Wuhan University
Journal of Natural Sciences

2023, Vol.28 No.4, 317-323

Article ID 1007-1202(2023)04-0317-07
DOI https://doi.org/10.1051/wujns/2023284317

An Anonymous Authentication Scheme with Selective Linkability and Threshold Traceability

PU Guangning[1], YIN Fengmei[2]

1. Information Engineering Faculty, Anhui Finance and Trade Vocational College, Hefei 230601, Anhui, China;
2. School of Computing and Artificial Intelligence, Hefei Normal University, Hefei 230601, Anhui, China

Abstract: In order to protect the user's privacy identity, authentication requires anonymous authentication. Anonymous authentication is divided into unconditional anonymous authentication and traceable anonymous authentication. Unconditional anonymous authentication can verify that the user belongs to an anonymous set, but the user's true identity cannot be obtained. However, in some applications, it is necessary to trace the true identity of the user. Therefore, a traceable anonymous authentication scheme is proposed. In order to prevent random tracing, the proposed scheme uses threshold joint tracing. When the identity of the authenticator needs to be traced, the threshold number of members can jointly trace the identity of the authenticator. In some special network applications such as anonymous electronic voting, in order to prevent repeated authentications and repeated elections, it is necessary to verify whether the two authentication signatures are signed by the same user without revealing the true identity of the user. Therefore, the proposed anonymous authentication scheme should have selective linkability. In order to achieve linkable authentication, the linkable tag is embedded by linkable ring signature. Compared with similar schemes through the simulation experiments, the implementation time of the proposed scheme is slightly better than other schemes.

Key words: anonymous authentication; traceability; threshold; ring signature; linkability
CLC number: TP309.7

0 Introduction

In some special applications today, based on computational intelligence[1,2], identity authentication requires anonymous authentication to protect user's privacy information[3]. Anonymous authentication is divided into unconditional anonymous authentication and traceable anonymous authentication. Unconditional anonymous authentication can verify that the user belongs to an anonymous set, but the user's true identity cannot be obtained. At the same time, criminals often use unconditional anonymity to engage in criminal activities, since their true identity cannot be traced, they cannot be punished. In order to prevent illegal and criminal activities from being unable to trace their true identity, traceable anonymous authentication schemes have emerged.

Anonymous authentication is often accompanied by anonymous signature. Using ring signature[4], with the help of an administrator and a verifier, Tian *et al*[5] can trace the privacy identity of the authenticator. But the

Received date: 2022-12-27
Foundation item: Supported by the Key Natural Science Foundation of Anhui Higher Education Institutions (2022AH052536)
Biography: PU Guangning, male, Professor, research direction: information security. E-mail: pgn_578@126.com

program only needs an administrator and a verifier to complete the tracing, which increases the risk of conspiracy attack. Using the democratic group signature[6], Liu *et al*[7] can trace the authenticator's privacy identity through cooperation with members whose number exceeds the threshold. However, the anonymous set size of the scheme is the total number of members n, and the authenticator cannot choose the anonymous set on its own. By using $1/n$ signature[8], the authenticator can independently choose the anonymous set, so Yin *et al*[9] can threshold trace the authenticator's privacy identity.

Anonymous authentication first needs to ensure the anonymity of users, and in some special applications, it is necessary to verify whether the identity authentication of the same person is the same in different occasions without disclosing the user's real identity. For example, anonymous electronic voting not only needs to ensure the anonymity of the voter's identity, but also needs to avoid repeated voting. But none of the above traceable anonymous authentication schemes have this linkable authentication. If the linkablity feature of ring signature is applied to anonymous authentication, linkable authentication can be achieved. Beullens *et al*[10] constructed linkable ring signatures (LRS) from isogeny and lattice assumptions. However, either the speed of isogeny-based LRS is relatively slow, or the lattice based LRS has larger signatures. Liu *et al*[11] proposed a linkable spontaneous anonymous group (LSAG) signature scheme, which enables two signatures of the same signer to be linked. In addition, they demonstrated the security of the signature using an improved bifurcation lemma. In this paper, based on the LSAG signature scheme, a selective linkable threshold tracing anonymous authentication scheme is proposed.

Based on the decisional Diffie-Hellman (DDH) assumption and discrete logarithm assumption, the proposed scheme can achieve linkable authentication without disclosing the user's real identity. The main contributions of this paper can be summarized as follows:

1) By embedding the linkable label to the authentication signature, the proposed scheme can achieve linkable authentication.

2) By using threshold joint tracing, the proposed scheme can realize anonymous tracing.

3) By the simulation experiment, the implementation time of the proposed scheme is slightly better than other similar schemes. Based on the DDH assumption and discrete logarithm assumption, the security of the scheme has been proven in the scheme analysis.

The rest of this paper is organized as follows. Some relevant basic theories are proposed in Section 1. A new anonymous authentication scheme is introduced in Section 2. Security analysis is provided in Section 3. Further analysis is performed in Section 4 and the conclusion is made in Section 5.

1 Preliminary

1.1 DDH Assumption

Let $G=<g>$ be a cyclic group of prime order q, which is determined by some security parameter n. For sufficient large q, define two 4-tuples (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c), where $a, b, c \in_R Z_q$. The DDH problem is to distinguish the two tuples.

A probabilistic polynomial time (PPT) distinguisher D's advantage is defined as

$$\mathrm{Adv}_{G,D}^{\mathrm{DDH}}(n)=|\Pr[D(g,g^a,g^b,g^{ab})=1] -\Pr[D(g,g^a,g^b,g^{ab})=1]|$$

If the advantage of any distinguisher D is negligible in n, we say that the DDH assumption holds.

1.2 Linkable Ring Signature

Assuming that n users make up the ring $U=\{U_1, U_2, \cdots, U_n\}$, the public/private key pair for each user U_i in the ring is (x_i, y_i), signer U_k uses its own private key x_k and the public key collection of all members $\mathrm{UA}=\{y_1||y_2||\cdots||y_n\}$ to generate a ring signature on message m.

1) Ring signature generation algorithm

Enter the message m, public key set UA, the private key x_k of signer U_k, and add the linkable label $\tilde{e}$. Output linkable ring signature $\sigma \leftarrow (m, y_1, y_2, \cdots, y_n, x_k, \tilde{e})$.

2) Ring signature verification algorithm

Enter $\sigma \leftarrow (m, y_1, y_2, \cdots, y_n, x_k, \tilde{e})$ output 0 or 1. 0 indicates that the signature is invalid, and 1 indicates that the signature is valid. The linkable ring signature needs to meet the following properties.

• **Correctness**: Any member of the ring can execute the ring signature generation algorithm and pass the ring signature verification algorithm.

• **Anonymity**: The probability of identifying ring membership by ring signature is less than $1/n$, that is, ring membership remains anonymous.

• **Unforgeability**: Illegal members falsify the signature $\sigma \leftarrow (m, y_1, y_2, \cdots, y_n, x_k', \tilde{e}')$ of signer U_k, thus it is impossible to verify the algorithm by linkable ring signature.

• **Linkability**: If two signatures

$$\sigma \leftarrow (m, y_1, y_2, \cdots, y_n, x_k, \tilde{e})$$

$$\sigma' \leftarrow (m', y_1', y_2', \cdots, y_n', x_k, \tilde{e})$$

have the same linkable label $\tilde{e}$, it can be judged that the two signatures were signed by the same signer.

2 Proposed Anonymous Authentication Scheme

2.1 System Initialization

n members make up a collection of $U=\{U_1, U_2, \cdots, U_n\}$, exposing $\{p,q,g,t,H,\mathrm{ID}_i\}$. Among them, p and q are large prime numbers, and $q|p-1$, g is the q-order element on Z_q, t is the threshold value, H is one-way hash function, ID_i is the identity of the member U_i.

Step 1 Each U_i randomly selects the $t-1$ secondary polynomial $f_i(x)$, exposes the polynomial coefficient commitment v_{ik}, calculates $f_i(\mathrm{ID}_j)$, and sends it to U_j via a secure channel, retaining the $f_i(\mathrm{ID}_i)$.

$$f_i(x)=\sum_{k=0}^{t-1} a_{ik}x^k \bmod q \tag{1}$$

$$v_{ik}=g^{a_{ik}} \bmod p \ (k=0,1,\cdots,t-1) \tag{2}$$

$$v_0=\sum_{i=1}^{n} v_{i0} \bmod q = g^{a_0} \bmod p \tag{3}$$

Step 2 U_j checks the correctness of $f_i(\mathrm{ID}_j)$ through formula (4) , calculates the private key x_j according to formula (5) and keeps secret, y_j will be disclosed as the public key. Other members can verify the correctness of y_j through the formula (7).

$$g^{f_i(\mathrm{ID}_j)}=\prod_{k=0}^{t-1} {v_{ik}}^{\mathrm{ID}_j^k} \bmod p \tag{4}$$

$$x_j=\sum_{i=1}^{n} f_i(\mathrm{ID}_j) \bmod q \tag{5}$$

$$y_j=\mathrm{g}^{x_j} \bmod p \tag{6}$$

$$y_j=\prod_{i=1}^{n}\prod_{k=0}^{t-1} {v_{ik}}^{\mathrm{ID}_j^k} \bmod p \tag{7}$$

2.2 Anonymous Authentication

Suppose the message that needs to be signed is $m\in\{0,1\}^*$, and the public key set is $\mathrm{UA}=\{y_1\|y_2\|\cdots\|y_n\}$. The authenticator U_k uses the private key x_k and the public key set UA to generate the signature σ using the linkable ring signature[11], and sends σ to the verifier U_v. If the result outputs 1, U_k belongs to the collection U, otherwise it does not belong to the collection U. The authentication process consists of two algorithms: signature generation and signature authentication.

1) Signature generation

The authenticator U_k follows the steps below.

Step 1 Select random number $t_k, r\in Z_q$, calculate and expose T_k, W_k and linkable label $\tilde{e}$.

$$T_k=g^{t_k} \bmod p \tag{8}$$

$$W_k=v_0^{t_k}y_k \bmod p \tag{9}$$

$$\tilde{e}=t_k^{-1}r \bmod p \tag{10}$$

Step 2 For $i=k$, select random number $u\in Z_q$ and secure Hash function $H_i: \{0,1\}^*\rightarrow Z_q$, calculate c_{k+1}.

$$c_{k+1}=H_{k+1}(\mathrm{UA}\|m\|\tilde{e}\|g^u \bmod p) \tag{11}$$

For $i=k+1,\cdots,n,1,\cdots,k-1$, select random number $s_i\in Z_q$, calculate c_{i+1}, make $H_{n+1}=H_1$.

$$c_{i+1}=H_{i+1}(\mathrm{UA}\|m\|\tilde{e}\|g^{s_i}T_k^{c_i}y_i^{c_i} \bmod p) \tag{12}$$

Step 3 Calculate s_k.

$$s_k=u-(t_k+x_k)c_k \bmod q \tag{13}$$

Step 4 Generate the signature $\sigma_L(m)$ and send it to the verifier U_v.

$$\sigma_L(m)=(c_1, H_1, \cdots, H_n, s_1\cdots, s_n, \tilde{e}, r) \tag{14}$$

2) Signature authentication

The verifier U_v receives the signature $\sigma_L(m)$, and verifies the correctness of the ring signature.

For $i=1,2,\cdots,n$, z_i is calculated in (15) and $c_{i+1}(i\neq n)$ is calculated in accordance with the formula (16). If the formula (17) is established and the signature is correct, U_k belongs to set U, output 1. Otherwise, U_k does not belong to set U, output 0.

$$z_i=g^{s_i}T_k^{c_i}y_i^{c_i} \bmod p \tag{15}$$

$$c_{i+1}=H_{i+1}(\mathrm{UA}\|m\|\tilde{e}\|z_i \bmod p) \tag{16}$$

$$c_1=H_{n+1}(\mathrm{UA}\|m\|\tilde{e}\|z_n \bmod p) \tag{17}$$

2.3 Linkable Authentication

In different situations, the authenticator may produce a different signature. To prevent consistency attacks, two different signatures need to be non-related. However, on special occasions, such as anonymous electronic voting systems, anonymous authentication requires linkable authentication in order to prevent duplicate voting.

Two different authentication signatures are $\sigma_{L1}(m_1)$ and $\sigma_{L2}(m_2)$.

$$\sigma_{L1}(m_1)=(c_1', H_1', \cdots, H_n', s_1'\cdots, s_n', \tilde{e}, r) \tag{18}$$

$$\sigma_{L2}(m_2)=(c_1, H_1, \cdots, H_n, s_1\cdots, s_n, \tilde{e}, r) \tag{19}$$

If the authenticator uses the same $(\tilde{e}, r)$, anonymous authentication is relevant. Otherwise, it is not. The authenticator determines whether the anonymous identity is relevant by verifying that two different anonymous au-

thentications have the same $(\tilde{e}, r)$.

2.4 Anonymous Tracing

Linkable authentication can only prove whether two authentication are relevant and does not obtain the true identity of the authenticator. In some cases, the anonymous identity of the authenticator also needs to be traced. For example, in the anonymous electronic voting system, some users use anonymous identities to repeatedly vote. At this time, it is necessary to trace the anonymous identities of such users. In order to prevent random tracing, this scheme uses threshold joint tracing.

Assume that the t members $u_i (1 \leqslant i \leqslant t)$ consist of an anonymous trace set $\mathrm{UT}=\{U_1, U_2, \cdots, U_t\}$, and follow the steps below.

Step 1 Use private key $x_i (1 \leqslant i \leqslant t)$ and T_k to jointly calculate E_k.

$$E_k = \prod_{i=1}^{t} T_k^{x_i h_i} \bmod p \tag{20}$$

In the formula,

$$h_i = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-\mathrm{ID}_j}{\mathrm{ID}_i - \mathrm{ID}_j} \bmod q \tag{21}$$

Step 2 Query the public W_k, calculate the identity information of the authenticator y_k according to formula (22).

$$\frac{W_k}{E_k} \bmod p = y_k \tag{22}$$

3 Characteristics Analysis

Theorem 1 (Anonymous authentication) Under DDH assumption, the authenticator's anonymous identity can pass authentication.

Proof It is available by formula (12), when $i=k+1, \cdots, n, 1, \cdots, k-1$,

$$c_{k+2} = H_{k+2}(\mathrm{UA}||m||\tilde{e}||g^{s_{k+1}} T_k^{c_{k+1}} y_{k+1}^{c_{k+1}} \bmod p)$$
$$\vdots$$
$$c_{n+1} = H_{n+1}(\mathrm{UA}||m||\tilde{e}||g^{s_n} T_k^{c_n} y_n^{c_n} \bmod p)$$
$$\vdots$$
$$c_k = H_k(\mathrm{UA}||m||\tilde{e}||g^{s_{k-1}} T_k^{c_{k-1}} y_{k-1}^{c_{k-1}} \bmod p)$$

When $i=k$, it is available by formula (11) and (13),

$$\begin{aligned} c_{k+1} &= H_{k+1}(\mathrm{UA}||m||\tilde{e}||g^{u} \bmod p) \\ &= H_{k+1}(\mathrm{UA}||m||\tilde{e}||g^{s_k + (t_k + x_k)c_k} \bmod p) \\ &= H_{k+1}(\mathrm{UA}||m||\tilde{e}||g^{s_k} T_k^{c_k} y_k^{c_k} \bmod p) \end{aligned}$$

It can be seen that $c_{k+1} (i=k)$ is consistent with $\{c_i\}$ $(i=k+1, \cdots, n, 1, \cdots, k-1)$, that is, the sequence $\{c_i\} (i=1, 2, \cdots, n)$ is consistent during the generation and authentication of ring signatures, so there is

$$\begin{aligned} c_{n+1} &= H_{n+1}(\mathrm{UA}||m||\tilde{e}||g^{s_n} T_k^{c_n} y_n^{c_n} \bmod p) \\ &= H_1(UA||m||\tilde{e}||g^{s_n} T_k^{c_n} y_n^{c_n} \bmod p) = c_1 \end{aligned}$$

formula (17) is valid, U_k can pass authentication.

During the signature generation process, the $s_i \in Z_q$ $(i=1, 2, \cdots, k, k-1, \cdots, n)$ contained in the signature sent by the authenticator is randomly selected and evenly distributed on Z_q. Therefore, the probability that the verifier calculates the true identity of the authenticator from the authentication signature $\sigma_L(m)$ is $1/q^n$ which is negligible. That is, the authenticator's identity can pass anonymous authentication.

Theorem 2 (Signature unforgeability) Under adaptive chosen message and selective public key attack, signature generation satisfies unforgeability.

Proof Referring to the non-counterfeiting proof method[12], it is assumed that there is a probabilistic polynomial algorithm PPT, a stochastic predictor $H_i (i=1, 2, \cdots, n)$, and a signature prophecy machine SO(m, UA). Counterfeiter A can simulate signature prophecy machine SO through PPT simulator sim, get each H_i, and in line with the signature prophecy machine SO prophecy. Because the private key x_i cannot be obtained, A only uses H_i and SO to simulate the signature generation process, and generate a signature σ. A follows the steps below.

Step 1 Randomly select $c_i \in Z_q (i=1, 2, \cdots, n), t_k, r \in Z_q$, and compute $\tilde{e} = t_k^{-1} r \bmod p$ and $T_k = g^{t_k} \bmod p$.

Step 2 For $i=k, \cdots, n, 1, \cdots, k-2$, randomly select $s_i \in Z_q$, calculate $z_i = g^{s_i} T_k^{c_i} y_i^{c_i} \bmod p$, $c_{i+1} = H_{i+1}(\mathrm{UA}||m||\tilde{e}||z_i)$. Among them, let $H_{n+1} = H_1$.

Step 3 Let $H_k(\mathrm{UA}||m||\tilde{e}||z_{k-1}) = c_k$, find z_{k-1}, and then find s_{k-1}.

Step 4 Output signature

$$\sigma = (c_1, H_1, \cdots, H_n, s_1, \cdots, s_n, \tilde{e}, r).$$

When A forges signature σ, it is necessary to inquire H_i n times $Q_{i_1}, Q_{i_2}, \cdots, Q_{i_n}$, $1 \leqslant i_1 < i_2 < \cdots < i_n$. A's inquiry about SO is negligible. Assuming that q-th $Q_{q_1}, Q_{q_2}, \cdots, Q_{q_n}$ are the n inquiries that satisfy the consistency with the validation equation, where Q_{q_k} is an inquiry into the stochastic predictor H_k satisfying $Q_{q_k} \to H_k(\mathrm{UA}||m||\tilde{e}||g^{s_{k-1}} T_k^{c_{k-1}} y_{k-1}^{c_{k-1}} \bmod p)$, k is a gap in the ring signature σ. So, A forges signature σ for (q,k)-forged signature.

At the beginning of the simulation, A selects a pair (q,k) through sim, and can query the stochastic predictor $H_i (i=1, 2, \cdots, n)$ up to q_h times, and the signature proph-

ecy machine SO(m, UA) can be asked for up to q_s times. Within the time ε, A takes the probability δ to ensure that the q-th query is in accordance with the authentication process, and receives

$$Q_{q_k} \to H_k(\mathrm{UA}||m||\tilde{e}||z_{k-1} \bmod p),$$

$$Q_{q_{k+1}} \to H_{k+1}(\mathrm{UA}||m||\tilde{e}||z_k \bmod p),$$

where $\delta \geqslant \dfrac{1}{n(q_h+nq_s)Q(k)}$, $Q(k)$ is a polynomial function, q_h and q_s can only carry on polynomial secondary growth under the security parameter k.

When asked about Q_{q_k}, authentication-related queries have occurred and the sim returns the value of c_k. Let $H_k(\mathrm{UA}||m||\tilde{e}||z_{k-1})=c_k$, A finds z_{k-1}, then A finds s_{k-1} from $z_{k-1}=g^{s_{k-1}}T_k^{c_{k-1}}y_{k-1}^{c_{k-1}} \bmod p$, and finally creates ring signature

$$\sigma=(c_1, H_1, \cdots, H_n, s_1, \cdots, s_n, \tilde{e}, r).$$

However, we found that the signature forgery process is in contradiction with the difficulty in solving discrete logarithm. Therefore, the signature generation satisfies unforgeability.

Theorem 3 (Linkable authentication) For a signature $\sigma_L(m)=(c_1, H_1, \cdots, H_n, s_1, \cdots, s_n, \tilde{e}, r)$, forger A is unlikely to falsify another signature associated with the same linkable label of the authenticator $\sigma_{L'}(m')=(c_1', H_1', \cdots, H_n', s_1', \cdots, s_n', \tilde{e}, r)$.

Proof Based on the understanding of linkability in Section 2.3, if the $(\tilde{e}, r)$ of two signatures are the same, the two signatures are relevant. Under normal circumstances, when anonymous authentication occurs, if the two generated signatures need to be linkable, the authenticator will choose the same $(\tilde{e}, r)$ by himself. Therefore, the main task of the proof is that the forger A cannot falsify another signature with the same $(\tilde{e}, r)$ associated with the identity of the authenticator.

As can be seen from Theorem 2, non-ring members can not falsify the legal signature, so the following is mainly to prove that other members outside the ring can not falsify the legal signature associated with the authenticator.

Known the authenticator U_k has produced a legitimate signature $\sigma_L(m)=(c_1, H_1, \cdots, H_n, s_1, \cdots, s_n, \tilde{e}, r)$, forger A forged the signature $\sigma_L(m')=(c_1', H_1', \cdots, H_n', s_1', \cdots, s_n', \tilde{e}, r)$ associated with $\sigma_L(m)$. From the proof of Theorem 2, A needs to find s_{k-1}' from $z_{k-1}'=g^{s_{k-1}'}T_k^{c_{k-1}'}y_{k-1}^{c_{k-1}'} \bmod p$, which is in contradiction with the difficulty in solving discrete logarithm at the present stage. Therefore, the anonymous authentication of this scheme has linkable authentication.

Theorem 4 (Threshold traceability) The threshold number of members can jointly trace the identity of the authenticator.

When the identity of the authenticator needs to be traced, each member of t tracing members use the private key x_i and the identification ID_i to jointly calculate E_k, the identity of y_k is obtained by the formula (22). According to (20), (8), (21), (3), we have

$$\begin{aligned} E_k &= \prod_{i=1}^{t} T_k^{x_i h_i} \bmod p \\ &= g^{t_k \sum_{i=1}^{t} x_i h_i} \bmod p \\ &= g^{t_k a_0} \bmod p \\ &= g^{a_0 t_k} \bmod p \\ &= v_0^{t_k} \bmod p \end{aligned}$$

By (22) and (9), we get

$$\frac{W_k}{E_k} \bmod p = y_k$$

4 Further Analysis

4.1 Property Comparison

Compared with the threshold traceable anonymous authentication scheme mentioned in the preface, the proposed scheme has the properties of anonymous authentication, signature unforgeability, threshold traceability, linkable authentication, as shown in Table 1.

Table 1 Property comparison

Scheme	Anonymous authentication	Signature unforgeability	Threshold traceability	Linkable authentication
Tian *et al*'s scheme[5]	√	√	×	×
Liu *et al*'s scheme[7]	√	√	√	×
Yin *et al*'s scheme[9]	√	√	√	×
The proposed scheme	√	√	√	√

4.2 Computational Cost Comparison

The following mainly compares this scheme with Liu *et al*'s scheme[7] and Yin *et al*'s scheme[9] at the computational cost. Assuming that T_{exp} represents the calculation cost of the modulus index, T_{mul} represents the cost of the modulus multiplication calculation, and the time complexity of the modulus plus, XOR, or other operations is quite small and negligible. n is the number of members, t is the threshold value, and d is the size of the anonymous collection. In the initialization stage, both the proposed scheme and Liu *et al*'s scheme adopt the secret sharing method without trusted center to compute member's private and public keys at the cost of $n(t-1)T_{mul}+n(t-2)T_{exp}$, while Yin *et al*'s scheme allows members to choose their own keys and then collaborate to generate the system's key at the cost of $(t-1)T_{mul}+(2n+3t)T_{exp}$. In the anonymous authentication stage, the proposed scheme uses the linkable ring signature, and the calculation cost is $(2n+1)T_{mul}+(6n+2)T_{exp}$. In the anonymous tracing stage, the proposed scheme uses threshold tracing, and the calculation cost is $T_{mul}+tT_{exp}$. See Table 2 for details.

Table 2 Computational cost comparison

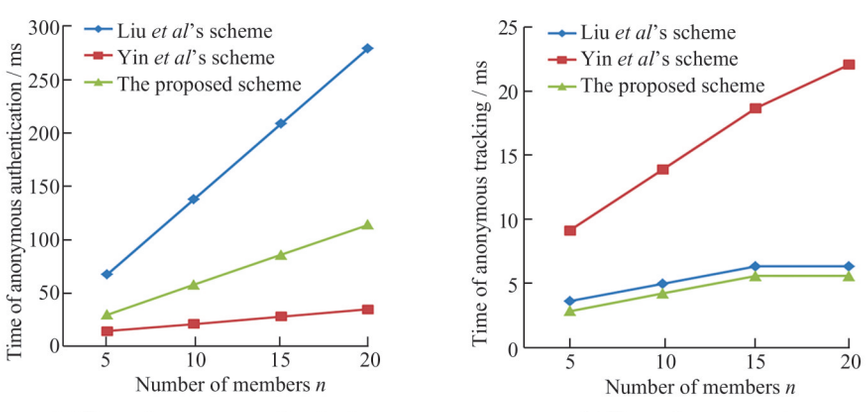
Threshold traceability scheme	Initialization phase	Anonymous authentication phase	Anonymous tracing phase
Liu *et al*'s scheme[7]	$n(t-1)T_{mul}+n(t-2)T_{exp}$	$(6n-2)T_{mul}+(14n-2)T_{exp}$	$2T_{mul}+tT_{exp}$
Yin *et al*'s scheme[9]	$(t-1)T_{mul}+(2n+3t)T_{exp}$	$7T_{mul}+(2d+4)T_{exp}$	$3T_{mul}+(t+d+2)T_{exp}$
The proposed scheme	$n(t-1)T_{mul}+n(t-2)T_{exp}$	$(2n+1)T_{mul}+(6n+2)T_{exp}$	$T_{mul}+tT_{exp}$

The data in Table 2 shows that the calculation cost of this scheme is similar to that of Liu *et al*'s scheme at various stages, and the anonymous authentication stage is even smaller. On the premise of similar calculation cost, this scheme also has linkable authentication, which is more suitable for special applications such as anonymous electronic voting.

4.3 Simulation Experiment

By the simulation experiment, the proposed scheme is compared with Liu *et al*'s scheme[7] and Yin *et al*'s scheme[9] for execution time. The elliptic curve $E: y^2=x^3+x \pmod p$[13] with the finite field F_p is chosen, where p is a large prime number of 512 bits. The hardware of the simulation is i3-8100T CPU, 8 GB RAM and the software is Windows 10 64 bits OS, codeblocks-17.12 software. The execution time of the three schemes is shown in Fig. 1. Figure 1(a) shows the execution time required for anonymous authentication, and Fig. 1(b) shows the execution time required for anonymous tracing.

From Fig. 1(a), we can see that in the anonymous authentication process, the execution time of the proposed scheme is slightly longer than that of Yin *et al*'s scheme, but much shorter than that of Liu *et al*'s. Figure 1(b) shows that the execution time of anonymous tracing in the proposed scheme is shorter than that of the other two schemes. Therefore, the implementation time of the proposed scheme is slightly better than that of the other two schemes.



(a) Time of anonymous authentication (b) Time of anonymous tracing

Fig. 1 Execution time for three schemes

5 Conclusion

The selectively linkable threshold tracing anonymous authentication scheme proposed in this paper, with the help of the linkable ring signature, adds the linkable tag to the authentication signature, which can not only can realize the threshold tracing, but also realize linkable authentication. In the special application of anonymous authentication and linkable authentication, such as anonymous electronic voting, this scheme has a good application prospect.

References

[1] Yang J Q, Chen C H, Li J Y, *et al*. Compressed-encoding particle swarm optimization with fuzzy learning for large-scale feature selection[J]. *Symmetry*, 2022, **14**(6): 1142.

[2] Tang Y M, Pan Z F, Pedrycz W, *et al*. Viewpoint-based kernel fuzzy clustering with weight information granules[J]. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2023, **7**(2): 342-356.

[3] Ateniese G, Herzberg A, Krawczyk H, *et al*. Untraceable mobility or how to travel incognito[J]. *Computer Networks*, 1999, **31**(8):871-884.

[4] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]// *Proceedings of ASIACR-YPT'* 01. Berlin: Springer-Verlag, 2001: 552-565.

[5] Tian Z J, Wang J L, Wu Y X. A dynamic anonymous authentication scheme with identity escrow[J]. *Journal of Electronics & Information Technology*, 2005, **27**(11):1737-1740.

[6] Manulis M. Democratic group signature: On an example of joint ventures[C]// *Proceedings of ACM Symposium on Information*, *Computer and Communications Security*. New York: ACM Press, 2006: 191-196.

[7] Liu F B, Zhang K, Li H, *et al*. Threshold traceability anonymous authentication scheme without trusted center for adhoc network[J]. *Journal of Communications*, 2012, **33**(8): 208-213.

[8] Abe M, Ohkubo M, Suzuki K. 1-out-of-*n* signatures from a variety of keys[C]// *Proceedings of ASIACRYPT'*02. Berlin: Springer-Verlag, 2002: 415-423.

[9] Yin F M, Hou Z F, Pu G N. Self-selecting share threshold traceable anonymous authentication scheme[J]. *Journal of Wuhan University* (*Natural Science Edition*), 2015, **61**(6): 549-553.

[10] Beullens W, Katsumata S, Pintore F. Calamari and falafl: logarithmic (linkable) ring signatures from isogenies and lattices[C]// *Advances in Cryptology-ASIACRYPT* 2020. Cham: Springer-Verlag, 2020: 464-492.

[11] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups[C]// *Australasian Conference on Information Security and Privacy.* Berlin: Springer-Verlag, 2004: 325-335.

[12] Zhang W F, Xiong D, Wang X M, *et al*. Selectively linkable and convertible ring signature based on RSA public key cryptosystem[J]. *Chinese Journal of Computers*, 2017, **40** (5): 1168-1180.

[13] Ming Y, Shen X Q. PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks[J]. *Sensors*, 2018, **18**(5): 1573-1596.

□