Research on Role Access Control Model Based on Identity Authentication

Ling Chen
School of Computer and Communication, Lanzhou University of Technology, Lanzhou, Gansu, China
Email: m406454494@126.com

Abstract. Cryptography and access control are the core technologies for a secure operating system. Cryptography can guarantee the confidentiality, integrity, availability and unforgeability of information in the access control system. In the identity-based cryptosystem, the user’s private key is centrally generated by the key distribution center, and key escrow is a major security risk. In view of this problem, it is proposed that multiple trusted entities participate in the key distribution scheme in a serial manner. At the same time, this paper adds a separate blind factor to each user to increase security of the scheme; it also introduces the concept of virtual key, which uses additivity of the key space in the pair-based encryption scheme. In key generation, a timestamp $T$ is added, which enables one-time pad of the system, enhances security of the system, and eliminates collusion attacks by KGC and multiple KPA. Finally, the improved signcryption scheme is combined with the RBAC model, and the I_RBAC model is proposed, which enables identity authentication and information confidentiality of users in simple communication in the RBAC model. Finally, the efficiency and safety of this scheme are analyzed.

Keywords. Cryptography; access control; identity-based cryptography; security.

1. Introduction
With the continuous development of computer network technology, excessive data is generated every day in the world. The Internet Data Center (IDC) shows that 148ZB data was created globally in 2021. Nearly a quarter of the data lacks of protection, so data privacy and security issues have become the focus of attention. The purpose of access control (AC) technology is to control access to key resources, prevent the intrusion of illegal users or damage caused by the careless operation of legitimate users, so that only users with corresponding permissions can access data [1]. As the core technology to realize a secure operating system, it is a key technology to guarantee information confidentiality and security. Therefore, it is of great significance to discuss the access control mechanism in the fields of cloud computing, the Internet of Things, and blockchain [2-4]. References [5-7] respectively proposes access control plan based on cryptography mechanisms, blockchain smart contracts and other related fields.

Traditional access control models include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC) [8], attribute-based access control (ABAC) [9], etc. Different access control models have respective authorization ways according to different access control strategies.
However, in traditional access control, all access to resources is managed through a reference monitor mechanism. Since the monitor needs to be permanently online and must be executed in a trust domain beyond the control of the data owner, it directly affects the scalability and deployability limitations of the application. Flexibility also has deficiencies, which is unable to adapt to the dynamic and distributed network environment and therefore will inevitably cause security issues [10, 11].

To solve the above problems, access control is combined with cryptography technology, and the traditional access control method is replaced by cryptography mechanism. This approach eliminates the need for online monitors.

Cryptography, as the core technology of information security, can guarantee the confidentiality, integrity, availability and unforgeability of information in the computer network environment. The traditional method is to achieve confidentiality and authentication at the same time in the way of “signature before encryption”. This method consumes computing resources equal to the sum of signature and encryption, which is less efficient. Zheng proposed the concept of signcryption in reference [12]. Signcryption can enable both signature and encryption functions within a reasonable logical step. Compared with the traditional “signature before encryption”, the required calculation amount and communication costs are low. Therefore, signcryption is an ideal way to guarantee the confidentiality and authentication of message transmission at the same time. In traditional public key cryptography, the identity and public key of an entity are usually managed by the certification authority CA. However, the storage and management of certificates requires high computing and storage overhead, which greatly increases the system burden. In order to simplify the management process, Shamir proposed the concept of identity-based cryptosystem in 1984, which does not require third-party services to bind public keys with identities. The private key is generated by KGC, which simplifies key management. In 2002, literature proposed an identity-based signcryption scheme. However, the identity-based cryptosystem also faces key escrow problem. Once KGC is no longer trusted or the private key of KGC is stolen by an attacker, the entire system is no longer secure.

In view of the above problems, this paper proposes a key distribution scheme involving KGC and multiple KPAs in serial mode, so that the key escrow problem can be solved. At the same time, to prevent KGC from colluding with multiple KPAs, each user is added to an independent blind factor to increase security of the scheme. At the same time, this paper introduces the concept of virtual key [13], which uses additivity of the key space in the pair-based encryption scheme. In key generation, a timestamp T is added, which enables one-time pad of the system, thus enhancing security of the system.

Access control must be based on trusted user identity authentication. However, the RBAC model itself cannot identify the user’s identity and cannot be operated independently. Therefore, it is quite necessary to add identity signcryption technology in the model implementation stage. In the system, information transmitted between users need to be kept confidential to prevent information leakage. Therefore, we combine identity-based signcryption technology with RBAC. First, the RBAC model is formally defined and some elements are extended, including users and roles, etc., so that an I_RBAC model with identity authentication characteristics is designed. Finally, efficiency and security are analyzed.

The rest of this paper is organized as follows. Section 2 introduces related work; Section 3 introduces research foundation; Section 4 introduces the role access control model based on identity authentication; Section 5 analyzes the efficiency and security of the scheme proposed herein. Finally, conclusion and future research work are introduced in the end.
2. Related Work

2.1. Traditional Access Control
There are several types of traditional access control, mainly discretionary access control (DAC) and mandatory access control (MAC), access control lists (ACLs), role-based access control (RBAC), attribute-based access control (ABAC), capability-based access control (CapBAC) [14], etc. For the main feature of DAC, the subject can autonomously grant access rights of the object it owns to other subjects or withdraw the granted permission from other subjects, while MAC restricts the subject access to the object based on the sensitivity level of the object and the subject’s permission level. Since DAC and MAC are access control systems proposed by the US military, their design ideas can be perfectly applied to military systems. For commercial systems, traditional DACs and MACs cannot meet their needs. For commercial systems, it is also necessary to consider its integrity requirements, and its security requirements will vary depending on the differences in the management of various departments and companies. Many requirements cannot be controlled via DAC and MAC. For example, for an enterprise, the information owner is not an individual employee, and the ability to access a certain resource is determined by the employee's position. Therefore, role-based access control is an effective access control strategy for enterprises.

2.2. Access Control Based on Cryptography
In traditional access control, the monitor needs to be permanently online and must be executed in a trust domain beyond the control of the data owner, which directly affects the scalability and deploy ability limitations of the application. In order to solve the above problems, Reference [15] proposes a method of combining access control with cryptography and replacing traditional access control with cryptography mechanism. Researchers have conducted a lot of researches. Reference [16] proposes access control based on identity authentication, which can ensure that any third-party malicious observer, who disguises as an honest user trying to sabotage the system, cannot learn any information about the identity verification process. Reference [17] proposes a proxy re-encrypted access control mandatory assignment scheme, which considers the access control strategy associated with the data item, supports dynamic access control strategy, and retains forward and backward confidentiality after any dynamic updates in the access strategy. The security of the proposed proxy re-encryption scheme and access control scheme is proved in the standard model. Based on a new type of re-encryption method, reference [18] proposes a key traceable access control assignment scheme, which supports any monotonic access instead of re-encrypting the key. Finally, each authority is responsible for generating different components of the key.

3. Research Foundation

3.1. Bilinear Pair
Bilinear pair: Let \( G_1, G_2 \) and \( G_3 \) be three \( q \)-order cyclic groups, \( g_1, g_2 \) are generators of \( G_1, G_2 \) respectively, \( \hat{e} \) is a bilinear mapping, namely: \( e: G_1 \times G_2 \rightarrow G_3 \) meets the following properties.

1. Bilinearity: for any \( a \in G_1, b \in G_2, c, d \in Z_q \), there is \( \hat{e}(a^c b^d) = \hat{e}(a, b)^{cd} \);
2. Non-degeneration: there exists \( a \in G_1, b \in G_2 \), so that the order of \( \hat{e}(a, b) \) at \( G_3 \) is \( q \);
3. Computability: For any \( a \in G_1, b \in G_2 \), there is a polynomial time algorithm \( \hat{e}(a, b) \).

3.2. Identity-Based Signcryption Scheme
The IBSUS scheme [19] consists of four stages: system initialization, key distribution, information
signcryption, and information unsigncryption.

**System initialization:** The system inputs are security parameter \( r \in \mathbb{Z}^* \), group \( G_1, G_2 \) and bilinear mapping \( \hat{e} \). Select Hash function \( H_1, H_2 \) and \( H_3 \), symmetric encryption/decryption algorithm \( E_k(\cdot) \) \( D_k(\cdot) \), and output public parameter \( \text{params} = \{ q, G_1, G_2, e, P, H_1, H_2, H_3, E_k(\cdot), D_k(\cdot) \} \).

**Key distribution:** The system randomly selects the master key \( s \in \mathbb{Z}_q^* \) and keeps it secretly, calculates \( P_p = sp \), calculates the user's private key \( s_i = sH_i(ID_i) \), and transmits \( S_i \) to the user through a secure channel, and at the same time publicizes \( P_p \).

**Information signcryption:** User A sends encrypted message \( m \) to user B, selects \( r \in \mathbb{Z}_q^* \) randomly, calculates \( w = \hat{e}(rS_A, H_i(ID_B)) \), and encrypts the key \( K = H_i(w) \), calculates \( c_1 = rH_i(ID_A) \) and \( m = H_3(c_1, m) \), connects \( c = (c_1, c_2) \) to \( m \), and obtains \( m \); calculates \( c_2 = E_k(m) \) and sends the ciphertext \( c = (c_1, c_2) \) to user B.

**Information unsigncryption:** calculate \( w' = \hat{e}(c_1, S_B) \) and decrypt the key \( K' = H_i(w') \), decrypt \( c_2 \) to get \( \bar{m} = D_k(c_2) \), then obtain \( \bar{m} \) and \( m \); finally check whether \( m \) meets the equation \( m = H_3(c_1, m) \), and authenticate information \( m \).

3.3. Role-Based Access Control Model
There are already many RBAC models. In 2001, Ferraiolo et al. [20] proposed the NIST standard RBAC model. The model consists of four parts: core RBAC; hierarchical RBAC; static separation of duty and dynamic separation of duty. Based on the core RBAC, this paper uses the concept of roles to control user access to resources. Each role has corresponding permissions. By assigning multiple corresponding roles to each user, the user can have the permissions corresponding to the role. Permissions are assigned to roles. Once a user is granted with a role, the user has the permissions corresponding to the role. Session indicates the mapping relationship between users and roles. The basic elements in the RBAC model include: Subject, Object, User, Role, Object, Session, Permission, User-Role Assignment (UA), Role-Permission Assignment (PA), Static Separation of Duty (SSD), Dynamic Separation of Duty (DSD). Figure 1 shows RBAC model’s main components.

![Figure 1. RBAC model.](image)

4. Role Access Control Scheme Based on Identity Authentication

4.1. Model Concepts
Reference [21] introduces the identity cryptosystem of multiple trusted authentication entities. This
paper draws on its ideas, and the simplified identity-based role access control model I_RBAC is shown in figure 2. In the RBAC model, the user’s identity ID is used as the public key, and the role is equivalent to entity authentication KPA. That is, the private key of each role determines part of the user’s private key. Each role has a pair of public and private keys. To prevent KGC from colluding with multiple KPAs, each user is added with an independent blind factor \( x \in \mathbb{Z}_q^* \) to increase security of the scheme. At the same time, the concept of virtual key is introduced, which uses additivity of the key space in the pair-based encryption scheme. In key generation, a timestamp T is added, which enables one-time pad of the system, thus enhancing security of the system. Extend the existing RBAC model elements, then the three sets in the model \( I_{RBAC} = \langle \text{Users}, \text{Roles}, \text{Prms} \rangle \) are as follows.

**User collection:** each user \( u = < ID, S, x > \), where, \( S = S_1 + S_2, ID \in \{0,1\}^* \), the identity of each user is unique, namely: \( \forall u_m, u_n \in \text{Users}, u_m \neq u_n \Rightarrow ID_m \neq ID_n \). \( S = \{ S_{I_D}, S_{H_1}, \ldots, S_{H_n} \} \) is the private key generated by the role, the number of \( S_{I_D} \) owned by the user concerns the number of roles owned, and \( S_2 \) is part of the private key generated by KGC, \( x \) is the blind factor of the user, \( X = xP \).

**Role set:** each role \( r = \{ P_r, S_r \} \), role private key \( S_r \in \mathbb{Z}_q^* \), public key \( P_r = S_r \cdot P \). Any two roles cannot have the same private key, namely: \( \forall r_m, r_n \in \text{Roles}, r_m \neq r_n \Rightarrow S_m = S_n \). Each role must contain a permission list \( PAL(\text{Privilege List}) \) to store the permissions corresponding to the role.

**Permission collection:** \( Prms = 2^{\text{OPS} \times \text{OBS}} \), \( \text{OPS} \) is the operation collection, \( \text{OBS} \) is the resource object collection. Each permission includes the object of operation and a series of operations performed on it.

4.2. Application Scheme

**RM(Role Manager):** Responsible for generating system parameters, defining roles, and assigning roles to users. Trusted RM centrally manages the private keys of all roles, and generates corresponding role private keys when assigning roles to users. The algorithm in the scheme is introduced below by assuming that all participating users share a common set of parameters.

**System setting:** RM executes algorithm and generates system parameters. Let \( P \) be the generator of \( q \)-order \( G_1 \) and the bilinear pair is \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \). RM chooses three Hash functions \( H_1, H_2, H_3 \), the public parameter of the system is \( \langle G_1, G_2, \hat{e}, P, P_P, H_1, H_2, H_3 > \), the system randomly selects the master key \( s \in \mathbb{Z}_q^* \) and keeps it secretly, and then calculates \( P_P = sP \).

**Add a role:** RM adds a new role \( r_i \) in the system.
(1) Randomly select the private key \( s_i \in \mathbb{Z}^*_q \), and public key \( P_i = s_i P \) of the role \( r_i \). \( RM \) must guarantee that \( (P_i, s_i) \) is different from the public-private key pair of the existing role \( r_j \). Otherwise, select \( s_i \) again;

(2) Assign corresponding permission to \( r_i \). Since the role-permission relationship is relatively stable, the role-permission mapping relationship is defined through the \( PAL \) list proposed in 4.1 above, and finally \( (r_i, s_i) \) is transmitted to \( RM \) and stored secretly through a secure channel.

**User assignment:** The user transmits the blind factor \( x \) to \( KGC \) and \( RM \).

The user applies to \( KGC \) for the private key:

1. Verify the identity \( ID \) of the user \( u \);
2. According to the master key \( s \) set by the system, generate \( KGC \) and send part of the private key \( S_i = sH(ID, X) \) to the user.

The user applies to \( RM \) for role assignment:

1. Verify the identity \( ID \) of the user \( u \), and confirm whether the user can have these roles according to the allocation strategy;
2. If the decision is passed, \( RM \) searches the private key \( s_i \) of the role \( r_i \), generates part of the private key \( S_{ir} = s_i H(ID, X) \) of the user \( u \), sends \( S_{ir} \) to the user through a secure channel, and adds it to \( S_i \); in this way, the user gets the complete private key \( S = S_i + S_2 \).

In the \( RBAC \) model, users need simple, fast, safe and confidential communication, so it is necessary to encrypt and decrypt information and verify the user’s identity.

**Information signcryption:** Alice sends encrypted information \( m \) to Bob, and wants to prove her identity (hereinafter A represents Alice and B represents Bob). The following steps are performed.

1. Randomly select \( r \in \mathbb{Z}^*_q \), \( c_1 = rP \), \( c_2 = rX_A \);
2. Add the timestamp \( T \), the encryption key \( K = H_i(w, T) \);
3. Calculate \( w_i = \hat{e}(r(P_1 + \hat{P}_B + X_B), X_A H_i(ID_B, X_B)) \). Where, the virtual public key \( \hat{P}_B \) is the sum of the public keys of user B’s roles.
4. Calculate \( c_3 = (r + x_A)H(ID_B, X_B), \bar{m} = H_2(m, c_3) \), connect \( \bar{m} \) to \( m \), then get \( \bar{m} \). If \( |\bar{m}| > n \), divide it into several units \( \bar{m} \) so that each unit meets \( \bar{m} \in \{0,1\}^n \). Calculate \( c_2 = E_w(\bar{m}) \).
5. User A sends \( c = (c_1, c_2, c_3, c_4, T) \) to user B.

**Information unsigncryption:** After user B receives \( c \), perform the following steps.

1. Check validity of the timestamp \( T \), \( T_0 = T_i - T \). If \( T_0 \) is not within the specified time, refuse to decrypt; otherwise, continue with decryption;
2. Calculate \( \nu_1 = \hat{e}(c_1 + X_A, S_B), \nu_2 = \hat{e}(P_1 + \hat{P}_B, c_3) \), verify whether \( \nu_1 \) is equal to \( \nu_2 \);
3. Use user B’s private key \( S_B \) and blind factor \( x_B \) to calculate \( w_i = \hat{e}(S_B + x_B H(ID_B, X_B), c_3) \), and calculate the decryption key \( K’ = H_3(w, T) \) to decrypt \( c_4 \). \( \bar{m} = D_{K} (c_4) \). User B gets the information \( m \) and \( \bar{m} \). Finally, check whether \( m \) meets the equation \( \bar{m} = H_2(m, c_3) \) and verify whether information \( m \) is satisfied. Otherwise, output \( \perp \).

5. Scheme Analysis

5.1. Efficiency Analysis

(1) For scheme 3.2, in the signcryption stage, the encryptor performs 1 Tate pair calculation and 4
Hash calculations. In the unsigncryption stage, the decryptor performs 1 Tate pair calculation and 2 Hash calculations. This solution employs the same Hash calculation with the same number. Although the entire encryption and decryption process has performed one more Hash function and two more Tate pair calculations, the algorithm for fast calculation of Tate pair is used in the implementation process, so the calculation efficiency is not greatly different, but is basically consistent.

(2) The communication cost of scheme 3.2 is \( q + n + |T| \). The timestamp \( T \) is added to this scheme, so that one-time pad of the system is possible, with security strengthened in authentication. Due to the small timestamp, the communication cost is basically the same.

It can be seen that, on the basis of basically maintaining the excellent characteristics of the original scheme, this scheme improves system security through authentication mechanism. The efficiency analysis is shown in table 1.

| Scheme  | Hash number | Hash time | Tate time | Communication cost          |
|---------|-------------|-----------|-----------|-----------------------------|
| IBSUS   | 3           | 6         | 2         | \( \log_2 q + n \)           |
| This scheme | 3     | 7         | 4         | \( \log_2 q + n + |T| \)     |

5.2. Security Analysis

This paper is also based on the calculation difficulty of the bilinear Diffie-Hellman problem and the security hypothesis of the Hash function. The specific analysis is as follows.

(1) Only the real receiver can decrypt the received ciphertext, while other users cannot decrypt the ciphertext even if they receive it. One needs to calculate with the private key of the real receiver to obtain key \( K' = H_s(\hat{e}(S_B + x_B H_l(ID_B, X_B), c_2), T) \);

(2) The attacker \( C \) sends information to the user \( B \). \( C \) first randomly selects a \( r \in \mathbb{Z}_q^* \), calculates \( c_3 = (r + x_B)H_l(ID_B, X_B) \), and then calculates whether it meets the key \( K \) or \( K' \). Since there is no user's private key or the user’s independent blind factor, the key cannot be calculated, and the ciphertext cannot be generated. Thus, it is impossible to generate the ciphertext \( c_4 = E_k(\hat{m}) \);

(3) To solve the key escrow problem, KGC and multiple KPAs are used to generate the user's private key at the same time. This paper uses the RBAC model, and regards the trust agency RM in the management role as KPA. If one of the two is unilaterally leaked, the user’s complete private key cannot be obtained, and it is impossible to disguise as the user to perform signcryption/unsigncryption;

(4) Finally, if the attacker \( C \) solves the problem in (3) above, he cannot disguise as be a user to perform all operations, because the user's independent blind factor cannot be obtained.

6. Conclusion and Outlook

At present, there are more and more researches on identity-based cryptosystems, and security of various schemes is constantly improving. This scheme adopts the bilinear mapping structure on the elliptic curve, the security of which is based on the bilinear calculation of Diffie-Hellman hypothesis and Hash function. Regarding the issue of third-party key escrow, a number of authentication entities are proposed in serial, and the user’s independent blind factor \( x \), timestamp \( T \), and additivity of virtual keys are applied to the RBAC model, thus realizing inter-user communication safety and convenient management, etc.

Assignment based on role access control is also one hot research direction in recent years. In actual applications, user B does not have the corresponding authority, and user A assigns the role to user B.
so that user B has the corresponding authority to replace A in work. The next work is possibly to continually extend this scheme and apply it to the assignable role access control model. Since SUN will provide elliptic curve cryptographic functions for free in the JDK, these research results will be applied to more practical models to improve security.

References

[1] Na S, Liang T and Ciaxia Y 2020 A blockchain-based access control scheme in distributed internet of things Peer-to-Peer Networking and Applications 36 1-15.
[2] Reddy B R and Kumar A 2020 Survey on access control mechanisms in cloud environments International Conference on Advances in Computational Intelligence and Informatics pp 141-149.
[3] Zhang Y, Kasahara S and Shen L 2019 Smart contract-based access control for the Internet of things Internet of Things Journal 24 1594-1605.
[4] Xu R, Chen Y and Erik B 2020 Decentralized access control for IoT based on blockchain and smart contract Modeling and Design of Secure Internet of Things 28 505-528.
[5] Lang B, Wang J M and Liu Y X 2017 Achieving flexible and self-contained data protection in cloud computing IEEE Access 5 1510-1523.
[6] Christidis K and Devets M 2019 Blockchains and smart contracts for the internet of things 2019 International Conference on ICT for Smart Society pp 2292-2303.
[7] Azaria A, Ekblaw A and Vieira T 2016 Using blockchain for medical data access and permission management 2016 2nd International Conference on Open and Big Data (OBD) pp 633-643.
[8] Carlo B, Elisa B and Elena F 2001 Future directions in role-based access control models International Workshop on Mathematical Methods, Models, and Architectures for Network Security pp 22-26.
[9] Ding S, Cao J and Li C 2019 A novel attribute-based access control scheme using blockchain for IoT IEEE Access 7 38431-38441.
[10] Wang W F, Xiao B and Pan S 2019 Research on big data security protection system and access control technology 2019 7th International Conference on Machinery Materials and Computing Technology pp 134-136.
[11] Servos D and Osborn S L 2017 Current research and open problems in attribute-based access control International Conference on IT Convergence and Security pp 1-45.
[12] Zheng Y 1997 Digital signcryptosystem or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption) Lecture Notes in Computer Science 1294 165-179.
[13] Chen L, Harrison K and Soldera D 2003 Applications of multiple trust authorities in pairing based cryptosystems International Conference on Infrastructure Security pp 260-275.
[14] Hussein D, Bertin E and Frey V 2017 A community-driven access control approach in distributed IoT environments IEEE Communications Magazine 55 (3) 146-153.
[15] Su M, Wang L C and Fu M 2018 Proxy re-encryption based multi-factor access control for ciphertext in cloud Journal of Shanghai JiaoTong University 23 666-670.
[16] Teh T Y, Lee Y S and Cheah Z Y 2015 IBI-mobile authentication: A prototype to facilitate access control using identity-based identification on mobile smart devices 2015 5th International Conference on IT Convergence and Security pp 127-144.
[17] Pareek G and Purus B R 2018 Proxy re-encryption scheme for access control enforcement delegation on outsourced data in public cloud International Conference on Information Systems Security pp 251-271.
[18] Guan Z, Li J and Zhang Y 2016 An efficient traceable access control scheme with reliable key delegation in mobile cloud computing EURASIP Journal on Wireless Communications and Networking 208 1-11.
[19] Murari M, Gaurav S and Anil K V 2016 A computational review of identity-based signcryption schemes *International Journal of Network Security* **365** 969-977

[20] Ferraiolo D, Sand R and Gavrila S 2001 Proposed NIST standard for RBAC *International Conference on IT Convergence and Security* pp 224-274.

[21] Chen L, Harrison L, Soldera D and Nigel P 2002 Applications of multiple trust authorities in pairing based cryptosystems *International Conference on Infrastructure Security* pp 260-275.