technology in the privacy data protection scheme of the logistics industry. This involved using the CP-ABE mechanism for encryption, achieving fine-grained access control for logistics information[2]. In 2021, Lin et al. categorized order information into logistics, personal, and product information. Administrators encrypted planned routes based on attributes, and logistics stations decrypted them based on acquired keys corresponding to attributes[3]. In 2022, Sheng et al. introduced a method called Cipher Policy Attrib

T. Yao et al. (eds.), *Proceedings of the 2024 3rd International Conference on Engineering Management and Information Science (EMIS 2024)*, Advances in Computer Science Research 111,
https://doi.org/10.2991/978-94-6463-447-1_41

coordinates of transit station locations as spatial attributes, the normal working hours of delivery personnel as temporal attributes, and the job identities of delivery personnel as access attributes to ensure that visitors possess relevant permissions[4]. In 2023, Liu Yuxi improved upon CP-ABE by integrating blockchain technology to achieve user-level revocation for malicious access[5]. However, the aforementioned solutions fail to address the security risks that arise when logistics personnel undergo attribute changes due to work adjustments or other circumstances. Additionally, CP-ABE still suffers from issues such as single-point failure and limited scalability[6].

Therefore, this paper proposes a logistics privacy protection scheme based on multi-authority attribute encryption that supports attribute revocation. By integrating with the logistics application scenario and enhancing the MA-ABE algorithm to support attribute revocation, it not only achieves fine-grained access control but also avoids the significant computational overhead caused by attribute revocation[7]. Through security analysis, it is proven to be secure against plaintext attacks.

2 System Model

In this scheme, the main entities involved include the Certificate Authority, Attribute Authority, Data Owner, and Data Requester. The system model diagram is shown in Fig. 1. System Model Diagram, and a detailed description is provided as follows:

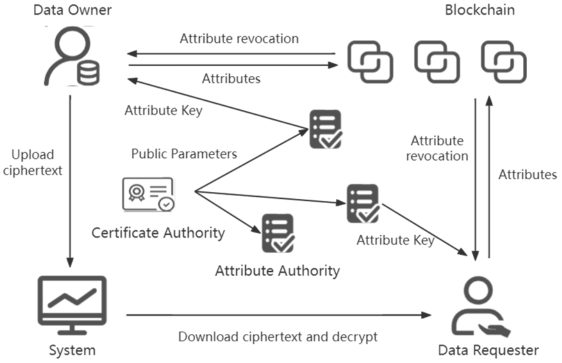

Fig. 1. System Model Diagram

Certificate Authority (CA): Responsible for generating public parameters and master keys for the system.

Attribute Authority (AA): Each authorization entity manages different sets of attributes and generates relevant attribute private keys for users.

Data Owner (DO): Typically, the sender user or the collection personnel. After placing an order, the system assigns a collection site for the sender user, and the collection site customizes the logistics route and access policies for them after collecting the package.

Data Requester (DR): Typically, the logistics systems and their personnel at various sites, sender users, and recipient users. They obtain the corresponding attribute private keys from various attribute authorization entities and then apply to the system to download the corresponding ciphertext information, and call the decryption algorithm for decryption.

Blockchain: Responsible for recording user attributes and Attribute Revocation Lists (ARL). Whenever the ARL is updated, users involved with the relevant attributes are promptly notified to update their keys.

3 Scheme Design

The overall key steps of the logistics information privacy protection scheme comprise five stages: system initialization stage, attribute key generation stage, logistics information encryption stage, logistics information decryption stage, and logistics information re-encryption stage. Below are detailed descriptions of each stage.

3.1 System Initialization Stage

This stage primarily involves the overall initialization of the system, including the initialization of the Certificate Authority (CA) and Attribute Authorization Centers (AA). The detailed explanations are provided below:

System Initialization.

System initialization is performed by the Central Authority. During initialization, the CA first selects prime-order cyclic groups G_1 and G_2 with p being a prime number, where g is a generator of G_1, and then constructs a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$. Subsequently, the CA randomly selects $\alpha, \gamma \in Z_p$, generates the global master key MK = $\{\alpha\}$, and computes the public parameters $PK = g^{\alpha}$, where the master key MK is securely stored by the CA. The global parameters include (G_1, G_2, e, g, $e(g, g)^{\alpha}$, g^{γ}, γ, PK).

Attribute Authorization Agency Initialization.

Each Attribute Authority needs to perform the following steps: for each attribute j, select two random numbers $y_j, z_j \in Z_p$. Calculate the public key $PK_j = g^{y_j}$, calculate the attribute public key $PK_j' = g^{z_j}$, calculate the attribute private key $SK_j = y_j$, and compute the attribute private key $SK_j' = z_j$.

3.2 Attribute Key Generation Stage

The data requester applies for attribute keys from multiple AAs, and each AA distributes private keys based on its attribute set S. For each attribute $j \in S$ of the data requeste, calculate the key $D_j = g^{\frac{\gamma}{\beta_j}}$, calculate the key $D'_j = g^{\frac{sk'_j}{\beta_j}}$, where β_j is a randomly selected secret value of DR. Calculate the key $D = g^{\frac{sk_j+sk'_j}{\beta_j}.\gamma+\alpha}$. The final set of attribute private keys obtained by the data requester DR is $(\{D, D_j, D'_j\}\{j \in S\})$. After the successful application for attributes by the Data Requester (DR), their attribute list will be uploaded to the blockchain, facilitating subsequent attribute matching and attribute revocation checks.

3.3 Logistics Information Encryption Stage

In the overall scheme, there are three roles involved that require logistics information encryption: sender: Needs to encrypt personal order privacy information initiated by individuals. Logistics Collection Personnel: Needs to encrypt segmented logistics routes after planning. Logistics Transit Personnel: Needs to encrypt the transit information of parcels.Their detailed descriptions are as follows:

Sender.

The sender initiates an order in the logistics system, which mainly includes four parts of information: sender information (name, phone number, address), recipient information (name, phone number, address), item information (type, volume, weight), and site information (collection site automatically located by the system based on the sender's address, delivery site automatically located by the system based on the recipient's address).

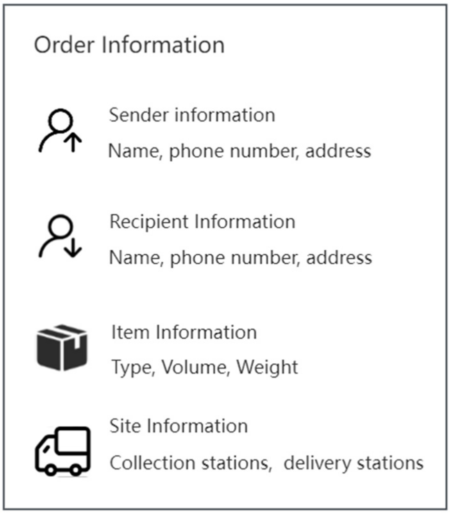

Fig. 2. Specific Content of Order Information

The ciphertext information after encrypting the order information mainly consists of two parts: CTsen and CTrec. CTsen is for the collection personnel to view, which mainly includes sender information, collection site, delivery site, and item information. Sender information is used for collection personnel to pick up parcels, collection sites, and delivery sites are used for collection personnel to plan logistics routes, and item information is used to check if the parcel contains hazardous items. CTrec is for delivery personnel to view, which mainly includes recipient information for parcel delivery. The information are shown in Fig. 2. Specific Content of Order Information.

Logistics collection personnel.

The collection site receives the user's order request, and the collection personnel apply to access the corresponding ciphertext information. After decrypting the ciphertext CTsen with their own attribute private key, they obtain the plaintext information. Subsequently, they proceed to the user's location to inspect and receive the package. The collection personnel then use the system's logistics route planning function based on the collection site and delivery site specified in the order to automatically generate the corresponding delivery route. They segment each segment of the logistics route and set corresponding access policies for them. Then, they encrypt each segment using the AR-MA-ABE algorithm. After completing the encryption operation, the collection personnel need to associate the generated ciphertext information with the order number for access by transit personnel.

Logistics transit personnel.

When a parcel arrives at a transit station, transit personnel need to upload the transit information of the parcel (including order number, transit time, transit station, etc.) and the status information of the parcel (such as parcel photos, damage conditions, etc.) before executing the transit operation. They also need to set corresponding access policies for them. Subsequently, they encrypt this information using the AR-MA-ABE algorithm. After completing the encryption operation, the generated ciphertext information is associated with the order number, allowing logistics users on both sides to view relevant information.

The specific encryption process is as follows:

① Choose a random number $s \in Z_p$. Randomly select the secret encryption exponent s, where $s \in Z_p$ is the secret value to be shared. Choose a random vector $\vec{v} = (s, y_2 ... y_n)$, where the random numbers $y_2, ..., y_n \in Z_p$.

② Calculate the ciphertext $\tilde{C}$ using the following formula, where M is the plaintext message.

$$\tilde{C} = M\,e(PK, g)^s = Me(g, g)^{\alpha s}$$

③ For each attribute in the access structure (A, ρ), where A is an $(l + 1) \times n$ matrix, calculate $\lambda_i = A_i \cdot \vec{v}, i \in [1, l]$. The obtained λ_i are l shared subkeys of the secret s, where λ_i belongs to the participant $\rho(i)$. A_i corresponds to the i-th row of the matrix. Calculate $C_x = g^{\gamma\lambda_i}$, and calculate $C'_x = PK_j^{\lambda_i}$.

④Calculate $C = g^s$.

After the above calculations, the ciphertext is finally composed of $\left(C, \widetilde{C}, \{C_x, C_x'\}\{x \in A\}\right)$.

3.4 Logistics Information Decryption Stage

The scheme involves five roles that require decryption of logistics information: the sender and recipient, who need to view the logistics status information of the order; the logistics collection personnel, who need to access sender-related information to complete doorstep collection operations; the logistics transfer personnel, who need to request access to transit station information in the order protocol stack; and the logistics delivery personnel, who need to request access to recipient-related information to complete doorstep delivery operations. The specific decryption operations are as follows:

① Request ciphertext CTi from the system.

② Use the attribute private keys $\left(\{D, D_j, D_j'\}\{j \in S\}\right)$ of the data accessor DR with attributes S, and the components of ciphertext CTi consisting of $\left(C, \widetilde{C}, \{C_x, C_x'\}\{x \in A\}\right)$, the plaintext (M) is obtained by the following formulas:

$$F = \prod_{x \in S} \left(e\left(D_j, C_x'\right) e\left(D_j', C_x\right)\right)^{\omega_i} = \prod_{x \in S} e(g, g)^{\frac{y_j}{\beta_j}\gamma\lambda_i\omega_i + \frac{z_j}{\beta_j}\gamma\lambda_i\omega_i} = e(g, g)^{(\frac{y_j}{\beta_j} + \frac{z_j}{\beta_j})\gamma s}$$

$$M = \frac{\widetilde{C} \cdot F}{e(D, C)} = \frac{Me(g, g)^{\alpha s} e(g, g)^{(\frac{y_j}{\beta_j} + \frac{z_j}{\beta_j})\gamma s}}{e(g^{\frac{sk_j + sk_j'}{\beta_j} \cdot \gamma + \alpha}, g^s)}$$

The data accessor DR performs the above operations in accordance with its corresponding access structure (A, ρ), successfully decrypting and obtaining plaintext information.

3.5 Logistics Information Re-encryption Stage

When logistics system personnel are transferred due to work or other reasons, causing changes in user attributes where certain attributes may no longer be possessed by the user, failure to promptly update the relevant ciphertext may enable logistics personnel to exploit their duties to access logistics privacy information. Therefore, it is necessary to design corresponding mechanisms for attribute revocation scenarios.

To support attribute revocation, each Attribute Authority needs to maintain an Attribute Revocation List (ARL). Whenever an attribute j needs to be revoked, the Attribute Authority AA must promptly update the revoked attribute public keys PK_j and PK_j', as well as the public keys UK_j^1 and UK_j^2 used for user key updates. Additionally, the Attribute Authority will publish UK_j^1 and UK_j^2, along with the revocation time, to the Attribute Revocation List ARL, which will be made available to all users for self-checking whether their attributes have expired and for timely updating of attribute private keys.

The attribute revocation list is publicly available on the blockchain for all users to view. The blockchain notifies users involved with relevant attributes to update their attribute keys based on the update time and updated attributes in the Attribute Revocation

List (ARL). The keys of affected users are automatically invalidated. When users devise access policies involving attributes listed in the ARL, they are alerted to the attribute's invalidation and prompted to reconfigure their access policies before encryption. All encrypted ciphertexts need to be recalculated for attributes: $C_x' = PK_j^{\lambda_i} = g^{y_j'\lambda_i}$.

The specific operation process for AA to update the Attribute Revocation List (ARL) is as follows:

① For the revoked attribute j, AA selects two new random numbers $y_j', z_j' \in Z_p$, and updates the public key $PK_j = g^{y_j'}$ for the revoked attribute, as well as the attribute public key $PK_j' = g^{z_j'}$.

②For each user requiring an update of their private key due to revoked attributes, AA will publish the new public keys for users to update their attribute private keys $UK_j^1 = g^{\frac{y_j' - y_j}{\beta_j}}$ and $UK_j^2 = g^{\frac{z_j' - z_j}{\beta_j}}$. At the same time, AA will release UK_j^1, UK_j^2, and the revocation time to the ARL.

The specific operational steps for updating user attribute private keys are as follows:

① When a portion of a user's attributes is revoked, their attribute keys become invalid. From the Attribute Revocation List (ARL), obtain UK_j^1, UK_j^2, and compute the following formula to derive the attribute private key.

$$D_j'' = D_j' \cdot UK_j = g^{\frac{sk_j'}{\beta_j}} \cdot g^{\frac{z_j' - z_j}{\beta_j}} = g^{\frac{z_j'}{\beta_j}}$$

$$D' = D \cdot UK_j = D \cdot \left(UK_j^1\right)^{\gamma} \cdot \left(UK_j^2\right)^{\gamma}$$

$$= g^{\frac{sk_j + sk_j'}{\beta_j} \cdot \gamma + \alpha} \cdot g^{\frac{y_j' - y_j}{\beta_j}\gamma} \cdot g^{\frac{z_j' - z_j}{\beta_j}\gamma} = g^{\frac{y_j' + z_j'}{\beta_j} \cdot \gamma + \alpha}$$

② The updated attribute private key for the user is denoted as $\left(\{D', D_j, D_j''\}\{j \in S\}\right)$.

4 Security Analysis

According to the definition of the Decisional Parallel Bilinear Diffie-Hellman Exponent (q-PDBDH) problem, if an adversary aims to successfully compromise the proposed attribute-based encryption scheme, there must exist a probabilistic polynomial-time algorithm capable of solving the q-PDBDH problem. The adversary-challenger game proceeds as follows:

Adversary A submits to the simulator B the compromised AA, the normal AA, the attribute set S, two plaintexts m_1 and m_2, and an access structure (M^*, ρ^*).

Query Phase: Adversary A issues attribute key queries and other processes, but is restricted from posing attribute key queries related to CT.

Challenge Phase: Simulator B randomly selects one plaintext from m_1 and m_2 for encryption, generates the challenge ciphertext CT^*, and sends it to adversary A.

Guess Phase: Adversary A guesses which plaintext was encrypted (1 or 2). If the guess is correct, adversary A wins the game. The advantage of adversary A in the above game is $Pr[b' = b] - \frac{1}{2}$.

Definition 1: If the probability of adversary A winning the above game in polynomial time is negligible, then the proposed multi-authority attribute-based encryption scheme is secure against chosen plaintext attacks.

Theorem 1: Assuming the security assumption holds, there does not exist an adversary A who, in polynomial time bounded by any time bound, can conduct a selective attack on this scheme using a challenge matrix M^* of size $l^* \times n^*$.

Proof: Assuming adversary A selects a challenge matrix M^* of order q, which breaks the indistinguishability of this scheme with non-negligible advantage, we can construct a simulator B leveraging adversary A to solve the security assumption problem with non-negligible advantage.

Initialization Phase: Simulator B inputs a set of challenge arrays $y = \left((g, g^a, \ldots, g^{a^q}, g^{a^{q+2}}, g^{a^{2q}}\right)$ for the q-BDHE problem, runs the initialization algorithm, and adversary A needs to select a set of compromised attribute structures AA' ⊂ AAθ and sends the compromised attribute structures to simulator B. Then, simulator B chooses $\alpha' \in Z_p,\ \alpha = \alpha' + a^{q+1}$, resulting in $e(g,g)^\alpha = e\left(g^a, g^{a^q}\right)e(g,g)^{\alpha'}$.

Interrogation Phase 1: Adversary A sends multiple attribute sets $S_1, S_2, \ldots, S_n$ to simulator B, where these attribute sets do not satisfy the access structure (A, ρ). Adversary A then queries simulator B for attribute keys. Simulator B runs the attribute key generation algorithm and returns the corresponding attribute keys to adversary A. By the reconstructability of the linear secret sharing matrix, it is certain that there $\exists \omega_i \in Z_p$ such that $\omega_1 = -1$ and for all j, $W = (\omega_1, \omega_2, \ldots \omega_n)$ such that $\omega_1 M_{j,1} + \omega_2 M_{j,2} + \ldots + \omega_n M_{j,n} = 0$. Expressing z_j, $\frac{1}{\beta_j}$, and y_j with linear relationships involving M, for each element j in the attribute set S, simulator B randomly selects $\eta \in Z_p$, $\frac{1}{\beta_j} = \eta + \omega_1 a^q + \omega_2 a^{q-1} + \ldots + \omega_n a^1$. Here, $x, \eta, \theta \in Z_p$. If $j \in U$, then let $z_j = x + M_{j,1}a + M_{j,2}a^2 + \ldots + M_{j,n}a^n$, $y_j = \theta + M_{j,1}a + M_{j,2}a^2 + \ldots + M_{j,n}a^n$. By calculation, the user private keys can be obtained as follows:

$$D_j = g^{\gamma(\eta + \omega_1 a^q + \omega_2 a^{q-1} + \ldots + \omega_n a^1)}.$$

$$D_j' = g^{(\theta + M_{j,1}a + M_{j,2}a^2 + \ldots + M_{j,n}a^n)(\eta + \omega_1 a^q + \omega_2 a^{q-1} + \ldots + \omega_n a^1)}$$

$$= g^{\theta\eta} \cdot \prod_{i=1,2,\ldots n} g^{M_{j,i}a^i\eta} \cdot \prod_{i=1,2,\ldots n} g^{\prod_{\substack{m=1,2,3\ldots n \\ m \neq i}} a^{(q+1+i-m)}\omega_m M_{j,i}}$$

$$D = g^{(\theta+x)(M_{j,1}a + M_{j,2}a^2 + \ldots + M_{j,n}a^n)\cdot(\eta + \omega_1 a^q + \omega_2 a^{q-1} + \ldots + \omega_n a^1)\cdot\gamma + \alpha' + a^{q+1}}$$

If $j \notin U$, then let $z_j = x$, $\beta_j = y$. $D_j' = g^{x\eta}, D_j = g^{\gamma\eta}, D = g^{(\theta+x)\cdot\eta\cdot\gamma + \alpha' + a^{q+1}}$

Challenge Plaintext Phase: Adversary A sends a plaintext set to simulator B, denoted as $m' = \{m_1, m_2\}$, where m_1, m_2 have the same length. Meanwhile, adversary A specifies a challenge access structure (M^*, ρ^*), and sends it to simulator B. Simulator B randomly selects $b \in \{0,1\}$, encrypts m_b, and sends the ciphertext CT to adversary A. Afterwards, simulator B randomly selects natural numbers $t'2, t'3, \cdots, t'n \in Z$, using the vector δ =$(s, sa + \ t'2, sa^2 + t'3, \cdots, sa^{n-1} + \ t'n)$, where s is the shared secret value. This yields $\lambda'_j = s \cdot M_{j,1} + \sum_{k=2,3,\ldots,n}(sa^{k-1} + t'_k)M_{j,k}$. Adversary A loads the parameters of q-BDHE. In cases where T is equal to $T = e(g,g)^{a^{q+1}s}$ and T=R, the correct probability of adversary A guessing the plaintext encryption is analyzed as follows:

①If $T = e(g,g)^{a^{q+1}s}$, according to the ciphertext calculation formula, we can derive:

$$\tilde{C} = M \cdot e(g,g)^{\alpha s} = M \cdot e(g,g)^{\alpha' s} \cdot e(g,g)^{a^{q+1}s},$$

$$C = g^s,$$

$$C'_x = \ PK_j^{\lambda'_j} = g^{(\theta + \sum_{k=1,2,\ldots,n} M_{j,k} a^k)\lambda'_j}$$

$$= g^{(\theta + \sum_{k=1,2,\ldots,n} M_{j,k} a^k)(s \cdot M_{i,1} + \sum_{k=2,3,\ldots,n}(sa^{k-1} + t'_k)M_{j,k})},$$

$$C_x = \ g^{\gamma \lambda'_j} = g^{\gamma(s \cdot M_{i,1} + \sum_{k=2,3,\ldots,n}(sa^{k-1} + t'_k)M_{j,k})}.$$

Query Phase 2: Adversary A similarly cannot query for an access structure satisfying (M^*, ρ^*), and other inquiries about attribute keys are the same as in Query Phase 1.

Guessing Phase: Adversary A needs to guess the value of b randomly chosen by simulator B and output $b' \in \{0,1\}$. If $b' = b$, simulator B outputs 0 and $Z = e(g,g)^{a^{q+1}s}$. If the guess is incorrect, B outputs 1 and Z is a random element of G. When Z is a random element of G, $Pr[B(y, Z = R) = 0] = \frac{1}{2}$, and when Z is a q-BDHE tuple, $Pr\left[B\left(y, Z = e(g,g)^{a^{q+1}s}\right) = 0\right] = \frac{1}{2} + \varepsilon$.

Since adversary A has broken the scheme with non-negligible advantage, B can solve the security assumption problem with non-negligible advantage. This contradicts the theory of security assumptions; therefore, the proposed scheme is secure.

$$\begin{aligned}\varepsilon' &= \frac{1}{2}\Pr\left[B\left(y, Z \ = e(g,g)^{a^{q+1}s}\right) = 0\right] \\ &+ \frac{1}{2}\Pr[B(y, Z \ = R) = 0] - \frac{1}{2} \\ &= \frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}\end{aligned}$$

5 Conclusion

This paper proposes a logistics privacy protection scheme based on multi-authority ciphertext-policy attribute-based encryption. Firstly, the overall system model of the scheme is constructed, and corresponding security goals are proposed. Then, the detailed design of the scheme is elaborated. In this scheme, there are mainly five stages: system initialization stage, attribute key distribution stage, logistics information encryption stage, logistics information decryption stage, and logistics information re-encryption stage. By designing the AR-MA-ABE technology that supports attribute revocation, fine-grained access control to logistics user privacy data is achieved. Finally, the security analysis of the scheme is conducted, laying the foundation for its feasibility.

References

1. Haibo Y .A secure logistics model based on blockchain[J].Enterprise Information Systems,2019,15(7):1-17.
2. Qi G. A Privacy Protection Scheme for Logistics Information Based on Attribute Encryption [D]. Xidian University,2019.DOI:10.27389/ d.cnki.gxadu.2019.002904.
3. Lin X, JING P, YU C, et al. TPLI:A Traceable Privacy-preserving Logistics Information Scheme via Blockchain, proceedings of the 2021 International Conference on Networking and Network Applications (NaNA), F 29 Oct.-1 Nov.2021,2021 [C].
4. Hong S, PAN H, FANG Y, et al. A Logistics Privacy Protection Scheme Based on Ciphertext Policy Attribute-Based Key Encapsulation; proceedings of the 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), F 15-17 July 2022, 2022 [C].
5. Yuxi L. A Logistics Privacy Protection Scheme Based on Blockchain and Attribute Based Encryption [D]. North China University of Technology,2023.DOI:10.26926/d.cnki.gbfgu.2023.000864.
6. BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption; proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), F 20-23 May 2007, 2007 [C].
7. CHASE M.Multi-authority atribute based encryptionl[C]. Proc of Cryptography Conference on Theory of Cryptography(TCC'07).Am sterdam,Springer Berlin Heidelberg,2007:515-534.