可追蹤簽署者之群體導向門檻簽章技術

Group-oriented Threshold Signature Schemes With Traceable Signers

王 清 德　　張 真 誠
Ching-Te Wang　Chin-Chen Chang

國立中正大學資訊工程研究所
Institute of Computer Science and Information Engineering.National Chung Cheng University. Chiayi. Taiwan. R.O.C.

林 祝 興
Chu-Hsing Lin

東海大學資訊科學系
Department of Computer and Information Sciences, Tunghai University. Taichung. Taiwan. R.O.C.

摘　要

本文首先提出一簽章技術，藉由相互信賴中心分配參數金匙，所有成員產生一群體公開金匙．簽章者各自獨立簽署一份文件，將此個別簽章經由系統秘書驗證，並產生一群體簽章。當群體簽章確認後，此技術在不洩漏金匙下，可避免非法者之共謀攻擊，更可追蹤出原始簽署人，以便確認簽章之責任歸屬。延伸此一技術，撤除信賴中心，我們亦設計出一群體導向門檻式簽章技術，並具有前述技術特性。此二法除具有 Harn 所提技術之各特性外，更能免於共謀攻擊，並追蹤簽署者責任歸屬問題。

關鍵字：相互信賴中心,群體導向簽章,門檻式簽章

Abstract

In this paper, we first present a new group-oriented (t, n) threshold signature scheme that requires the assistance of a mutually trusted center. The proposed scheme can withstand the conspiracy attacks without attaching a secret number. The group's public key is determined by all group members, each member signs a message independently and transmits the individual signature to a designated clerk. The clerk verifies the individual signature and combines them into a group signature. The verifier can authenticate the group signature and trace back to find signers. Further, by extending the scheme, we also develop another group-oriented (t, n) threshold signature scheme without the assistance of a mutually trusted center. The two proposed schemes possess all of the characteristics listed in Harn's scheme and are more difficult to break.

Keywords: Mutually Trusted Center, Group-oriented Signature, Threshold Signature

1. Introduction

In 1991, Chaum and Heyst [1] proposed an *(n, n)* group-oriented signature scheme, which used several groups' public keys in the system. At the same year, Desmedt and Frankel [2] proposed the concept of *(t, n)* threshold signature scheme based on the RSA [3] system. In the scheme, they applied a trusted key authentication center to determine the group's secret key and the secret keys of all group members. In 1994, Harn [4] used the cryptographic technique of Shamir's perfect secret sharing scheme [5] based on the Lagrange interpolating polynomial and digital signature algorithm to construct a *(t, n)* threshold signature scheme. His scheme is designed to partitioning the group secret key K into n different shadows. By collecting any t shadows, the group signature can be easily generated. Unfortunately, the schemes [2,4] may be suffered the conspiracy attacks and the secret keys can be revealed with high probability [6]. To avoid the attacks, the scheme [6] attach a random number to the secret key, which is concealed. Both of the schemes [4,6], there exist a problem that how to know who participate the signature, after the signature has been verified. As an example, there are t members with responsibility to sign the signature, make a company's policy decision, and obtain a great of profit. The company's manager intends to know the signers and will give an award for those decisions. An intuitive method to find the signers is that the trusted center make the t individual secret

keys public and authenticate the partial and group signature. In this case, the system requires renew the group secret and redistribute an individual secret key to each member. The cost is very expansive.

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 the conspiracy attacks without attaching a secret random number as in Li et al.'s scheme [6]. 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 solve 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 generate the legitimate group signature. Moreover, compared to Harn's scheme, our schemes are more difficult to break.

In the next section, we will propose a new *(t, n)* group-oriented threshold signature scheme with the assistance of a mutually trusted center. In Section 3, we propose a new *(t, n)* group-oriented threshold signature scheme in which the mutually trusted center is withdrawn. Finally, we make some conclusions in the last section.

2. A *(t, n)* Threshold Signature Scheme with the Assistance of a Mutually Trusted Center

In Harn's method [4], it employed Shamir's perfect secret sharing scheme [5], Lagrange interpolating polynomials, and ElGamal's signature scheme [7,8]. In Harn's *(t, n)* threshold signature scheme [4], 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. There are three phases in the scheme: (1).Group and individual secret keys generation phase. (2).Threshold signature generation phase.(3).Threshold signature verification phase. 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 [6] to our scheme are considered.

Lemma 2.1[9] If $x_1, x_2, \ldots, x_n$ are n distinct numbers and $y_1, y_2, \ldots, y_n$ are function values, respectively, then the Lagrange interpolating polynomial f of degree $n-1$ with the property that $f(x_k) = y_k$ 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, 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). Parameters 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 $f(x) \equiv a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod Q$ with degree $t-1$, where $0 < a_i < Q$, $i = 0,1,\ldots,t-1$, and a_i's 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 $y_i \equiv g^{\alpha^{f(x_i)}} \bmod P$, 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. If each member u_i selects a random number d_i, computes a value $r_i \equiv g^{\alpha^{d_i}} \bmod P$, and makes r_i publicly available by a broadcast channel. Once all r_i's are available, each member can compute the value R by

$$R \equiv \prod_{i=B} r_i \bmod P. \quad (2.1)$$

Next, 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

$$s_i \equiv \alpha^{f(x_i)} \times (H(m) \times \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}) + \alpha^{d_i} \times R \bmod P' \quad (2.2)$$

Then $\{m, s_i\}$ is transmitted to the designated clerk. Note that the designed clerk does not contain any secret information. He takes the responsibility to authenticate each individual signature and create a group signature. On receiving the individual signature $\{r_i, s_i\}$ from u_i, the clerk utilizes the public values x_i and y_i to compute the following equation and authenticate the validity of the partial signature :

$$g^{s_i} \stackrel{?}{=} r_i^R \times y_i^{H(m) \cdot \prod_{j\in B, j\neq i} \frac{0-x_j}{x_i-x_j}} \bmod P. \quad (2.3)$$

If the equation holds, the individual signature $\{r_i, s_i\}$ of the message m from u_i is valid. Further, the clerk uses subset B's t pairs public values (y_i, x_i) to construct a Lagrange polynomial function $h(y)$ as in Lemma 2.1, where

$$h(y) = \sum_{i=1}^{t} x_i \prod_{j=1, j\neq i}^{t} \frac{y - y_j}{y_i - y_j}. \quad (2.4)$$

Note that the roles of x_i and y_i are exchanged here.

(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

$$S \equiv \sum_{i=B} s_i \bmod P'. \quad (2.5)$$

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:

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

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

In step 2 and step 3, the individual and group signatures have been authenticated, but the verifier does not know who is the signer. If he intends to find out the singers, he can substitute the public value y_i to $h(y)$ as in Equation (2.4). If $h(y_i) = x_i$, then the signer with public value y_i is belongs to B. Otherwise, the member with public value y_i does not participate in the signature.

Theroem 2.1 If $g^S \equiv R^R \times y^{H(m)} \bmod P$, then the group signature $\{R, S\}$ of the message m is authentic.

Proof: In the second phase, the individual signatures $\{r_i, s_i\}$ of the message m satisfy the equations

$$g^{s_i} \equiv r_i^R \times y_i^{H(m) \cdot \prod_{j\in B, j\neq i} \frac{0-x_j}{x_i-x_j}} \bmod P.$$

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

$$\prod_{i=1}^{t} g^{s_i} \equiv \prod_{i=1}^{t} (r_i^R \times y_i^{H(m) \cdot \prod_{j\in B, j\neq i} \frac{0-x_j}{x_i-x_j}}) \bmod P. \quad (2.6)$$

The right hand side of Equation (2.6) can be rewritten as

$$(\prod_{i=1}^{t} r_i^R) \times (\prod_{i=1}^{t} y_i^{H(m) \cdot \prod_{j\in B, j\neq i} \frac{0-x_j}{x_i-x_j}}) \bmod P$$

$$\equiv (R^R)(g^{\sum_{i=1}^{t} \alpha^{f(x_i)} \cdot H(m) \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j}}) \bmod P$$

$$\equiv (R^R)(g^{\sum_{i=1}^{t} \alpha^{f(x_i)} \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j}})^{H(m)} \bmod P. \quad (2.7)$$

Let $h(x) = \alpha^{f(x)}$, by Lemma 2.1, Equation (2.7) can be rewritten as:

$$(R^R)(g^{\sum_{i=1}^{t} h(x_i) \prod_{j=1, j\neq i}^{t} \frac{0-x_j}{x_i-x_j}})^{H(m)} \bmod P$$
$$\equiv R^R (g^{h(0)})^{H(m)} \bmod P$$
$$\equiv R^R (g^{\alpha^{f(0)}})^{H(m)} \bmod P$$
$$\equiv R^R \times y^{H(m)} \bmod P$$

On the other hand, the left hand side of Equation (2.6) can be expressed by using Equation (2.5) as

$$\prod_{i=1}^{t} g^{s_i} \bmod P \equiv g^{\sum_{i=1}^{t} s_i} \bmod P \equiv g^S \bmod P .$$

Therefore, if $g^S \equiv R^R \times y^{H(m)} \bmod P$, then the group signature $\{R, S\}$ can be verified. Q.E.D.

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 there is an outsider wants to reveal the secret keys by knowing the public keys.

(1) To obtain the individual secret keys $\alpha^{f(x_i)} \bmod P$, for $i=1,2,...,n$, from the public keys $y_i \equiv g^{\alpha^{f(x_i)}} \bmod P$, obviously, 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 requires to solve the discrete logarithm problem.

Secondly, we assume that there is an attacker intends to reveal the secret keys from the signature.

(3) To drive the individual secret keys $\alpha^{f(x_i)} \bmod P$ from the signature pairs $\{r_i, s_i\}$'s by Equations (2.2). There are two unknown values $\alpha^{f(x_i)}$ and α^{d_i} in one equation, he cannot solve the problem, if he does not known the random value d_i.

(4) To drive the group secret key $f(0)$, from the signature pair $\{R, S\}$, by Equations (2.1) and (2.5).

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

If any t or more malicious members act in collusion, the term $\sum_{i=1}^{t} \alpha^{d_i} \cdot R$ can be determined, then they can find $\alpha^{f(0)}$. However, if $f(0)$ is further intended, it has to solve the discrete logarithm problem.

(5) To drive the secret polynomial function $f(x)$, from any t pairs $(x_i, \alpha^{f(x_i)})$ in collusion, they cannot reconstruct the function by 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 $r_i' \equiv g^{\alpha^{d_i'}} \bmod P$. Since the value $R' \equiv (\prod_{j=1, j\neq i}^{t} r_j) \times r_i' \bmod P$ is computed by all t members, without knowing the individual secret key $\alpha^{f(x_i)}$, the forger cannot obtain a correct signature pair $\{r_i', s_i'\}$ to satisfy Equation (2.3). 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. However, the security of our scheme is based on the difficulty of solving the discrete logarithm problem. Obviously, the security of our method will be increased.

3. 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 mutually trusted center existed, more parameters and complicated computations are required. The scheme is also divided into three phases as the following:

(1). Parameters selection and secret keys generation

phase.

Here. the parameters H, P, P', Q, g, α will be defined as in the previous section. Each member. say u_i. randomly selects a public value $x_i \in [1, Q-1]$, a secret polynomial 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 as $y \equiv \prod_{i \in A} y_i \bmod P$. 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 member u_j. where

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

(2) Individual signature generation and verification phase.

Assume there are t members representing the group to sign a message m. In the scheme. all of the members can sign the message at the same time. Member u_i selects a random number d_i. computes a value $r_i \equiv g^{\alpha^{d_i}} \bmod P$, and makes r_i publicly known by a broadcast channel. Once all r_i's are available. each member can compute the value R by

$$R \equiv \prod_{i=1}^{t} r_i \bmod P. \qquad (3.1)$$

Member u_i 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:

$$s_i \equiv ((\alpha^{f_i(0)} + \sum_{j \in A, j \notin B} \alpha^{f_j(x_i)} \times \prod_{l \in B, l \neq i} \frac{0 - x_j}{x_i - x_l}) H(m) + \alpha^{d_i} \times R \bmod P, \qquad (3.2)$$

and transmits $\{m, s_i\}$ to a designated clerk. Here. the individual signature $\{r_i, s_i\}$ is a partial signature of the message m. On receiving the individual signature $\{r_i, s_i\}$. the clerk uses the public key x_i, y_i and y_{ji} for $j \in A, j \notin B$. and the partial signature $\{r_i, s_i\}$ to check whether the following equation is true:

$$g^{s_i} \stackrel{?}{=} r_i^R \times (y_i \times \prod_{j \in A, j \in B} y_{ji}^{\prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}})^{H(m)} \bmod P$$

If the equation holds. the partial signature $\{r_i, s_i\}$ 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 public values (y_{ji}, x_i) to construct Lagrange polynomial function $h_j(y)$ as in Lemma 2.1. where

$$h_j(y) = \sum_{i=1}^{t} x_i \prod_{l=1, l \neq i}^{t} \frac{y - y_{jl}}{y_{ji} - y_{jl}}. \qquad (3.3)$$

(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 obtained as $\{R, S\}$. where

$$S \equiv \sum_{i \in B} s_i \bmod P'. \qquad (3.4)$$

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

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

If the equation holds. the group signature $\{R, S\}$ is valid. Similarly. to find the singers. we can substitute the public value y_{ji} to $h_j(y)$ as in Equation (3.3). If $h_j(y_{ji}) = x_i$. then the signer with public value y_{ji} is belongs to B. Otherwise. the member with public value y_{ji} does not participate in the signature.

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

Proof : In the second phase. the individual signatures $\{r_i, s_i\}$ of the message m satisfy the equations

$$g^{s_i} \equiv r_i^R \times (y_i \times \prod_{j \in A, j \in B} y_{ji}^{\prod_{l \in B, l \neq i} \frac{0 - x_l}{x_i - x_l}})^{H(m)} \bmod P.$$

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

$$\prod_{i=1}^{t} g^{s_i} \equiv \prod_{i=1}^{t} (r_i^R \times (y_i \times \prod_{j \in A, j \in B} y_{ji}^{\prod_{i \neq j, i \in B} \frac{0-x_i}{x_j - x_i}})^{H(m)}) \bmod P \quad (3.5)$$

By using Equation (3.4), the left hand side of Equation (3.5) can be rewritten as

$$\prod_{i=1}^{t} g^{s_i} \bmod P \equiv g^{\sum_{i=1}^{t} s_i} \bmod P \equiv g^S \bmod P$$

On the other hand, the right hand side of Equation (3.5) can be expressed by using Equation(3.1) as

$$(\prod_{i=1}^{t} r_i)^R \times (\prod_{i=1}^{t} (y_i \times \prod_{j \in A, j \in B} y_{ji}^{\prod_{i \neq j, i \in B} \frac{0-x_i}{x_j - x_i}})^{H(m)}) \bmod P$$

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

Therefore, the group signature $\{R, S\}$ can be verified. Q.E.D.

The security analysis of this scheme is similar to that of the previous section. However, this scheme does not need the assistance of a mutually trusted center. From the discussions of Sections 2 and 3, two *(t, n)* threshold signature schemes, with or without the assistance of a mutually trusted center respectively, are established. Any t members in a group can represent the group to sign a message and an outsider can use a group public key to authenticate the validity of the group signature. Any subgroup of less than t members cannot generate the legitimate group signature or authenticate the validity of the signature. Moreover, the security of both schemes proposed is based on the difficulty of solving the discrete logarithm problem.

4. 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 under 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 the conspiracy attacks. Besides, a verifier can also trace back to find the signers.

References

[1] D. Chaum and E. van Heyst, "Group Signature," In Advances in Cryptology, Proc. of Eurocrypt '91, Brighton, UK, April 1991, pp. 257-265.

[2] Y. Desmedt, and Y. Frankel, "Shared Generation of Authenticators," In Advances in Cryptology, Proc. of Crypto '91, Santa Barbara, August 1991, pp. 457-469.

[3] R.L. Rivest, A. Shamir, and L. Addleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem ," Comm. ACM, Vol. 21, No. 2, Feb. 1978, pp. 120-126.

[4] L. Harn, "Group-oriented *(t, n)* Threshold Signature and Digital Multisignature", IEE Proceedings-Computers and Digital Techniques, Vol. 141, No. 5, Sept. 1994, pp. 307-313.

[5] A. Shamir, "How to Share a Secret," Comm. ACM, Vol. 22, 1979, pp. 612-613.

[6] C. M. Li, T. Hwang and N. Y. Lee, "*(t, n)* Threshold Signature Schemes Based on Discrete Logarithm," Advances in Cryptology, Eurocrypt'94 Proceedings, Springer-Verlag, 1995, pp.191-200.

[7] T. ElGamal, "A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, Vol. IT-31, 1985, pp. 469-472.

[8] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, "Improved Digital Signature Scheme Based on Discrete Exponentiation," Electronics Letters, Vol. 26, No 14, July 1990, pp. 1024-1025.

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