Attribute-Based Identity Authentication Scheme Based on Linear Codes

Zhiqiang Zhang¹, Suzhen Cao¹*, Longbo Han¹ and Xueyan Liu²

¹College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China
²College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China
Email: 1187001535@qq.com

Abstract. In the multi-user application environment, the simple use of user private key to achieve identity authentication is too single and can not carry out fine-grained access control to users. And there is the problem of user key management, which is easy to produce system bottleneck. In order to solve the above problems, a traceable and revocable attribute-based authentication scheme is constructed based on linear codes, which divides user access rights in a fine-grained manner. The method of direct revocation is adopted in the scheme, and the cost of revocation is lower. When a key abuse occurs or the system suffers a denial of service attack, the true identity of the malicious user can be tracked based on the signature. Finally, the MBDH problem proves that the scheme meets unforgeability, and the performance comparison and numerical analysis show that the scheme has a shorter key length and less computational overhead.

1. Introduction
Attribute Based Encryption (ABE) was first proposed by Sahai and Waters [1] in 2005 and realized the “one-to-many” encryption and decryption mode. Different from the traditional public key encryption technology for identity authentication. ABE's identity authentication can solve the key escrow problem, and can achieve fine-grained control of user access rights, which is more suitable for the network environment where multiple users participate in encryption and decryption [2-4]. For example, in a smart community, a private key can be generated based on unique identity information such as the unit number, house number, hometown, occupation, etc. of the community residents. Flexibly formulate access strategies to make the management of personnel safer and more efficient. Zhang et al. [5] applied ABE access control and authentication to the Internet of Things. An effective access control strategy is proposed to protect the security of sensitive data in the Internet of Things, and identity authority authentication is adopted when accessing resources to classify user access levels. Li et al. [6] used ABE for access control in mobile medicine to ensure the security and effective access of personal medical records.

In practical applications, attribute revocation is an inevitable topic. Attrapadung et al. [7-8] for the first time clarified that there are two main ways of attribute revocation: direct revocation and indirect revocation. Indirect revocation completes the revocation of attributes by affecting the user's private key. Although this revocation mode is more flexible, it has a larger overhead and can easily become a system bottleneck. The direct revocation mode is to embed the revocation list in the ciphertext and complete the revocation of the user's attributes without updating the user's private key at a relatively...
low cost. In an environment where multiple users participate in authentication, we also do not want the
user to bear the high computational overhead. Therefore, this paper adopts the direct revocation
method, and the certification center maintains the attribute revocation list. Zhang et al. [9] adopted a
tree-structured access strategy and introduced an attribute revocation list to achieve fine-grained direct
attribute revocation. And prove the security of the scheme under the attack of adaptive ciphertext
selection. Qi et al. [10] also use the direct revocation mode to realize the revocation of user attributes
without updating the system public key and user private key. At the same time, the user’s identity can
be traced according to the decryption key, thereby effectively preventing the key from being leaked. Li
et al. [11] added a malicious user tracking mechanism to mobile medicine and proved its adaptive
security under the standard model. Considering the problem of key leakage in the environment where
multiple users participate in authentication and malicious users’ denial of service attacks on
authentication center, this paper adds the user’s identity tracking and attribute revocation to the
scheme. For the key abuse problem caused by key leakage in the system, the holder can be tracked and
accountable. In addition to accountability, malicious users who perform denial-of-service attacks on
the authentication center can also revoke attribute rights. Unlike the LSSS-based access structure,
Massey [12] secret sharing based on linear codes can break through the threshold limit and diversify
the attribute set of authentication participants. Based on Massey’s work, Carlet et al. [13] constructed a
secret sharing scheme with two access structures based on error correction codes for completely
nonlinear functions. Song et al. [14] introduced the theory of secret sharing schemes based on linear
codes into attribute-based signcryption schemes, which met the needs of complex attribute
applications.

In summary, this paper proposes an attribute-based identity authentication scheme suitable for
multi-user participation based on linear codes. Hereinafter referred to as the AIASLC scheme. The
main work of the thesis has the following four points:

• Combined with the advantages of ABE’s “one-to-many”, it is possible to perform fine-grained
access control on identity authentication involving multiple users. And break through the previous
“one-to-one” certification mode, improve certification efficiency.

• In attribute-based encryption, users are identified by attribute sets. Therefore, different users
may have the same attribute set, and the user identity cannot be uniquely determined. Add an identity
tracking mechanism to the AIASLC, and track and account for malicious users when necessary. This
mechanism can effectively prevent user key misuse.

• In response to a denial of service attack by a malicious user to the certification center and a
change in user attribute permissions, AIASLC added the revocation of user attribute rights. And the
direct revocation method makes revocation more efficient.

• The access structure is constructed based on linear codes, and the linear relationship between
vectors is used to construct secret values, which breaks through the threshold limit and meets the
needs of diversified attribute sets in practical applications.

2. Preliminaries

2.1. Bilinear Maps

Definition $G_1$ and $G_2$ are cyclic groups of order $p$ ($p$ is a prime number). $g$ is a generator of $G_1$, and
e:$G_1\times G_1 \rightarrow G_2$ is a map if the map satisfies the following three properties:

• Bilinear: For all $a,b \in \mathbb{Z}_p$ and $g_1,g_2 \in G_1$, we have $e(g_1^a,g_2^b) = e(g_1,g_2)^{ab}$.

• Non-degenerate: $e(g,g) \neq 1$.

• Computable: $\forall g_1,g_2 \in G_1, e(g_1,g_2)$ can be effectively calculated in polynomial time.

Then this map is called a bilinear map.
2.2. Secret Sharing Based on Linear Codes
Definition $C \subseteq V(n,q)$ is a subspace of $V(n,q)$, where $V(n,q) = \{(x_1, x_2, \ldots, x_n) | x_i \in F_q, i = 1, 2, \ldots, n\}$ represents an $n$-dimensional vector space on the finite field $F_q$, then $C$ is called a $q$-ary linear code. If $C$ is a $k$-dimensional subspace of $V(n,q)$, then $C$ is called a $[n,k;q]$ linear code, where $n$ is called the code length of $C$, and each vector in $C$ is called a code word. $C$ is a linear code if and only if:
- For any $c_1, c_2 \in C$, there is $c_1 + c_2 \in C$.
- For any $c \in C$ and $a \in F_q$, there is $ac \in C$.

When constructing a secret sharing scheme using linear code $C$, it is assumed that there are $n-1$ users $P_1, P_2, \ldots, P_{n-1}$ in the system. Let $G = (g_0, g_1, \ldots, g_{n-1})$ be the generator matrix of the linear code $C$, the center authorization authority randomly selects the vector $u = (u_0, \ldots, u_{k-1}) \in F_q^k$ and calculates the secret value $y = ug_0$. The center authorization authority calculates the code word $uG = (ug_0, ug_1, \ldots, ug_{n-1})$ corresponding to the vector $u$, and distributes the $ug_i$ to each user $P_i$ in the system, that is, $P_i = ug_i$, where $1 \leq i \leq n-1$. If $g_0$ is a linear combination of $g_1, \ldots, g_{n-1}$, then the set $\{P_1, \ldots, P_n\}$ is called the authorized subset of the access structure of the linear code $C$, that is $g_0 = \sum_{j=1}^{n-1} x_j g_j, x_j \in F_q, 1 \leq j \leq m, 1 \leq m \leq n-1$, then the secret value $y = ug_0 = \sum_{j=1}^{n-1} x_j ug_j$. The coefficients $x_j$ can be publicly calculated by the participants in the set $\{P_1, \ldots, P_n\}$ [11-13]. In summary, the access structure based on linear codes is defined as follows:
$$\Gamma = \{\{P_i, \ldots, P_n\} | g_0 \text{ is a linear combination of } g_1, \ldots, g_{n-1}\}.$$ 

2.3. Decisional Modified Bilinear Diffie-Hellman Assumption (MBDH)
Define the group $G$ of order $p$, $g$ is the generator of the group $G$, choose $a,b,c,z \in Z_p$ randomly. Let $Z = e(g, g)^{abc}$, there is no adversary can distinguish the two tuples $(g^a, g^b, g^c, Z)$ and $(g^a, g^b, g^c, g^d)$ with a non-negligible advantage in polynomial time.

3. Model Definition
3.1. Scheme Model
As shown in figure 1 the AIASLC scheme model has three main entities, namely the Central Authority (CA), Users (USER), and Authentication Center (AC).
- CA: It is a trusted organization, consisting of one or more sets of communication and computing equipment. It is used for system initialization and user key generation. The CA receives the user’s key generation request and returns the key to the user through a reliable communication channel.
- USER: Refers to the system user and can apply for a key from CA. When the user has an authentication request, the private key is used to complete the signature work, and the authentication request is made to the AC. If the user abuses the key, the AU will track the identity based on the user’s signature. If the user has a malicious denial of service attack on the authentication center or the AU needs to change the user’s attribute rights. The user will be revoked to perform attribute rights.
- AU: It is a trusted institution and contains one or more reliable computing devices. In the AIASLC scheme, AU processes user identity authentication requests, tracks malicious users based on signatures, and maintains revocation lists to manage user attribute revocation. There are two main authentication results: (1) Successful authentication. If the user attribute meets the established access policy and the attribute is not in the revocation list, then the authentication will be passed. (2)
Authentication failed. If the user attributes do not meet the specified access policy or some user attributes are in the revocation list, the authentication will fail.

3.2. Algorithm Model

- **Setup(κ, U) → (PK, MK)**: System initialization algorithm. The algorithm inputs the security parameter κ and the full set of attributes U to generate the system public key PK and the system master key MK.
- **Keygen(S_p, ID_p, PK, MK) → (sk, pk)**: Key generation algorithm. The algorithm inputs user P attribute set S_p, user unique identity ID_p, system public key PK, system master key MK, and generates user private key sk and user public key pk.
- **Usersign(PK, sk, pk) → (σ)**: User signature algorithm. The algorithm inputs the system public key PK, the user private key sk and the user public key pk, and outputs the user-generated signature σ = (σ_1, σ_2, σ_3, σ_4).
- **Authentication(PK, pk, σ, R, Γ) → (result)**: Identity authentication algorithm. The algorithm inputs the system public key PK, user public key pk, user signature σ, user attribute set R, and access structure Γ. Calculate the authentication result, and finally output Succeed or Failed.
- **Trace(σ_a) → (ID_p)**: Identity tracking algorithm. If there is a malicious user in the system that misuses the key or conducts a denial-of-service attack on the authentication center, it can be tracked for identity. The algorithm inputs the user’s signature σ_a and outputs the user’s unique identity ID_p.

3.3. Security Model

The unforgeability of the AIASLC refers to the existential unforgeability against under adaptive chosen message (EUF-CMA). Defined by the interactive game between adversary and challenger:

- Initialization: The adversary A chooses an access structure Γ* to be challenged. For the attribute i* , specify the user attribute revocation list S* and send it to the challenger C.
- System setup: Challenger C runs the system establishment algorithm. Send the generated public parameters to adversary A and save the system master key MK.
- Phase one: Adversary A adaptively conducts the following polynomial bounded query.
- Key extraction query: Adversary A queries the attribute i* in the attribute set U. Challenger C runs the key extraction algorithm and sends the key sk* to adversary A.
• Authentication query: Adversary $A$ chooses a user signature $\sigma^*$ under access structure $\Gamma^*$ and sends it to challenger $C$. Challenger $C$ runs the identity authentication algorithm and returns the authentication result to adversary $A$.

• Forgery: Adversary $A$ outputs a forged signature $\sigma^*$ about the attribute set $S^*_p$ and any identity $ID^*$. If adversary $A$ has not asked $S^*_p$ and $ID^*$ in the above game and forged signature $\sigma^*$ passed identity authentication, then adversary $A$ is successfully forged.

If there are no polynomial bounded adversaries, the game can be won with a non-negligible advantage $\epsilon$. Then the AIASLC scheme meets EUF-CMA security.

4. Scheme Construction
This section gives the specific structure of the AIASLC scheme based on linear codes. It mainly includes five algorithms: system setup, key generation, user signature, identity authentication, and identity tracking. The scheme is described as follows:

• Setup$(\kappa, U) \rightarrow (PK, MK)$: Select a bilinear group $G_i$ with prime order $p$ and generator $g$. $\kappa$ is the system safety parameter. Choose the hash function $H(x)$, which can map strings of any length to elements on $Z_p$.

Define the bilinear map $e: G_i \times G_i \rightarrow G_2$, and define the attribute set as $U = \{1, 2, \ldots, n\}$. According to the secret sharing scheme based on linear codes [15-16], the access structure is defined as $\Gamma$, satisfying $\Gamma = \{\{i_1, \ldots, i_m\} | \{P_{i_1}, \ldots, P_{i_m}\} \in \Gamma\}$. Choose $t_i \in Z_p$ randomly, where $i \in U$.

Then the system public key $PK$ is: $\{T_i = g^{bi}, T_i = g^{i_2}, \ldots, T_{y(i)} = g^{bi}\}$ and the system master key $MK$ is: $\{t_1, t_2, \ldots, t_{|U|}\}$.

• Keygen$(S_p, ID_p, PK, MK) \rightarrow (sk, pk)$: Let $S_p$ be the set of attributes of user $P$, where $S_p \in \Gamma$. $ID_p$ is the user’s unique identity, and $G = (g_{00}, g_{10}, \ldots, g_{n-1})$ is the $[n, k; p]$ linear code generation matrix.

(1) Randomly select the vector $u = (u_0, \ldots, u_{k-1}) \in F_p^k$ and calculate $y = u \cdot g^0$, $Y = g^y$, $W_i = g^{u_i}$, where $i \in S_p$.

(2) Choose $\alpha \in Z_p^*$ randomly and calculate $I_0 = g^{y + \alpha H(I_{0p})}, I_1 = g^{\alpha H(I_{1p})}, E = ID_p \cdot e(I_{0}, g)$. Then the user’s private key $sk$ is: $\{W, y, I_1, E\}$ and the user’s public key $pk$ is $\{PK, Y\}$.

• Usersign$(PK, sk, pk) \rightarrow (\sigma)$: User $P$ randomly selects $x \in Z_p^*$ and calculates $\sigma_1 = W_i, \sigma_2 = g^{r}, \sigma_3 = g^{\frac{1}{x}}, \sigma_4 = I_1 \| E$. Generate the final signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and send it to the authentication center.

• Authentication$(PK, pk, \sigma, R, \Gamma) \rightarrow (result)$: After receiving the user’s signature, the authentication center performs the following operations:

(1) First calculate the coefficient $\lambda_i$, where $\lambda_i$ satisfies $g_0 = \sum_{i \in S_p} \lambda_i g_i$, where $S_p = S_p - S$, where $S$ is the set of revoked attributes.

(2) Calculation verification equation: $\prod_{i \in S_p} e(\sigma_i, T_i)^{\lambda_i} = e(Y, \sigma_2)$ and $e(Y \sigma_2, \sigma_3) = e(g, g)$. If the user attribute set satisfies the access structure $\Gamma$, the equation is established and the identity authentication is successful.
• Trace(σₜ) → (IDₚ): The certification center uses the signature σₜ of user P for identity tracking and calculates E / e(Iₜ, g)e(Y, g) = IDₚ.

5. Comprehensive Analysis

5.1. Correctness Analysis

In the above AIASLC scheme, if some attributes of the user have been revoked by the authentication center. That is, the access structure is no longer satisfied rₖ ∈ Γ, and the authentication center cannot obtain the correct coefficient rₖ through g₀ = ∑ₖ rₖ gₖ. As a result, in the further calculation, the correct g₀ cannot be recovered. That is, the equation is not established and the identity authentication fails.

If the attribute of user P is not in the revoked set, that is P S = ∅, rₖ ∈ Γ meet the access structure. Then it will pass the certification. Given:  

\[ (Y, Y_{12}) = (g^y, g^{\frac{1}{(g^y, g^x)})} = e(Y, \sigma_2) \]

That is, \( \prod_{i \in S_y} e(\sigma_i, T_i)^{\lambda_i} = e(Y, \sigma_2) \) is established. Secondly:

\[ e(Y \sigma_2, \sigma_1) = e(g^y g^x, g^{\frac{1}{(g^y, g^x)})} = e(g, g) \]

(2)

From the above analysis, it can be concluded that the authentication scheme is correct.

In the proposed AIASLC scheme, when a malicious user appears in the system. The true identity of the malicious user can be tracked according to the user’s signature σₜ:

• The certification center first calculates: e(Iₜ, g)e(Y, g).

• Secondly, calculate E / e(Iₜ, g)e(Y, g) to get the user’s real identity IDₚ:

\[ \frac{E}{e(Iₜ, g)e(Y, g)} = \frac{E}{e(g^{a_I g_{IDₚ}}), g)e(g^y, g)} = \frac{IDₚ \cdot e(Iₜ, g)}{e(g^{g^y a_I g_{IDₚ}}), g) = IDₚ = IDₚ} \]

(3)

5.2. Unforgeability Proof

Theorem 1. If the MBDH assumption is established, then the AIASLC scheme meets the existence of unforgeability under the adaptive selection message attack.

Proof. Suppose there is a polynomial time algorithm that allows adversary A to win the game with a non-negligible advantage \( \varepsilon \) within the bounded time of the polynomial. Then challenger C can use adversary A to solve the MBDH problem with a non-negligible probability \( \frac{\varepsilon}{2} \) in polynomial time.

• Initialization: Challenger C chooses a bilinear group \( G_1 \) with prime order \( p \) and generator \( g \).

And then define the bilinear map \( e: G₁ \times G₁ \rightarrow G₂ \), the complete set of attributes \( U \). Challenger C plays a coin-tossing game, randomly selecting \( \theta \in \{0,1\} \) and \( a, b, c, z \in \mathbb{Z}_p \). Set
\((A,B,C,Z) = \left(g^a, g^b, g^c, e(g,g)^c\right)\) when \(\theta = 0\), and set \((A,B,C,Z) = \left(g^a, g^b, g^c, e(g,g)^c\right)\) when \(\theta = 1\). Adversary \(A\) declares the access structure \(\Gamma^*\) to be challenged. For attribute \(i^*\), specify user attribute revocation list \(S^*\) and send it to challenger \(C\).

- System setup: Challenger sets the public key parameter \(Y = A = g^a\) firstly. For \(i^* \in U\) in the set, if \(i^* \in S^*_p\), choose \(\beta_i \in \mathbb{Z}_p\) randomly. Let \(T_p = g^{c\beta_i} = C^{\beta_i}\), that is \(t_i = c\beta_i\). Otherwise, randomly choose \(\gamma_{i'} \in \mathbb{Z}_p\). Let \(T_p = g^{\gamma_{i'}}\), which means \(t_i = \gamma_{i'}\), and then send the public key \(PK = \{Y, T_p\}\) to adversary \(A\).

- Phase one: In this phase, Challenger \(C\) answers the enquiry of adversary \(A\) according to the following process.

  - Key extraction inquiry: Adversary \(A\) performs an adaptive key extraction query on \(i^* \in U\) in the set, and challenger \(C\) defines the key tuple \(W_{i^*}\). When \(i^* \in S^*_p\), select \(k_{\iota^*} \in \mathbb{Z}_p\) randomly so that \(W_{i^*} = g^{k_{\iota^*}}\). Otherwise, choose \(\xi_{i^*} \in \mathbb{Z}_p\) randomly and let \(W_{i^*} = g^{\xi_{i^*}}\). That is, when \(i^* \in S^*_p\), \(u_{\iota^*} = c\beta_i k_{\iota^*}\), when \(i^* \notin S^*_p\), \(u_{\iota^*} = \xi_{i^*}\).

  - Authentication inquiry: Adversary \(A\) can select a user signature \(\sigma^* = (\sigma_i^*, \sigma^*_i, \sigma^*_i, \sigma^*_i)\) under access structure \(\Gamma^*\) at any time and send it to challenger \(C\) for authentication query. Challenger \(C\) runs the identity authentication algorithm and returns the authentication result to adversary \(A\).

  - Forgery: Adversary \(A\) submits two equal-length messages \(ID_0\) and \(ID_1\) to challenger \(C\). Challenger \(C\) selects \(\theta \in \{0,1\}\) randomly and runs a signature algorithm to generate a challenge ciphertext \(W_{i^*} = g^{k_{\iota^*}}, CT^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^* = B^{\delta^*}, \sigma_5^* = B^{\xi^*}, \sigma_6^* = Z)\) with message \(ID_0\) under \(\Gamma^*\).

  When \(\mu = 0\), \(Z = e(g,g)^c\), let \(\delta = \frac{b}{c}\), then:

\[
\sigma_1^* = W_{i^*}^{\delta^*} \tag{4}
\]

\[
\sigma_2^* = B^{\delta^*} = g^{\frac{b}{c} \delta^*} = g^{\delta^* \beta^*} = T_p^{\delta^*} \tag{5}
\]

\[
\sigma_3^* = B^{\xi^*} = g^{\delta^* \xi^*} = g^{\delta^* \beta^*} = W_p^{\delta^*} \tag{6}
\]

\[
\sigma_4^* = ID_p Z = ID_p e(g,g)^{\delta^*} = ID_p e(g,g)^{\delta^*} \tag{7}
\]

When \(\mu = 1\), \(Z = e(g,g)^c\), then \(\sigma_1^* = ID_p Z = ID_p e(g,g)^{\delta^*}\). Because \(z \in \mathbb{Z}_p\) and randomly selected, then \(\sigma_1^*\) will be a random element in group \(G_2\). In other words, \(\sigma_4^*\) will not include any information about \(ID_0\).

When \(\theta = \theta^*\), Challenger \(C\) outputs \(\mu^* = 0\), which means that the above given is an MBDH tuple. When \(\theta \neq \theta^*\), Challenger \(C\) outputs \(\mu^* = 1\), which means that the given above is a random value.

When \(\mu = 1\), the adversary will not get any information about \(ID_0\), then there is \(Pr(\theta = \theta^* | \mu = 1) = \frac{1}{2}\). Because when \(\theta \neq \theta^*\), Challenger \(C\) guesses \(\mu^* = 1\), then there is
Pr[\mu = \mu^* | \mu = 1] = \frac{1}{2}. When \mu = 0, the advantage of adversary \(A\) is defined as \(\epsilon\), so there is

\[
Pr[\theta = \theta^* | \mu = 0] = \frac{1}{2} + \epsilon.
\]

Because when \(\theta = \theta^*\), challenger \(C\) guesses \(\mu^* = 0\), then there is

\[
Pr[\mu = \mu^* | \mu = 0] = \frac{1}{2} + \epsilon.
\]

In summary, the advantages of challenger \(C\) in the decisional MBDH game are as follows:

\[
\frac{1}{2} Pr[\mu = \mu^* | \mu = 1] + \frac{1}{2} Pr[\mu = \mu^* | \mu = 0] - \frac{1}{2} = \frac{1}{2} (\frac{1}{2} + \epsilon) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} = \frac{1}{2} \epsilon
\]

(8)

Challenger \(C\) must possess the key \(sk = \{W_i, y, I_i, E\}\) to forge the signed ciphertext. Where \(\frac{\mu}{W_i} = g^{h}\), \(y = ug_0\), and \(I_i\) is the system master key, which is randomly selected and satisfies \(I_i \in \mathbb{Z}_p\). \(ug_i\) is the corresponding codeword generated by the random vector \(u\). If calculating the secret value \(y\), you need to obtain \(g_0\) by calculating \(\lambda_i\) firstly. \(g_0\) satisfies \(g_0 = \sum_{j=1}^{\infty} \lambda_j g_{i_j}\), and the coefficient \(\lambda_j\) is calculated publicly by the participants in the set \(\{P_1, \ldots, P_n\}\). Therefore, adversary \(A\) cannot obtain the private key \(sk\). If adversary \(A\) can obtain the private key \(sk\), it means that the challenger \(C\) can use adversary \(A\) to solve the difficult problem of decisional MBDH with a non-negligible probability \(\frac{\epsilon}{2}\).

Obviously, this is impossible, then the assumption is not true. Therefore, the AIASLC scheme proposed in this paper satisfies the existential unforgeability.

5.3. Performance Analysis

It can be seen from table 1 that the length of the public key of the AIASLC scheme system is significantly smaller than Li [6], Zhang [9], Qi [10]. Li [6] involves the public key parameters of multiple authorities, Zhang [9] A signature algorithm is encapsulated in the public key parameters. The length of the ciphertext of the AIASLC scheme is slightly larger than Li [6] and smaller than Zhang [9]. The length of the ciphertext of Zhang [9] is related to the number of authorized authorities and is not much different from Qi [10]. AIASLC scheme user private key length is shorter than Li [6], Zhang [9] and Qi [10].

As can be seen from table 2, Li [6] does not support attribute revocation and user identity tracking. Zhang [9] only supports user identity tracking. Both Qi [10] and AIASLC scheme support attribute revocation and user identity tracking. In terms of computational overhead, the AIASLC scheme is significantly better than Li [6], Zhang [9], and Qi [10]. The AIASLC scheme uses fewer pair operations and exponential operations.

| Scheme | System public key | Ciphertext length | User private key |
|--------|-------------------|-------------------|-----------------|
| Li [6] | \((n + F + 3)|G_1| + F|G_2|\) | \((n + 2)|G_1|\) | 2\(n|G_1|\) |
| Zhang [9] | \((n + 3)|G_1| + 2|G_2| + Sign\) | \((F + 2)|G_1| + F|G_2|\) | \((n + 1)|F|G_1|\) |
| Qi [10] | \((n + 2)|G_1| + |G_2|\) | \((n + 2)|G_1| + 2|G_2|\) | \((n + 3)|G_1| + 1\) |
| AIASLC | \(n|G_1|\) | \((n + 3)|G_1| + |G_2|\) | \((n + 1)|G_1| + |G_2| + 1\) |

\(^a|G_1||G_2|\): Group element length; \(^bF\): Number of authority in the system; \(^cSign\): Signature algorithm.
Table 2. Computation cost and feature comparison.

| Scheme  | Encryption-Signature | Decryption-Authentication | Revocable | Traceable |
|---------|-----------------------|---------------------------|-----------|-----------|
| Li [6]  | \((2n+1)E + nP\)     | \((2n^2 + n + 3)P\)      | NO        | NO        |
| Zhang [9]| \((3n + 3)E\)        | \((n + 2)E + (2n + 1)P\) | NO        | YES       |
| Qi [10] | \((n + 2)E + 2P\)    | \((n + 5)P + E\)         | YES       | YES       |
| AIASLC  | \((n + 2)E + 1\)     | \((n + 3)P\)             | YES       | YES       |

*P*: Bilinear pairing; \(E\): Exponential calculation.

In 64bit memory 8GB Windows 7 system, i5-3230M 2.60GHzCPU notebook computer. Through the IntelliJ IDEA platform, JPBC was used to numerically analyze the AIASLC scheme with Li [6], Zhang [9], and Qi [10].

As shown in figure 2, the running time comparison of Li [6], Zhang [9], Qi [10] and AIASLC scheme. Since the application environment of Li [6], Zhang [9], Qi [10] is different from the AIASLC scheme, this section counts the total running time of the scheme’s encryption and decryption. The running time of Li [6], Zhang [9], Qi [10] includes user encryption time and decryption time. The running time of AIASLC scheme includes user’s signature and decryption authentication time. The Zhang [9] scheme is constructed on a composite order group, and its cost is larger than that on a prime order group. The total cost of the encryption and decryption phase is about 45.54s, which is not comparable, so it is not shown in figure 2. For display. Compared with Li [6] and Qi [10], as the number of attributes increases, the computational cost increases linearly, but it is obvious that the AIASLC scheme takes less time.

In summary, compared with Li [6], Zhang [9], Qi [10], the overall computational cost of the AIASLC scheme is lower, and the numerical analysis experiment results are basically consistent with the results in table 2.

Figure 2. Run time comparison.

6. Conclusions
This paper combines the characteristics of attribute-based encryption “one-to-many”, and gives a scheme suitable for multiple users to participate in identity authentication based on linear codes. While realizing the revocation of user attributes, it can track the identity of malicious users in the system. It can effectively prevent key misuse and denial of service attacks against authentication centers. The MBDH assumption proves the unforgeability of the scheme. The numerical analysis and efficiency comparison of the scheme are also carried out. In the future, the efficiency of the algorithm will be further optimized on the basis of the existing, and the application in specific scenarios will be considered.
Acknowledgments
This research was funded by the National Natural Science Foundation of China (Grant No. 61662071 and 61662069).

References
[1] Sahai A and Waters B 2005 Fuzzy identity-based encryption Proceeding of Advances in Cryptology—EUROCRYPT 2005 (Berlin: Springer-Verlag) pp 457-473.
[2] Usha S and Tamilarasi A 2019 A trust based security framework with anonymous authentication system using multiple attributes in decentralized cloud Cluster Computing 22 (2) 3883-3892.
[3] Wang H, Zheng Z H, Wu L, et al. 2017 New directly revocable attribute-based encryption scheme and its application in cloud storage environment Cluster Computing 20 (3) 2385-2392.
[4] Cui H, Yuen T Hon, Deng Robert H, et al. 2020 Server-aided revocable attribute-based encryption for cloud computing servicesConcurrency Computat: Pract. Exper. e5680.
[5] Zhang Q, Li Y, Li Z, et al. 2019 Access control based on ciphertext attribute authentication and threshold policy for the internet of things Sensors 19 (23) 5237-5258.
[6] Li Q, Zhu H B, Xiong J B, et al. 2019 Fine-grained multi-authority access control in IoT-enabled mHealth Annales Des Télécommunications 74 (7) 389-400.
[7] Attrapadung N and Imai H 2009 Conjunctive Broadcast and Attribute-Based Encryption International Conference on Pairing-Based Cryptography pp 248-265.
[8] Attrapadung N, Libert B, and Panafieu E. 2011 Expressive key-policy attribute-based encryption with constant-size cipher-texts International Conference on Practice and Theory in Public Key Cryptography pp 90-108.
[9] Zhang W, Chen Z, Liu X D, et al. 2019 CP-ABE scheme supporting fine-grained attribute direct revocation Journal of Software 30 (9) 2760-2771.
[10] Qi F, Li Y and Tang Z 2018 Revocable and traceable key-policy attribute-based encryption scheme Journal on Communications 39 (11) 63-69.
[11] Li Q, Zhu H B, X J B, et al. 2018 Multi-authority attribute-based access control system in mHealth with traceability Journal on Communications 39 (06) 1-10.
[12] Massey J L 1993 Minimal codewords and secret sharing Proc. 6th Joint Swedish-Russian Workshop on Information Theory pp 276-279.
[13] Carlet C, Ding C, Yuan J, et al. 2005 Linear codes from perfect nonlinear mappings and their secret sharing schemes IEEE Transactions on Information Theory 51 (6) 2089-2102.
[14] Song Y, Li Z H, Li Y M, et al. 2017 Attribute-based signcryption scheme based on linear codes Information Sciences 301-309.
[15] Li Z H, Xue T and Lai Hong 2010 Secret sharing schemes from binary linear codes Information Sciences 180 (22) 4412-4419.
[16] Song Y, Li Z H, Li Y M, et al. 2015 A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes Security and Communications Networks 8 (2) 202-211.