ELSEVIER

Computer Communications 21 (1998) 771–776

computer communications

Research note
Threshold signature schemes with traceable signers in group communications

Ching-Te Wang[a], Chu-Hsing Lin[b,*], Chin-Chen Chang[a]

[a]*Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 62107, R.O.C.*
[b]*Department of Computer and Information Sciences, Tunghai University, Taichung, Taiwan 407, R.O.C.*

Received 14 November 1997; received in revised form 19 February 1998; accepted 24 February 1998

Abstract

We propose a new group-oriented (t,n) threshold signature scheme that can withstand conspiracy attacks without attaching a secret number. The group's public key is determined by all members, each member signs a message independently and transmits the individual signature to a designated clerk who checks and integrates them into a group signature. A verifier can authenticate the group signature and trace back to find the signers. Further, we develop another threshold signature scheme without a trusted center. The proposed schemes possess all of the characteristics listed in Harn's scheme and are more difficult to break. © 1998 Elsevier Science B.V.

Keywords: Mutually trusted center; Group-oriented cryptography; Threshold signature

1. Introduction

The concept of group-oriented cryptography was first proposed by Desmedt [1]. The group-oriented cryptography problem refers to the study of ciphering schemes for secure communications among groups. In this kind of secure system, each group, instead of all internal members of the group, publishes a single group's public key. An outsider can use this public key to send a confidential message to a group, but only a specified subset of the group members, in a cooperative manner, can reveal the message. Recently, several schemes have been developed and can be categorized in two classes. The first type needs the assistance of a mutually trusted center to select the parameters and generate the secret keys for group members [2–4]. Another type does not need the assistance of a mutually trusted center to select the parameters and generate the secret keys, but extra computations will be required [5–8]. Obviously, the latter type of scheme is more common in some commercial applications when there does not exist any third party who can be trusted by all members in a group.

By applying the concept of group-oriented cryptography, signature schemes or threshold signature schemes in groups are developed. In a threshold signature scheme, the group's public key is generated by all of the members, but the group signature can be generated by the participating members in a subgroup. That is, in a (t,n) threshold signature scheme, any t members can represent this group to generate the group signature. Later, in the signature verification process, an outsider can employ the group's public key to authenticate the validity of the group signature.

Chaum and Heyst [9] proposed an (n,n) group-oriented signature scheme, which used several groups' public keys in the system. Desmedt and Frankel [10] proposed the concept of a (t,n) threshold signature scheme based on the RSA [11] system. In this scheme, they applied a trusted key authentication center to determine the group's secret key and the secret keys of all group members. Harn [12] used the cryptographic technique of Shamir's perfect secret sharing scheme [13] which is based on the Lagrange interpolating polynomial and digital signature algorithm to construct a (t,n) threshold signature scheme. This scheme is designed to partition the group secret key K into n different shadows. By collecting any t shadows, the group signature can be easily generated. Unfortunately, the schemes [10,12] may suffer from the conspiracy attacks and the secret keys can be revealed with high probability [14]. To avoid the attacks, the schemes [14] attach a random number to the secret key, which is concealed. In both of the schemes [12,14] there exists a problem: how do we know who participated in making the signature? For example, there are t members who are responsible for the signature, making a policy decision, and obtaining a profit for their company. The company's manager wants to know who the signers are and will

* Corresponding author. e-mail: chlin@s867.thu.edu.tw

PII S0140-3664(98)00142-X

reward them. An intuitive method to find the signers is that the trusted center makes the t individual secret keys public and authenticates the partial and group signatures. Using this method, the system needs to renew a group secret key and redistribute an individual secret key for each member. This can be very expensive.

In this paper, we shall first propose a threshold signature scheme in which a mutually trusted center is required to generate the parameters and the secret keys of group members. Our methods can withstand conspiracy attacks without attaching a secret random number as in the scheme of Li et al. [14]. We can trace back to find the signers without revealing the secret keys. Further, we also propose a threshold signature scheme without the assistance of a mutually trusted center. By the use of our (t,n) group-oriented threshold schemes, the difficulty of breaking the systems is equal to solving the discrete logarithm problem. By applying the concept of shadow secret keys, the group secret key can be considered as a set of individual secret keys. With the knowledge of any t individual secret keys, the group signature can be easily generated. On the other hand, any less than t members cannot regenerate the legitimate group signature. Moreover, compared with Harn's scheme, our schemes are more difficult to break.

In the next section, we will review the group-oriented threshold signature scheme [12] proposed by Harn. In Section 3, we will present a new (t,n) group-oriented threshold signature scheme with the assistance of a mutually trusted center. In Section 4, a new (t,n) group-oriented threshold signature scheme is proposed in which the mutually trusted center is no longer used. Finally, we make some conclusions in the final section.

2. Harn's (t,n) threshold signature scheme

In this section, we will review briefly the concept of threshold signature. In Harn's (t,n) threshold signature scheme [12], there is a trusted key authentication center (KAC) which is responsible for selecting all parameters; the secret keys for members in a group and the group's secret key. Assume that KAC selects the following parameters:

- P = a large prime modulus, where $2^{511} < P < 2^{512}$;
- Q = a prime divisor of $P-1$, where $2^{159} < Q < 2^{160}$;
- a polynomial function $f(x) \equiv a_0 + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod Q$ with degree $t-1$, where $0 < a_i < Q$, $i = 0,1,\ldots,t-1$, and a_i are kept secretly;
- a positive integer $g \equiv h^{(P-1)/Q} \bmod P$, where $1 \le h \le P-1$, and g is a generator with order Q in GF(P).

Harn's threshold signature scheme contains three phases.

1. Group and individual secret keys generation phase. The KAC determines the following keys:

   (a) Computes each member's secret key $f(x_i) \bmod Q$, for $i = 1,2,\ldots,n$, where x_i is the public value associated with each member.

   (b) Selects a group's secret key $f(0)$ and computes the group's public key $y \equiv g^{f(0)} \bmod P$.

   (c) Computes each member's public key, $y_i \equiv g^{f(x_i)} \bmod P$, for $i = 1,2,\ldots,n$.

2. Threshold signature generation phase. The threshold signature scheme allows any t members to represent the group to sign a message m. Without loss of generality, assume that the t group members can be denoted as $u_1,u_2,\ldots,u_t$. Firstly, the member u_i, $i = 1,2,\ldots,t$, randomly selects an integer K_i, $K_i \in [1,Q-1]$, then computes a public value r_i, $r_i \equiv g^{K_i} \bmod P$, and makes r_i publicly available through a broadcast channel. After all values are available, each member u_i computes the value $R \equiv \prod_{i=1}^{t} r_i \bmod P$, and uses his secret keys $f(x_i)$ and K_i to compute the signature s_i:

$$s_i \equiv f(x_i) \times m' \times \left(\prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j} \right) - K_i \times R \bmod Q,$$

   where $m' = f(m)$

Then he transmits $\{m,s_i\}$ to a designated clerk C. After receiving the individual signature $\{r_i,s_i\}$ from u_i, $i = 1,2,\ldots,t$, the clerk uses the public keys x_i, y_i, and the individual signature $\{r_i,s_i\}$ to check if the following equation is true:

$$y_i^{m' \times \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j}} \stackrel{?}{=} r_i^R \times g^{s_i} \bmod P$$

If the above equation holds, the partial signature $\{r_i,s_i\}$ of the message m received from u_i is valid. Once t partial signatures are received and verified, the clerk can compute and generate the group signature S of the message m, where

$$S \equiv \sum_{i=1}^{t} s_i \bmod Q$$

3. Threshold signature verification phase. After receiving the group signature $\{R,S\}$ of the message m, any verifier can use the group's public key y to authenticate the validity of the signature by the following equation:

$$y^{m'} \equiv R^R \cdot g^S \bmod P, \text{ where } m' = f(m)$$

If the equation holds, the group signature $\{R,S\}$ is valid.

3. A (t,n) threshold signature scheme with the assistance of a mutually trusted center

Harn's method [12] employed Shamir's perfect secret sharing scheme [13], Lagrange interpolating polynomials, and ElGamal's signature scheme [15,16]. Based on the modified ElGamal's signature scheme, we will improve

Harn's method and propose a more efficient signature scheme. Further, several possible attacks [14] to our scheme are considered.

Lemma 3.1 [17]. If $x_1,x_2,\ldots,x_n$ are n distinct numbers and $y_1,y_2,\ldots,y_n$ are the associated function values, respectively, then Lagrange interpolating polynomial $f(x)$ of degree $n-1$ with the property $f(x_k)=y_k$ for $k=1,2,\ldots,n$, is given by

$$f(x)=\sum_{i=1}^{n} y_i \times \prod_{j=1,j\neq i}^{n} \frac{x-x_j}{x_i-x_j}$$

Assume that there are n members in a group, and the set of group members is denoted as A. Here $|A|=n$. The set of any t legitimate members of A is denoted as B. Note that $|B|=t$. Further, the system contains a mutually trusted center (MTC), which is responsible for selecting all parameters, individual secret keys and the group's secret key. The scheme is composed of the following three phases.

1. Parameter selection and secret keys generation phase. The MTC selects the following parameters:

- a one-way hash function H;
- two large prime numbers P and P', g is a generator with order P' in $GF(P)$;
- a large prime factor Q of $P'-1$, α is a generator with order Q in $GF(P')$;
- a polynomial function $f(x)\equiv a_0+a_1x+\ldots+a_{t-1}x^{t-1} \bmod Q$ with degree $t-1$, where $0<a_i<Q$, $i=0,1,\ldots,t-1$, and a_i are kept secretly.The MTC also selects the following secret and public keys:
- computes each member's secret key $\alpha^{f(x_i)} \bmod P'$, for $i=1,2,\ldots,n$, where x_i is the public value associated with each member;
- selects a group secret key $f(0)$, and computes the group's public key $y\equiv g^{\alpha^{f(0)}} \bmod P$;
- computes each member's public key $y\equiv g^{\alpha^{f(x_i)}} \bmod P$, for $i=1,2,\ldots,n$, and $y_i\neq y_j$ if $i\neq j$.

2. Individual signature generation and verification phase. Assume that there are t group members representing the group to sign a message m. Each member u_i selects a random number d_i, and computes a secret value $r_i\equiv\alpha^{d_i} \bmod P'$. Then, each member uses the secret key $\alpha^{f(x_i)} \bmod P'$, and the random number d_i to compute the value s_i by

$$s_i\equiv\left(\alpha^{f(x_i)}\prod_{j=1,j\neq i}^{t}\frac{0-x_j}{x_i-x_j}\right)\times H(m)\times\alpha^{d_i} \bmod P' \qquad (3.1)$$

To generate a group signature and protect against a forged signature from an outsider, the signer's identification needs to be verified by a designated clerk. So, each member u_i regards the individual signature s_i as a message and uses his secret key $\alpha^{f(x_i)}$ and public key $y^{\alpha^{f(x_i)}}$ to sign the message s_i by ElGamal's signature scheme [15]. First, member u_i selects a random number k_i, where $(k_i,P')=1$, and computes two numbers z_i,s_i', where $z_i\equiv g^{k_i} \bmod P$, $s_i'\equiv k_i^{-1}(s_i-\alpha^{f(x_i)}z_i) \bmod P'$. Then, the messages $\{m,r_i,s_i,z_i,s_i'\}$ are transmitted to a designated clerk. Note that the designated clerk does not contain any secret information. He merely takes the responsibility to authenticate each signer's identification and create a group signature. The authenticated identification is supplied to verify and trace the signers and the group signature is supplied to check the validity with threshold members. On receiving the messages $\{m,r_i,s_i,z_i,s_i'\}$ from u_i, the clerk utilizes the public value y_i to compute the following equation and authenticate the validity of the partial signature:

$$g^{s_i}\stackrel{?}{=}y_i^{z_i}\cdot z_i^{s_i'} \bmod P \qquad (3.2)$$

If the equation holds, the individual signature s_i from member u_i is valid. Further, the clerk uses subset B's t pairs of public values (y_i,x_i) to construct a Lagrange polynomial function $h(y)$ by using Lemma 3.1, where

$$h(y)=\sum_{i=1}^{t}x_i\prod_{j=1,j\neq i}^{t}\frac{y-y_j}{y_i-y_j}=b_{t-1}y^{t-1}+\ldots+b_1y+b_0 \qquad (3.3)$$

Note that in using Lemma 3.1 the roles of x_i and y_i are exchanged here. The subset B's t pairs (y_i,x_i) are integrated by the function $h(y)$. In fact, the purpose of the above function is to authenticate who the signers are in the next phase.

3. Group signature generation and verification phase. After t individual signatures are received and verified by the clerk in the second phase, the group signature of the message m can be obtained as $\{R,S\}$, where

$$R\equiv\prod_{i\in B}r_i \bmod P' \qquad (3.4)$$

$$S\equiv\prod_{i\in B}s_i \bmod P' \qquad (3.5)$$

Any verifier can use the group public key y and the group signature $\{R,S\}$ of the message m to authenticate the validity of the signature. The verification equation is given as follows:

$$g^S\stackrel{?}{=}y^{(H(m))'R} \bmod P$$

If the above equation holds, the group signature $\{R,S\}$ is valid.

As stated, the group signature has been authenticated, but the verifier does not know who are the signers. If he intends to determine the singers, he can substitute the public value y_i to $h(y)$ as in Eq. (3.3). If $h(y_i)=x_i$, then the signer with public value y_i belongs to the set B. Otherwise, the member with public value y_i is not one of the original signers. In the process of verification, the verifier computes the function $h(y_i)$ and checks whether it is equal to x_i. There are only two public parameters required.

Theorem 3.1. If $g^S\equiv y^{(H(m))'R} \bmod P$, then the group signature $\{R,S\}$ of the message m is authentic.

Proof. In the second phase, the individual signatures s_i of the message m satisfy the equations

$$s_i \equiv \left(\alpha^{f(x_i)} \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j} \right) \times H(m) \times \alpha^{d_i} \bmod P'$$

By multiplying the above equations for $i = 1,2,\ldots,t$, we have

$$\prod_{i=1}^{t} s_i \equiv \prod_{i=1}^{t} \left(\left(\alpha^{f(x_i)} \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P' \tag{3.6}$$

The right-hand side of Eq. (3.6) can be rewritten as

$$\left(\alpha^{\sum_{i=1}^{t} f(x_i)} \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j} \right) \times (H(m))^t \times \alpha^{\sum_{i=1}^{t} d_i} \bmod P' \tag{3.7}$$

By Lemma 3.1, Eq. (3.7) can be rewritten as $\alpha^{f(0)} \times (H(m))^t \times R$. Therefore

$$g^S \equiv g^{\prod_{i=1}^{t} s_i} \bmod P \equiv g^{\alpha^{f(0)} \cdot (h(m))^t R} \bmod P \equiv y^{(H(m))^t R} \bmod P$$

If $g^S \equiv y^{(H(m))^t R} \bmod P$, then the group signature $\{R,S\}$ can be verified, and the proof is completed.

Now we will analyze the security of our scheme. Several possible attacks will be considered, but none of them can successfully break the scheme. Firstly, we assume that an outsider wants to reveal the secret keys by knowing the public keys.

1. To obtain the individual secret keys $\alpha^{f(x_i)}$, for $i = 1,2,\ldots,n$. From the public keys $y_i \equiv g^{\alpha^{f(x_i)}} \bmod P$, it is obvious that he should solve the discrete logarithm problem.
2. To obtain the group secret key $f(0)$. From the public key $y \equiv g^{\alpha^{f(0)}} \bmod P$, he is still required to solve the discrete logarithm problem. Secondly, we assume that there is an attacker who intends to reveal the secret keys from the signature.
3. To derive the individual secret key $\alpha^{f(x_i)} \bmod P'$ from the signature s_i in Eq. (3.1). There are two unknown values $\alpha^{f(x_i)}$ and d_i in one equation; therefore he cannot solve the problem.
4. To derive the group secret key $f(0)$, from the signature pair $\{R,S\}$, by Eq. (3.1), Eq. (3.5), and

$$S \equiv \prod_{i=1}^{t} s_i \bmod P' \equiv \left(\alpha^{\sum_{i=1}^{t} f(x_i)} \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j} \right) \times (H(m))^t \times \alpha^{\sum_{i=1}^{t} d_i} \bmod P' \equiv \alpha^{f(0)} \times (H(m))^t \times R \bmod P'$$

If, unfortunately, any t or more malicious members act in collusion, then the term $(H(m))^t R$ can be determined, and they can find $\alpha^{f(0)}$. However, when $f(0)$ is further intended, it has to solve the discrete logarithm problem.

5. To derive the secret function $f(x)$, from any t pairs $(x_i, \alpha^{f(x_i)})$ in collusion, they cannot reconstruct the function by the Lagrange interpolating function.

Further, if a forger wants to impersonate a member u_i by randomly selecting a number $d_i' \in [1, Q-1]$ and broadcasting $r_i' \equiv \alpha^{d_i'} \bmod P'$. Since the value

$$R' \equiv \left(\prod_{j=1, j\neq i}^{t} r_j \right) \times r_i' \bmod P'$$

is computed by all t members, without knowing the individual secret key $\alpha^{f(x_i)}$, the forger cannot obtain a correct signature s_i'. Moreover, as in Harn's scheme, the signature value s_i is based on a linear equation with two unknown parameters, the security of their scheme is based on the modified ElGamal's signature scheme. On the other hand, the security of our scheme is based on the difficulty of solving the discrete logarithm problem as described previously. The security of the proposed method will be improved.

4. A (t,n) threshold signature scheme without the assistance of a mutually trusted center

In this section, we will develop a new (t,n) threshold signature scheme without the assistance of a mutually trusted center. Again, assume that there are n members in the group, the set of group members is denoted as A, the subset of any t legitimate members of A is denoted as B. Since there is no trusted center, more parameters and complicated computations are required. The scheme is also composed of three phases as follows:

1. Parameter selection and secret keys generation phase. Here, the parameters H, P, P', Q, g, α are defined as in the previous section. Each member, say u_i, randomly selects a public value $x_i \in [1, Q-1]$ and a secret function $f_i(x)$ with degree $t-1$. Member u_i keeps the value $\alpha^{f_i(0)}$ secret and computes a corresponding public key $y_i \equiv g^{\alpha^{f_i(0)}} \bmod P$. Then, the group public key y is determined by all members [18]. All members need to be connected in any order ring and generate the group public key y as follows: $y \equiv g^{\alpha^{f_1(0)} \cdot \alpha^{f_2(0)} \cdots \alpha^{f_n(0)}} \bmod P$. Instead of the trusted center, the member u_i should compute a secret key v_{ij} and a corresponding public key y_{ij} for each other member u_j, where

$$v_{ij} \equiv \alpha^{f_i(x_j)} \bmod P', \quad y_{ij} \equiv g^{v_{ij}} \bmod P \text{ and } y_{ij} \neq y_{ik} \text{ if } j \neq k$$

2. Individual signature generation and verification phase. Assume there are t members representing the group to

sign a message m. Member u_i selects a random number d_i, and computes a secret value $r_i \equiv \alpha^{d_i} \bmod P'$. Then he uses the secret key $\alpha^{f_i(0)}$, the random number d_i and the secret values $\alpha^{f_j(x_i)}$, where $j \in A$ and $j \notin B$, to sign the message m:

$$s_i \equiv \left(\left(\alpha^{f_i(0)} \times \prod_{j \in A, j \notin B} \alpha^{f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P' \quad (4.1)$$

As in the previous section, each member u_i considers the individual signature s_i as a message and uses his secret key $\alpha^{f_i(0)}$ and public key $y^{\alpha^{f_i(0)}}$ to sign the message s_i by ElGamal's signature scheme [15]. First, member u_i selects a random number k_i, where $(k_i, P') = 1$, and computes two numbers z_i, s_i', where $z_i \equiv g^{k_i} \bmod P$, $s_i' \equiv k_i^{-1}(s_i - \alpha^{f_i(0)} z_i) \bmod P'$. Then, the messages $\{m, r_i, s_i, z_i, s_i'\}$ are transmitted to a designated clerk who is only responsible for collecting and evaluating information. Note that the clerk here is different from a mutually trusted center since he does not select any parameter for users. Here, the individual signature s_i is a partial signature of the message m. On receiving the messages $\{m, r_i, s_i, z_i, s_i'\}$, the clerk uses the public key y_i to check whether the following equation is true:

$$g^{s_i} \stackrel{?}{=} y_i^{z_i} \cdot z_i^{s_i'} \bmod P$$

If the equation holds, the individual signature s_i of the message m received from u_i has been verified. Moreover, the clerk randomly selects a member u_j and uses subset B's t pairs of public values (y_{ji}, x_i) to construct a Lagrange polynomial $h_j(y)$ as in Lemma 3.1, where

$$h_j(y) = \sum_{i=1}^{t} x_i \prod_{l=1, l \neq i}^{t} \frac{y - y_{jl}}{y_{ji} - y_{jl}} = b_{t-1} y^{t-1} + \ldots + b_1 y + b_0 \quad (4.2)$$

Similarly, $h_j(y)$ will be used to authenticate the signers in the next phase.

3. Group signature generation and verification phase. When t individual signatures are received and verified by the clerk in the second phase, the group signature of the message m can be computed as $\{R, S\}$, where

$$R \equiv \prod_{i \in B} r_i \bmod P', \quad S \equiv \prod_{i \in B} s_i \bmod P'$$

Any verifier can use the group public key y and the group signature $\{R, S\}$ of the message m to authenticate the validity of the signature. The verification equation is given as follows

$$g^S \stackrel{?}{=} y^{(H(m))^t R} \bmod P$$

If the equation holds, the group signature $\{R, S\}$ is valid. Similarly, to find the signers, we can substitute the public value y_{ji} to $h_j(y)$ as in Eq. (4.2). If $h_j(y_{ji}) = x_i$, then the signer with public value y_{ji} belongs to the set B. Otherwise, the member with public value y_{ji} is not one of the original signers.

Theorem 4.1. If $g^S \equiv y^{(H(m))^t R} \bmod P$, then the group signature $\{R, S\}$ of the message m is authentic.

Proof. In the second phase, the individual signatures s_i of the message m satisfy the equations

$$s_i \equiv \left(\left(\alpha^{f_i(0)} \times \prod_{j \in A, j \notin B} \alpha^{f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P'$$

By multiplying the above equations for $i = 1, 2, \ldots, t$, we have

$$\begin{aligned} \prod_{i=1}^{t} s_i &\equiv \prod_{i=1}^{t} \left(\left(\alpha^{f_i(0)} \times \prod_{j \in A, j \notin B} \alpha^{f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P' \\ &\equiv \prod_{i=1}^{t} \left(\left(\alpha^{f_i(0)} \times \alpha^{\sum_{j \in A, j \notin B} f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P' \\ &\equiv \prod_{i=1}^{t} \left(\left(\alpha^{f_i(0) + \sum_{j \in A, j \notin B} f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times H(m) \times \alpha^{d_i} \right) \bmod P' \\ &\equiv \left(\alpha^{\sum_{i=1}^{t} f_i(0) + \sum_{j \in A, j \notin B} f_j(x_i) \prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}} \right) \times (H(m))^t \times \left(\alpha^{\sum_{i=1}^{t} d_i} \right) \bmod P' \end{aligned}$$

Therefore

$$g^S \equiv g^{\prod_{i=1}^{t} s_i} \bmod P \equiv g^{\sum_{i=1}^{n} f_i(0) \times (H(m))^t R} \bmod P \equiv y^{(H(m))^t R} \bmod P$$

the group signature $\{R, S\}$ can be verified, and the proof is completed.

The equations in Theorem 4.1 do not seem obvious. For a

better understanding, we give an example. Consider in a (2,4) threshold signature system, $A = \{1,2,3,4\}$, $B = \{1,2\}$, each member $y_i, i \in B$ uses Eq. (4.2) to sign the message m:

$$s_1 \equiv \left(\left(\alpha^{f_1(0)} \cdot \left(\alpha^{f_3(x_1)\frac{0-x_2}{x_1-x_2}} \cdot \alpha^{f_4(x_1)\frac{0-x_2}{x_1-x_2}}\right)\right) \times H(m) \times \alpha^{d_1}\right) \bmod P'$$

$$\equiv \left(\left(\alpha^{f_1(0)+f_3(x_1)\frac{0-x_2}{x_1-x_2}+f_4(x_1)\frac{0-x_2}{x_1-x_2}}\right) \times H(m) \times \alpha^{d_1}\right) \bmod P'$$

$$s_2 \equiv \left(\left(\alpha^{f_2(0)} \cdot \left(\alpha^{f_3(x_2)\frac{0-x_1}{x_2-x_1}} \cdot \alpha^{f_4(x_2)\frac{0-x_1}{x_2-x_1}}\right)\right) \times H(m) \times \alpha^{d_2}\right) \bmod P'$$

$$\equiv \left(\left(\alpha^{f_2(0)+f_3(x_2)\frac{0-x_1}{x_2-x_1}+f_4(x_2)\frac{0-x_1}{x_2-x_1}}\right) \times H(m) \times \alpha^{d_2}\right) \bmod P'$$

Therefore

$$g^{s_1 \times s_2} \bmod P \equiv \left(g^{\alpha^{f_1(0)+f_2(0)+f_3(0)+f_4(0)}}\right)^{(H(m))^2 R} \bmod P$$

$$\equiv y^{(H(m))^2 R} \bmod P$$

The security analysis of this scheme is similar to that of the previous section and the difficulty of breaking is based on the problem of solving the discrete logarithm.

5. Conclusions

We have proposed two new schemes to solve the group-oriented (t,n) threshold signature problem. The securities of both schemes rely on the difficulty of solving the discrete logarithm problem. The first (t,n) threshold signature scheme is established with the assistance of a mutually trusted center. It is proved to be secure and efficient. Further, by withdrawing the mutually trusted center, the second (t,n) threshold signature scheme is constructed. The security is the same as the previous one, and the scheme seems more suitable for practical applications. The proposed schemes can withstand conspiracy attacks. Besides, a verifier can also trace back to check who the signers are.

References

[1] Y. Desmedt, Society and group oriented cryptography: a new concept, in: Advances in Cryptology, Proceedings of Crypto '87, Santa Barbara, August 1988, pp. 120–127.

[2] Y. Desmedt, Y. Frankel, Threshold cryptosystem, in: Advances in Cryptology, Proceedings of Crypto '89, Santa Barbara, August 1989, pp. 307–315.

[3] Y. Frankel, A practical protocol for large group oriented networks, in: Advances in Cryptology, Proceedings of Eurocrypt '89, Houlthalen, Belgium, April 1989, pp. 56–61.

[4] T. Hwang, Cryptosystem for group oriented cryptography, Lecture Notes in Computer Science, vol. 473, Springer-Verlag, Berlin, 1990, pp. 352–360.

[5] C.C. Chang, H.C. Lee, A new generalized group-oriented cryptoscheme without trusted centers, IEEE Journal on Selected Areas in Communications 11 (5) (1993) 725–729.

[6] I. Ingemarsson, G.J. Simmons, A protocol to set up shared secret schemes without the assistance of a mutually trusted party, Lecture Notes in Computer Science, vol. 473, Springer-Verlag, Berlin, 1990, pp. 266–282.

[7] C.S. Laih, L. Harn, Generalized threshold cryptosystem, in: Advances in Cryptology, Proceedings of Asiacrypt '91, Fujiyoshida, Japan, November 1991, pp. 88–92.

[8] T.P. Pedersen, A threshold cryptosystem without a trusted party, in: Advances in Cryptology, Proceedings of Eurocrypt '91, Brighton, UK, April 1991, pp. 522–526.

[9] D. Chaum, E. van Heyst, Group signature, in: Advances in Cryptology, Proceedings of Eurocrypt '91, Brighton, UK, April 1991, pp. 257–265.

[10] Y. Desmedt, Y. Frankel, Shared generation of authenticators, in: Advances in Cryptology, Proceedings of Crypto '91, Santa Barbara, August 1991, pp. 457–469.

[11] R.L. Rivest, A. Shamir, L. Addleman, A method for obtaining digital signatures and public-key cryptosystem, Comm. ACM 21 (2) (1978) 120–126.

[12] L. Harn, Group-oriented (t,n) threshold signature and digital multisignature, IEE Proceedings of Computers and Digital Techniques 141 (5) (1994) 307–313.

[13] A. Shamir, How to share a secret, Comm. ACM 22 (1979) 612–613.

[14] C.M. Li, T. Hwang, N.Y. Lee, (t,n) Threshold signature schemes based on discrete logarithm, in: Advances in Cryptology, Proceedings of Eurocrypt '94, Springer-Verlag, 1995, pp. 191–200.

[15] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. on Information Theory IT-31 (1985) 469–472.

[16] G.B. Agnew, R.C. Mullin, S.A. Vanstone, Improved digital signature scheme based on discrete exponentiation, Electronics Letters 26 (14) (1990) 1024–1025.

[17] S.D. Coute, C. deBoor, Elementary Numerical Analysis, McGraw-Hill, New York, 1972.

[18] L. Harn, S. Yang, Group-oriented undeniable signature schemes without the assistance of a mutually trusted party, in: Advances in Cryptology, Proceedings of Auscrypt '92, Springer-Verlag, 1993.