1998 International Computer Symposium
Workshop on Cryptology and Information Security
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

GROUP-ORIENTED UNDENIABLE SIGNATURE SCHEMES WITHOUT A TRUSTED CENTER

Narn-Yih Lee[1] and Tzonelih Hwang[2]

[1]Department of Applied Foreign Language, Nan-Tai Institute of Technology, Tainan
Email: nylee@nantai.ntc.edu.tw
[2]Institute of Information Engineering, National Cheng-Kung University, Tainan
Email: hwangtl@server2.iie.ncku.edu.tw

ABSTRACT

At Auscrypt'92, Harn and Yang firstly propose the concept of group-oriented undeniable signatures. Two threshold undeniable signature schemes were devised in their paper to realize the $(1, n)$ and (n, n) cases. However, Langford in 1996 showed that Harn-Yang's (n, n) threshold undeniable signature scheme is not secure enough by presenting a conspiracy attack on it. Recently, Lin et al. also proposed a new (t, n) threshold undeniable signature scheme. Unfortunately, the Langford attack can be applied to Lin et al.'s scheme as well. Thus, the problem of designing a general group-oriented (t, n) threshold undeniable signature scheme is remained open. This paper will try to solve the open problem by proposing a general (t, n) threshold undeniable signature scheme without the assistance of a mutually trusted party. Moreover, this paper will extend the signing policy to the generalized case and propose a generalized group-oriented undeniable signature scheme.

Keywords: Digital Signature, Group-Oriented Undeniable Signature, Lagrange Interpolating Polynomial, Undeniable Signature.

1. INTRODUCTION

An undeniable signature, like a digital signature, is a number, which is generated from the message and the signer's secret key. But unlike a digital signature, an undeniable signature cannot be verified without the signer's consent. An undeniable signature scheme was firstly invented by Chaum and Antwerpen [1] in 1989. Later, Chaum also proposed a zero-knowledge undeniable signature scheme [2] based on discrete logarithms.

Group-oriented activities play a very important role in the modern society. A group-oriented signature scheme is a method which allows a group to decide its signing policy in such a way that only the authorized subsets of this group can cooperate to sign a message. If the authorized subsets are any set of t members of this group, then it is called a *threshold signature scheme* [3][4][5]. If the authorized subsets are arbitrarily specified, then it is termed as the *generalized group-oriented signature scheme.*

In 1992, Harn and Yang [6] incorporated both concepts of the undeniable signature and the group-oriented signature to devise $(1, n)$ and (n, n) threshold undeniable signature schemes. The responsibility of signing a signature can be shared by an authorized subset. Besides, the verification of a signature needs the agreement of an authorized subset. It is quite useful for many applications. However, Langford [11] showed that Harn-Yang's (n, n) threshold undeniable signature scheme has an actual security of only 2-out-of-n. That is, any two adjacent signers can collude to sign an arbitrary message successfully. Later, Lin, Wang and Chang [12] proposed a (t, n) threshold undeniable signature scheme without a trusted center. Any t members in a group can represent the group to sign a message and a verifier can verify the validity of the undeniable signature with the consent of any t members in the original group. Unfortunately, the Langford attack [9] can be applied to Lin-Wang-Chang's scheme [12] as well. Thus, this paper will try to propose new group-oriented undeniable signature schemes which can prevent from the Langford attack.

Based on Chaum's zero-knowledge undeniable signature scheme [2], we are going to propose a (t, n) threshold undeniable signature scheme without a trusted center, where $1 \leq t \leq n$. Moreover, we will try to extend the signing policy to the generalized case. In 1991, Laih and Harn [10] proposed gen-

eralized threshold cryptosystems for group-oriented secret communications. However, Langford [11] also showed that their second scheme without a trusted center is insecure for some access structures. But, Laih-Harn's second scheme can be modified to avoid the Langford attack by simply adding an one way hash function on it. Based upon the modified Laih-Harn generalized threshold cryptosystem, we are going to propose a generalized group-oriented undeniable signature scheme. In the new proposed group-oriented undeniable signature schemes, any authorized subset in the group can cooperate to sign a message. Further, with the consent of any authorized subset, a verifier can verify the validity of the undeniable signature. The security of both schemes are based on the discrete logarithm problem.

The rest of this paper is organized as follows. In Section 2, we will propose a new (t, n) threshold undeniable signature scheme. A generalized group-oriented undeniable signature scheme will be presented in Section 3. Finally, concluding remarks will be made in Section 4.

2. A (t, n) THRESHOLD UNDENIABLE SIGNATURE SCHEME

In this section, a (t, n) threshold undeniable signature scheme without the assistance of a trusted center will be proposed on the basis of Chaum's zero-knowledge undeniable signature scheme [2].

[*System setup phase*]

The method proposed by Pedersen [9] for threshold cryptosystem without a trusted party is modified here and applied in this phase. Assume that there are n members, say U_1, U_2, ..., U_n, in the group. Let A ($|A| = n$) be the set of all members in the group. B ($|B| = t$, $t \leq n$), any subset of size t in A, is authorized to generate group undeniable signatures. Firstly, all users cooperate to generate the following system parameters: P, p and α, where P, p are large primes, $P = 2p + 1$, and α is an element of order p in $GF(P)$. $H()$ is a collision free one way hash function.

Then, each member U_i executes the following steps to generate the secret keys of all group members and a group public key.

Step 1. U_i randomly selects a secret number s_i and a public value x_i between 0 and p.

Step 2. U_i computes a value $y_i = \alpha^{s_i} \bmod P$ and generates a commitment $Blob(d_i, y_i)$, where d_i is a random number. Then, he/she broadcasts $Blob(d_i, y_i)$. Upon all $Blob(d_i, y_i)$, $i \in A$, are published, U_i opens $Blob(d_i, y_i)$. The group public key Y is calculated as $Y = \prod_{i \in A} y_i \bmod P$ and the corresponding group secret key S is equivalent to $S = \sum_{i \in A} s_i \bmod p$.

Step 3. U_i randomly selects a secret polynomial $f_i(x)$ of degree $(t-1)$ over $GF(p)$, $f_i(x) = f_{i,0} + f_{i,1}x + \cdots + f_{i,t-1}x^{t-1} \bmod p$, such that $f_i(0) = f_{i,0} = s_i$.

Step 4. U_i secretly distributes a $s_{i,j} = f_i(x_j) \bmod p$ to U_j, where x_j is U_j's public value and $j = 1, 2, ..., n$.

Step 5. U_i computes his secret key S_i as $S_i = \sum_{j=1}^{n} s_{j,i} \bmod p$.

Let $F(x)$ be the polynomial over $GF(p)$:
$F(x) = f_1(x) + \cdots + f_n(x) \bmod p$.
Then, $S_i = f_1(x_i) + \cdots + f_n(x_i) = F(x_i) \bmod p$ for every $i = 1, 2, ..., n$. Thus, the secret key S_i of user U_i is a share of $F(0) = \sum_{i=1}^{n} s_i \bmod p$ [9].

[*Undeniable signature generation phase*]

Assume that t users $U_1, U_2, ..., U_t$ in the signing group want to generate a group undeniable signature on the message M. They do the following:

Step 1. Each user U_i computes a hash value $M_h' = H(M) \bmod P$. If the order of M_h' modulo P is $P-1$, let $M_h = (M_h')^2 \bmod P$. Otherwise, let $M_h = M_h'$ (see Remark 1).

Step 2. Each user U_i computes a partial undeniable signature z_i,

$$z_i = M_h^{(S_i \prod_{U_j \in B, U_j \neq U_i} \frac{-x_j}{x_i - x_j}) \bmod p} \bmod P,$$

and sends z_i to a designated combiner.

Step 3. Upon receiving t partial undeniable signatures, the designated combiner computes a Z by

$$Z = \prod_{U_i \in B} z_i \bmod P$$
$$= M_h^{(\sum_{U_i \in B} S_i \prod_{U_j \in B, U_j \neq U_i} \frac{-x_j}{x_i - x_j}) \bmod p} \bmod P$$
$$= M_h^{F(0)} = M_h^S \bmod P.$$

Z is the group undeniable signature of M.

Remark 1: Assume that P and p are two large prime numbers and $P = 2p+1$, the order of an unspecified number M'_h modulo P will be $2p$, p or 2. If the order of M'_h modulo P is $2p$, let $M_h = (M'_h)^2 \bmod P$. Then, the order of M_h modulo P will be p [8]. On the other hand, if the order of M'_h modulo P is 2, M'_h shall be 1 or $P-1$. The probability of having the hash value M'_h=1 or $P-1$ is only $\frac{2}{p}$, which is extremely low and can be almost neglected. Therefore, the order of M_h modulo P can be assumed to be p.

[*Undeniable signature verification phase*]

Assume that a set $B = \{U_1, U_2, ..., U_t\}$ of arbitrary t members (not necessary the same as those who generate the signature) in the group agrees to help the verifier V to verify the group undeniable signature Z of the message M. These t members in B cooperate to do the following steps:

Step 1. V computes M_h as stated before. Then, V randomly selects two integers a and b from $GF(p)$, and computes $W = M_h^a \alpha^b \bmod P$. W is sent to B.

Step 2. Each user U_i in B chooses a random number k_i from $GF(p)$ and computes the value $\alpha^{k_i} \bmod P$. Then, α^{k_i} is broadcasted to all members in B. Then, U_i computes R_1,
$R_1 = W \prod_{U_i \in B} \alpha^{k_i} = W\alpha^{\sum_{U_i \in B} k_i} \bmod P$.
Moreover, U_i computes $R_{2,i}$,
$$R_{2,i} = R_1^{(S_i \prod_{U_j \in B, U_j \neq U_i} \frac{-x_j}{x_i - x_j}) \bmod p} \bmod P.$$
Similarly, $R_{2,i}$ is broadcasted to all members in B. Then, R_2 is calculated as $R_2 = \prod_{U_i \in B} R_{2,i} \bmod P$. R_1 and R_2 are sent back to V.

Step 3. V sends a and b to B.

Step 4. The member U_i in B checks whether $W = M_h^a \alpha^b \bmod P$. If it does hold, then $k = \sum_{U_i \in B} k_i \bmod p$ is revealed to V.

Step 5. V checks whether $R_1 = W\alpha^k \bmod P$ and $R_2 = Z^a Y^{b+k} \bmod P$. If these two equations do hold, the group undeniable signature is verified.

[*Disavowal phase*]

Any t members (not necessary the same as those who generate/verify the signature) can prove that whether the signature is generated by their group or not. To do this, these t members in B and the verifier choose a mutually agreed constant l, e.g. l=1023.

Step 1. V randomly selects an integer q between 0 and l and chooses c from $GF(p)$, then computes $e_1 = M_h^q \alpha^c \bmod P$ and $e_2 = Z^q Y^c \bmod P$. Then e_1 and e_2 are sent to B.

Step 2. All members in B cooperate to determine the value of q by trial and error. Besides, Each member U_i in B randomly chooses an integer d_i and uses $Blob(d_i, q)$ to commit q. $Blob(d_i, q)$'s are sent back to V, $1 \leq i \leq t$.

Step 3. V sends c to B.

Step 4. Each member U_i in B checks whether $e_1 = M_h^q \alpha^c \bmod P$ and $e_2 = Z^q Y^c \bmod P$. If they do hold, then U_i reveals d_i to V, $U_i \in B$.

Step 5. V opens all blobs. If the values committed by t blobs are equivalent to q, Z is not generated by the group.

[*Correctness*]

The following theory proves the correctness of the proposed scheme.

Theorem 1: The proposed scheme is a (t, n) threshold undeniable signature scheme.
<Proof> Let $F(x)$ be the polynomial over $GF(p)$: $F(x) = f_1(x) + \cdots + f_n(x) \bmod p$.
$S_i = f_1(x_i) + \cdots + f_n(x_i) = F(x_i) \bmod p$ for every $i = 1, 2, ..., n$. Thus the secret key S_i of user U_i generated in the System setup phase is a share of $F(0) = \sum_{i=1}^{n} s_i \bmod p$.

By Lagrange Interpolation Scheme, the group secret key $\sum_{i=1}^{n} s_i \bmod p$ can be computed from any t integer pairs (x_1, S_1),(x_2, S_2), ...,(x_t, S_t) by the following equation:
$\sum_{i=1}^{n} s_i \bmod p$
$= F(0) \bmod p$
$= \sum_{U_i \in B} S_i (\prod_{U_j \in B, U_j \neq U_i} \frac{-x_j}{x_i - x_j}) \bmod p$
Hence, following the Undeniable signature generation phase, these t group members, $U_1, U_2, ..., U_t$, will generate a value Z
$$Z = M^{\sum_{U_i \in B} S_i (\prod_{U_j \in B, U_j \neq U_i} \frac{-x_j}{x_i - x_j}) \bmod p} \bmod P,$$
which is a valid group signature.

Similarly, during the Step 2 of the Undeniable signature verification phase and the step 1 of the

Disavowal phase, the users in B will generate values R_2 and $e_1^{\sum_{i=1}^{n} s_i} \bmod P$ respectively, which are used to check the validity of the signature and disavow the generation of the signature. (Q.E.D.)

[*Security Analysis*]

The group secret key S cannot be derived from the group public key Y or the group undeniable signature Z unless one can solve the discrete logarithm problem. Due to the same reasons, the secret keys of members will not be revealed during the Undeniable signature verification phase and the Disavowal phase.

According to the Lagrange interpolating scheme [7], less than t members cannot reconstruct the secret value $F(0)$ correctly. Thus, less than t members cannot generate, verify or disavow group signatures. Because our scheme is based on Chaum's zero-knowledge undeniable signature scheme, the security of our scheme is the same as Chaum's scheme [2]. Moreover, each signer knows what message he/she does sign and release his/her partial undeniable signature simultaneously. Thus, our scheme can avoid the Langford attack.

3. GENERALIZED GROUP-ORIENTED UNDENIABLE SIGNATURE SCHEME

In this section, a generalized group-oriented undeniable signature scheme will be proposed on the basis of the modified Laih-Harn generalized threshold cryptosystem.

[*System setup phase*]

Let A denote the set of all members in the group and $B = B_1 + B_2 + ... + B_r$ denote the collection of all authorized subsets in A, such that the valid group signature can be generated by the cooperation of the members in B_i, $1 \le i \le r$. As similar to the previously proposed threshold case, all users cooperate to determine the public values P, p and α where P and p are values as described before. α is a element of order p in $GF(P)$.

Each member U_i, $i \in A$, randomly selects a secret key s_i $(0 < s_i < p-1)$ and computes a value $y_i = \alpha^{s_i} \bmod P$. Then, he/she generates and broadcasts a commitment $Blob(d_i, y_i)$, where d_i is a random number. Upon all $Blob(d_i, y_i)$, $i \in A$, are published, U_i opens $Blob(d_i, y_i)$. The group public key Y is calculated as $Y = \prod_{i \in A} y_i \bmod P$ and the corresponding group secret key S is equivalent to $S = \sum_{i \in A} s_i \bmod p$.

Any member U_i who does not belong to the authorized subset B_j has to compute a public value $T_{i,j}$ which satisfies

$$s_i = \sum_{h \in B_j} H(K_{i,h}, j) + T_{i,j} \mod p, \qquad (1)$$

where $K_{i,h} = y_h^{s_i} = \alpha^{s_i s_h} = y_i^{s_h} = K_{h,i} \bmod P$ and j is the authorized subset number in the group. $H()$ is a collision free one way hash function.

[*Undeniable signature generation phase*]

Assume that the authorized subset B_j wants to generate a group undeniable signature on the message M. Each member U_i, $U_i \in B_j$, computes a Z_i,

$$Z_i = M^{s_i} \prod_{h \notin B_j} M^{H(K_{h,i},j)} \bmod P, \qquad (2)$$

where $K_{h,i}$ is the common secret key between members U_i and U_h $(h \notin B_j)$. Then, U_i broadcasts Z_i. Once all Z_i's, $i \in B_j$, have been published, The group undeniable signature Z of the message is computed as

$$\begin{aligned}
& Z \\
= & \Big(\prod_{i \in B_j} Z_i\Big)\Big(\prod_{h \notin B_j} M^{T_{h,j}}\Big) \\
= & \Big(\prod_{i \in B_j} \big(M^{s_i} \prod_{h \notin B_j} M^{H(K_{h,i},j)}\big)\Big)\Big(\prod_{h \notin B_j} M^{T_{h,j}}\Big) \\
= & \Big(\prod_{i \in B_j} M^{s_i}\Big)\Big(\prod_{i \in B_j} \prod_{h \notin B_j} M^{H(K_{h,i},j)}\Big)\Big(\prod_{h \notin B_j} M^{T_{h,j}}\Big) \\
= & \Big(\prod_{i \in B_j} M^{s_i}\Big)\Big(\prod_{h \notin B_j} M^{\sum_{i \in B_j} H(K_{h,i},j)+T_{h,j}}\Big) \\
= & \Big(\prod_{i \in B_j} M^{s_i}\Big)\Big(\prod_{h \notin B_j} M^{s_h}\Big) \\
= & M^S
\end{aligned}$$

[*Undeniable signature verification phase*]

Assume that an authorized subset B_j agrees to verify the group undeniable signature Z of the message M for the verifier V.

Step 1. V randomly selects two integers a and b, and computes $W = M^a \alpha^b \bmod P$. W is sent to B_j.

Step 2. Each member U_i in B_j chooses a random number k_i and computes the value $\alpha^{k_i} \bmod P$. Then, α^{k_i} is broadcasted to all members in B_j. Then, U_i computes the $R_1 = W \prod_{U_i \in B_j} \alpha^{k_i} = W\alpha^{\sum_{U_i \in B_j} k_i} \bmod P$. Moreover, all members in B_j cooperate to compute a R_2, $R_2 = R_1^S \bmod P$. (similar as the undeniable signature generation phase) R_1 and R_2 are sent back to V.

Step 3. V sends a and b to B_j.

Step 4. The member U_i in B_j checks whether $W = M^a\alpha^b \bmod P$. If it does hold, then $k = \sum_{U_i \in B_j} k_i \bmod p$ is revealed to V.

Step 5. V checks whether $R_1 = W\alpha^k \bmod P$ and $R_2 = Z^a Y^{b+k} \bmod P$. If these two equations do hold, the group undeniable signature is verified.

[*Disavowal phase*]

Assume that an authorized subset B_j in A wishes to prove that the group signature, Z, is not generated by A. To do this, the B_j and the verifier choose a mutually agreed constant l, e.g. l=1023.

Step 1. V randomly selects an integer q between 0 and l and chooses a random c, then computes $e_1 = M^q\alpha^c \bmod P$ and $e_2 = Z^q Y^c \bmod P$. Then e_1 and e_2 are sent to the B_j.

Step 2. All members in B_j cooperate to determine the value of q by trial and error. Besides, each member U_i in B_j randomly chooses an integer d_i and uses $Blob(d_i, q)$ to commit q. $Blob(d_i, q)$'s are sent back to V, $U_i \in B_j$.

Step 3. V sends c to the B_j.

Step 4. Each member U_i in B_j checks whether $e_1 = M^q\alpha^c \bmod P$ and $e_2 = Z^q Y^c \bmod P$. If they do hold, then U_i reveals d_i to V, $U_i \in B_j$.

Step 5. V opens all blobs. If the values committed by all blobs are equivalent to q, Z is not generated by the group.

[*Security Analysis*]

The group secret key S cannot be derived from the group public key $Y = \alpha^S \bmod P$ or a group signature $Z = M^S \bmod P$ unless one can solve the discrete logarithm problem. Since p is a large prime, the secret value s_i of a member U_i will not be derived from his/her public value $y_i = \alpha^{s_i} \bmod P$.

Instead of $K_{i,h}$, the common secret value $H(K_{i,h}, j)$ between members i and h is used to generate $T_{i,j}$. It is hard to compute the hash value $H(K_{i,h}, j)$ for a malicious user without knowing $K_{i,h}$. Moreover, the hash value $H(K_{i,h}, j)$ is different from the hash value $H(K_{i,h}, k)$, $j \neq k$. Therefore, the malicious user cannot use the Langford attack to reveal the secret keys of the other users.

Since the group secret key S can be computed from the following congruence
$S = \sum_{i \in A} s_i \bmod p$
$= \sum_{i \in B_j} s_i + \sum_{i \notin B_j} (\sum_{h \in B_j} H(K_{i,h}, j) + T_{i,j})$,
it is obvious that a valid group signature can be derived only when *all* users in the authorized subset B_j are present. Similarly, only the authorized subsets can help the verifier to verify the validity of a group undeniable signature.

4. CONCLUSIONS

This paper has proposed a new (t, n) threshold undeniable signature scheme to solve the open problem proposed by Harn and Yang. Moreover, we have extended the signing policy to the generalized case, and proposed a new scheme based on modified Laih-Harn generalized threshold cryptosystem. Since a group public key is constructed by all group members, any authorized subset in the group can work together to generate, verify and disavow a group undeniable signature.

Acknowledgement. This work was supported by the National Science Council of Republic of China under the contract number NSC87-2213-E006-001.

5. REFERENCES

[1] D. Chaum and H. V. Antwerpen, "Undeniable Signatures", *Advances in Cryptography: Proceedings of Crypto '89*, pp. 212-216, 1989.

[2] D. Chaum, "Zero-Knowledge Undeniable Signatures", *Advances in Cryptography: Proceedings of Eurocrypt '90*, pp. 458-464, 1990.

[3] Y. Desmedt, and Y. Frankel, "Shared Generation of Authenticators and Signatures", *Advances in Cryptography: Proceedings of Crypto '91*, pp. 457-469, 1991.

[4] L. Harn, "Group-Oriented (t,n) Threshold Digital Signature Scheme and Digital Multisignature", *IEE Proc.-Comput. Digit. Tech.*, Vol. 141, No. 5, pp.307-313, Sep., 1994.

[5] C.M. Li, T. Hwang and N.Y. Lee, "Threshold-Multisignature Schemes where Suspected Forgery Implies Traceability of Adversarial Shareholders", *Advances in Cryptology - EuroCrypto '94, Proceedings*, Springer Verlag, 1994.

[6] L. Harn, and S. Yang, "Group-Oriented Undeniable Signature Schemes without the Assistance of a Mutually Trusted Party", *Advances in Cryptography: Proceedings of Auscrypt '92*, pp. 133-142, 1992.

[7] A. Shamir, "How to Share a Secret", *Communications of the Association for Computing Machinery*, Vol. 22, No.11, pp. 612-613, 1979.

[8] K.H. Rosen, "Elementary Number Theory and Its Applications", *Addison-Wesley Publishing Company*, Second Edition, pp. 249-254, 1987.

[9] T.P. Perdersen,"A Threshold Cryptosystem without a Trusted Party", *Advances in Cryptography: Proceedings of Eurocrypt '91*, pp. 522-526, 1991.

[10] C.S. Laih, and L. Harn, "Generalized Threshold Cryptosystem", *Advances in Cryptography: Proceedings of AsiaCrypt '91*, pp. 88-92, 1991.

[11] S.K. Langford, "Weaknesses in some threshold cryptosystems", *Advances in Cryptography: Proceedings of Crypto '96*, pp. 74-82, 1996.

[12] C.H. Lin, C.T. Wang and C.C. Chang, "A group-oriented (t,n) undeniable signature scheme without trusted center", *First Australasian Conference, ACISP'96*, pp. 266-274, 1996.