A Group Digital Signature Technique for Authentication

Chin-Ming Hsu¹, Shih-Hsiung Tu², and Hui-Mei Chao¹

¹ Department of Electronic Engineering  
Kao-Yuan Institute of Technology  
Lu-Ju Hsiang 82101, Kao-Hsiung, Taiwan, R.O.C.

² Department of Electrical Engineering  
Chung Yuan Christian University  
Chung-Li 32023, Taiwan, R.O.C.

ABSTRACT

A group digital signature technique using a digital signature algorithm and a challenge-response identification protocol is proposed to provide effective authentication. The proposed digital signature algorithm is based on solving quadratic congruence, factorization, and discrete logarithm problems. Based on the public key infrastructure, group members generate their public-private keys first. The designed authority generates the group member’s identity code (ID), the group identity mark, and the group secret key. Every group member keeps his/her private key and the ID for signing. These parameters can ensure only members who can make signatures and provide data authenticity and non-repudiation for any signer. The challenge-response identification protocol with overlapping-shifting-EXOR logical operations is proposed to ensure the signer to obtain group secret key securely and prevent any signer from making false claims. According to the security analysis, the processing time of the proposed approach is faster than the existing RSA and ElGamal group digital signature systems. Moreover, the proposed method would be suited to microprocessor-based devices such as smart cards, computer systems, networks and control systems because of its simplicity, confidentiality, and fast processing speed.

Keywords: Group digital signatures, challenge response, authentication, public-private keys, and non-repudiation.

1. INTRODUCTION

With the popularity of the Internet and the legislation of digital signatures in Taiwan, transmitting official electronic documentation among different departments to increase the productivity of an institution is encouraged. This encouragement therefore brings group signature authentication problems. Some general properties of group signatures are briefly introduced as follows [1]:

Anonymity:

Given a signature, it is infeasible to find out the identity of the actual signer except the designated group manager or the authority institution.

Un-linkability:

Given two signatures, it is computationally difficult to determine whether the signatures generated by the same member or not.

Unforgeability:

Only registered members can sign messages on behalf of their group.

Traceability:

In order to identify the actual signer, the group manager or the authority institution is always able to open a valid signature.

Coalition-resistance:

There is no colluding subset of group members can generate a valid signature that the group manager cannot trace.

In the past decade, some group signature techniques have been proposed. Chaum and van Heyst [2] first propose four group signature schemes that are based on solving factorization and discrete logarithm problems. However, two drawbacks exist: (1) the group manager must cooperate with group members in the case of dispute; (2) joining new members or deleting old members needs to change key sizes of the group. Two efficient group signature schemes [3] [4] also are based on solving discrete logarithm mathematical problems. However, they have the same problem: the sizes of secret keys of the group member will increase with the number of signatures. Two efficient group signature techniques for large groups [5-6] are proposed to solve this problem. L. Chen and T. Pedersen [7] propose another information-theoretic group signature scheme. However, this technique allows the group manager to sign messages in the name of any members of group. Moreover, some attacking the existing group signature works are done in [8-11].

In this paper, a new group signature scheme with a challenge-response identification protocol and a digital signature algorithm is proposed to provide effective authentication with three functions: (1) allowing only members to make signatures; (2) remaining actual member who made signatures anonymous; (3) providing
data authenticity and non-repudiation for any signer in the group. The detail description of the proposed group digital signature scheme is shown in the following section.

2. PROPOSED GROUP DIGITAL SIGNATURE SCHEME

The structure of the proposed group digital signature scheme that consists of an authority institution (AI) and group members is illustrated in Figure 1. The interaction between the AI and group members is based on a challenge-response identification scheme. The challenge-response identification scheme supports data confidentiality on transmission and anonymous signature made by the actual member. The AI associated with the challenge-response identification scheme ensures that only members can make the signature, data authenticity, and non-repudiation for any signer in the group.

Figure 1. The structure of the proposed group digital signature technique

The digital signature algorithm [12] based on solving quadratic congruence, factorization and discrete logarithm problems is used to correctly identify the signer in the group. The group members first apply this digital signature algorithm to generate their public-private key pairs respectively and register their identities in the AI. According to enrolled group members’ identities, the AI then generates a group secret key in the database for further transmission. Five processes are included. They are:

1. Public-private key generation by group members
2. Group identity mark and member identity code generation for group members
3. The challenge-response identification
4. Signing Process
5. Verification Process

Public-private key generation for group members

Step1: Let p, q, r, and s be four prime numbers that satisfy
\[ n_1 = 2 \left[ \frac{p}{q} \right] + 1 \quad \text{and} \quad n_2 = 2 \left[ \frac{r}{s} \right] + 1, \]
where \( n_1 \) and \( n_2 \) are also prime numbers. Let \( N = n_1 n_2 \), therefore, \( \Phi(N) = (n_1 - 1)(n_2 - 1) = 4 \left[ \frac{p}{q} \right] \left[ \frac{r}{s} \right] \), where \( \Phi(N) \) is Euler phi-function that is the number of positive integers not exceeding \( N \), which is relatively prime to \( N \). If \( N \) is prime, \( \Phi(N) \) is equal to \( N-1 \).

Step2: Choose an odd number \( t \) that satisfies following equations:
\[ X_1 = t^2 \mod (\Phi(N)) \]
\[ X_1 \cdot d = 1 \mod (\Phi(N)) \]
\[ X_2 = t^{(\Phi(N)^2)} \mod N = t^{X_1 \cdot 2 + 1} \mod N \]

Step3: Publish the public keys (\( X_1 \), \( X_2 \), and \( N \)) to the AI.

Step4: Keep the private keys (\( t \) and \( d \)) securely.

Group identity mark and member identity code generation for group members

Let \( G \) and \( ID_i \) be the group identity mark, \( i \)th identity code of a group member, where \( i = 1, 2, \ldots, n \). These two parameters are set by the AI securely.

The challenge-response identification

The challenge-response identification process is shown in Figure 2, where \( R_1 \) and \( R_2 \) are random numbers as challenges.

![Figure 2. The challenge-response identification scheme](image-url)
Step 1: The user sends the group identity mark $G$ to the AI.
Step 2: The AI sends the random number $R_1$ to the user if the received $G$ is identified correctly.
Step 3: The user sends $ID_i \otimes R_1$ and the random number $R_2$ to the AI. The AI would take the received $ID_i \otimes R_1$ through the decrypting process. If the $R_1$ can be decrypted by $ID_i$, the user is then identified.
Step 4: After the user is identified, the AI would respond an acknowledgement and send $S_G \otimes R_2$ to the user. The user would take the received $S_G \otimes R_2$ through the decrypting process to find the group secret key $S_G$ for further signing process.

**Signing Process**

If B wants to sign a message $m$ to A, four steps are included in the signing process.

Step 1: B gets the group secret key $S_G$ from the AI by the challenge-response protocol.

Step 2: B uses his private keys ($t$ and $d$) to sign the message such as

$$S(m) = (m^d \cdot t^{d+2r+1}) \mod N$$

Step 3: B computes two parameters: $X_3$ and $P$, by following equations:

$$X_3 = S_G \otimes ID_i \otimes S(m),$$

$$P = G \otimes X_3$$

Step 4: B sends the $(P, X_3, S(m), m)$ to the A.

**Verification Process**

Two steps are included in the verification process.

Step 1: After A receives the signature information ($P, X_3, S(m), m$) from B, A uses $P$ and $X_3$ to verify the received data by calculating $P \otimes X_3$. If the result is the same as the group identity mark $G$, then the received message is ensured and signed by the group.

Step 2: In the case of dispute, the AI will check the equation $X_3 \otimes S(m) = S_G \otimes ID_i$. If it is true, the AI then checks the public key verification table to find the $t^{th}$ public key to decrypt $S(m)$.

Such as

$$m' = V(S) = S(m)^{X_3} \cdot X_2^{-1} \mod N$$

If $m = m'$, the signer is identified.

**Proof:**

$$V(S) = m' = X_2^{-1} \cdot S^{X_3} \mod N$$  
$$\equiv X_2^{-1} \cdot (m^d \cdot t^{d+2r+1})^{X_3} \mod N$$  
$$\equiv X_2^{-1} \cdot m^{d \cdot X_3} \cdot t^{d \cdot 2r+1} \mod N$$  
$$\equiv m \cdot X_2 \cdot X_2^{-1} \mod N$$  
$$\equiv m \mod N$$

**Security Analysis:**

The authentication security capability would be provided by the challenge-response identification scheme and the digital signature algorithm. They are analyzed as follows.

(1) **The challenge-response identification scheme**

Using random numbers as challenges and $\Box$ function as the cipher ensures dynamic messages transmitted on the network for each process. These challenges can prevent the user from denying their transmission and any entry from forgery or making false claims. Therefore, the non-repudiation is provided.

(2) **The digital signature algorithm**

The difficulties of the proposed digital signature algorithm are based on solving three mathematical problems: discrete logarithm, factorization, and quadratic congruence. Therefore, the enough complexity of the proposed method is provided.

### 3. IMPLEMENTATION METHODS

The implementing proposed group signature scheme consists of four procedures: setup, sign, verify, and open. They are described in the following and an example is shown.

**Setup**

An interactive identification protocol between the AI and the group member is built. Some parameters such as the group identity mark, the user ID, and the user’s public-private keys are also set.

**Sign**

A signature generating algorithm is applied to generate a signature for a message.

**Verify**

An algorithm is established to check the validity of a group signature with respect to some related parameters.

**Open**

An algorithm allows the AI or the group manager to determine the identity of the group member who issued the signature, and provides a proof of this fact.

**An example:**

**Setup**

The interactive challenge-response identification protocol is set as shown in Figure 2. Assuming the group identity mark $G$ is 372, the user’s ID is 965, user’s public keys ($X_1$, $X_2$, $N$) equals (3259, 3096, 4757) and its private keys ($d, t$) equals (2689, 113).

**Sign**

Let the group secret key $S_G$ be 1453 set by the AI. The user can obtain the $S_G$ by the challenge-response
identification protocol. If the message \( m = 813 \), then the signer’s signature can be generated by

\[
S(m) = m^d \equiv X_i^{m} \mod N = 813^{3689} \times 113^{564} \mod 464
\]

\[
X_i = S_G \cdot ID = S(m) = 1453 \cdot 965 \equiv 464 = 1234,
\]

\[
P = G \cdot X_i = 372 \cdot 1234 = 251
\]

Therefore, the related parameters are generated such as:

\( (P, X_i, S(m), m) = (251, 1234, 464, 813) \)

**Verify**

By checking \( P \cdot X_i = G \) the validity of a group signature is identified.

**Open**

By checking Is \( X_i \cdot S(m) \) equal to \( S_G \cdot ID \)? If the answer is yes, the AI then checks the public key verification table to find the \( i^{th} \) public key to decrypt \( S(m) \). Such as

\[
m^e = V(S) = S(m)^X_i \cdot X_i^{-1} \mod N
\]

If \( m = m' \), the signer is identified.

### 4. CONCLUSIONS

A new group digital signature technique with a challenge-response identification protocol and a digital signature scheme is proposed to 1) allow only members to make signatures, (2) remain actual member who made signatures anonymous, and (3) provide data authenticity and non-repudiation for any signer in the group. The proposed method provides two improvements: faster processing time and the key sizes of the group member will not increase with the number of signatures.

**Faster processing time:**

Because the parameters of \( G, ID, \) and \( S_G \) are independent from the group members’ signatures, signing, verification, joining new members or deleting old members can be performed by adding or erasing the related public parameters without changing any keys of other members. Therefore, the numbers of calculation are decreased. Furthermore, the proposed method uses only one public-private key pair instead of two pairs for existing works. This reduces the time for generating keys and computing the related parameters.

**The sizes of keys of the group member will not increase with the number of signatures:**

Because key generation is independent from other group members, therefore, the key sizes of the group member will not increase with the number of signatures. Furthermore, the use of the challenge-response identification protocol and \( \Box \) function instead of uses of mathematical calculation to increase the complexity of the scheme, the key sizes are not absolutely needed too long to increase system security.

### REFERENCES