http://www.zju.edu.cn/jzus; E-mail: jzus@zju.edu.cn
ISSN 1009-3095 *Journal of Zhejiang University SCIENCE* V.5, No.1, P.50-54, Jan., 2004

Verifiable threshold signature schemes against conspiracy attack

GAN Yuan-ju(甘元驹)†

(*College of Information Science and Engineering, Central South University, Changsha 410075, China*)

†E-mail: yjgan@eyou.com

Received Mar.30, 2003; revision accepted June 22, 2003

Abstract: In this study, the author has designed new verifiable (t, n) threshold untraceable signature schemes. The proposed schemes have the following properties: (1) Verification: The shadows of the secret distributed by the trusted center can be verified by all of the participants; (2) Security: Even if the number of the dishonest member is over the value of the threshold, they cannot get the system secret parameters, such as the group secret key, and forge other member's individual signature; (3) Efficient verification: The verifier can verify the group signature easily and the verification time of the group signature is equivalent to that of an individual signature; (4) Untraceability: The signers of the group signature cannot be traced.

Key words: Cryptography, Threshold group signature, Conspiracy attack, Forgery attack
Document code: A **CLC number:** TP309

INTRODUCTION

Digital signatures play an important role in our modern electronic society due to their properties of integrity and authentication. The integrity property ensures that the received message is not modified, and the authentication property ensures that the sender is not impersonated. In well-known that in conventional digital signatures, such as RSA and DSA, a single signer is sufficient to produce a valid signature; and that anyone can verify the validity of any given signature. However, on many occasions, we need to share the responsibility of signing the message with a set of signers. Issuing checks for a company is an example of this. For the sake of security, it may be a policy of a company that checks must be signed by a group of individuals rather than by one person. Threshold signature schemes and multi-signature schemes are designed to solve such problems. There are two major differences between multi-signature and threshold signature schemes. Firstly, it is not necessary to restrict the number of signers to generate a valid signature in a multi-signature scheme. In contrast to a multi-signature scheme, a threshold value t must be predetermined to guarantee the security of the system in a threshold signature scheme. Secondly, a threshold signature represents the signature signed by the group, while a multi-signature is a signature which represents a set of individuals who sign the message. Consequently, a threshold signature is suitable for the case where the members of a group are allowed to sign on behalf of the group.

Desmedt and Frankel (1992) proposed the concept of a (t, n) threshold signature scheme based on RSA 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 (1994) used the cryptographic technique of Shamir's perfect secret sharing which is based on the Lagrange interpolating polynomial and digital signature algorithm to construct a (t, n) threshold signature scheme designed to partition the group secret key K into n different shadows. By collecting any of the t shadows, the group signature can be easily generated. However, Li *et al.* (1995) pointed out that Desmedt and Frankel's scheme and Harn's scheme may suffer from conspiracy attacks and the secret keys can be revealed if t or more participants act in collusion. To avoid conspiracy attacks, the proposed schemes (Li *et al.*, 1995) attach a random number to the secret key held by each member, so that the security of their schemes is guaranteed. But, the additional random number makes the (t, n) threshold sign-

atures schemes have the property of traceability. However, Michels and Horster(1997), Wang *et al*.(2000;2001) pointed out that threshold signature schemes (Li *et al*., 1995)are vulnerable to forgery attack by an insider attacker. Wang *et al*.(1998) proposed two new (t, n) threshold signature schemes with traceable signers that can withstand conspiracy attacks without attaching a secret number. However, Tseng and Jan(1999) and Li *et al*.(2001) showed that the proposed schemes are insecure by presenting a forgery attack on them. Lee *et al*.(2000) proposed a (t, n) threshold signature with untraceability. In their scheme, the group signature can be verified by any outsider without the need to identify the identities of the signers. However, t or more shareholders can reveal the group secret key if they conspire attack.

To prevent cheating by the dealer, Verifiable Secret Sharing(VSS) was first proposed by Chor *et al*.(1985). VSS schemes allow each participant to verify that his share is consistent with the other shares, and hence allow the honest participants to ensure that the secret to be reconstruct is unique.

In this study, the author has designed new verifiable (t, n) threshold untraceable signature schemes by employing both the idea of a (t, n) threshold untraceable signature (Lee *et al*., 2000) and the idea of VSS(Chor *et al*., 1985).

PROPOSED SCHEME

The verifiable (t, n) threshold untraceable signature scheme uses a mutually trusted center. The word "trusted" implies that the trusted center must ensure that the secret information is not disclosed or revealed to unauthorized people and prevent unauthorized alteration or destruction of data.

The scheme consists of four phases: the system initiation phase, the distribution of secret shadows and verification phase, the partial signature generation phase, and the group signature generation and verification phase. The four phases detailed below.

Phase 1 System Initialization Phase

The system contains a mutually trusted center responsible for selecting all parameters. Assume that there are n members in a group, and the set of group members is denoted as A. Here $|A| = n$. Any t legitimate members of A can represent the group to sign a message m. The set of any t legitimate members of A is denoted as B. Note that $|B| = t$. The mutually trusted center selects the following parameters:

A number, $N = p \cdot q = (2p' + 1) \cdot (2q' + 1)$, where p, q, p' and q' are distinct large safe primes.

A generator g with order $v = p' \cdot q'$ in Z_N^*.

A system public value e such that $\gcd(e, v) = 1$, where $e \cdot d = 1 \bmod v$ and d is a system secret value.

A one-way hash function $h()$.

A secret polynomial function

$$f(x) = c_{t-1}x^{t-1} + \cdots + c_1 x + c_0 \bmod v \quad (1)$$

with degree $t - 1$, where $c_{t-1}, \cdots, c_1, c_0 \in Z_v^*$, and computes

$$f_k = g^{c_k} \bmod N \quad (2)$$

where $k = 0, 1, \ldots, t - 1$.

A secret key x and a public key y, where

$$x = f(0) \bmod v, \text{and} \quad (3)$$

$$y = g^x \bmod N. \quad (4)$$

Thus, the mutually trusted center publishes $e, y, N, g, h()$ and f_k, and keeps d, x, v, p, q, p' and q' in secret.

Phase 2 Distribution of Secret Shadows and Verification Phase

For each group member U_i with a public value ID_i ($ID_i \neq ID_j$, $i \neq j$), for $i, j \in A$, the mutually trusted center computes U_i's secret key

$$x_i = (g^{f(ID_i)})^d \bmod N. \quad (5)$$

The mutually trusted center sends x_i to each U_i via a secure channel. To ensure the validity of x_i sent from the trusted center, U_i can check whether the equality $x_i^e \equiv \prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N$ holds. If $x_i^e \equiv \prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N$ holds, then the secret shadow that the U_i received is valid. The correctness of this equation can be easily seen as follows:

$$\begin{aligned}\prod_{j=0}^{t-1} f_j^{(ID_i^j)} \bmod N &\equiv \prod_{j=0}^{t-1} (g^{c_j})^{(ID_i^j)} \bmod N \\ &\equiv g^{\sum_{j=0}^{t-1}(ID_i^j \cdot c_j)} \bmod N \\ &\equiv (g^{(d \cdot f(ID_i))})^e \bmod N \\ &\equiv x_i^e \bmod N\end{aligned}$$

Phase 3 Partial Signature Generation Phase

Suppose B represents the group to sign a message m. Each shareholder U_i in B has to generate a partial signature for m as follows.

U_i chooses a random number k_i between 1 and $N-1$, and computes r_i as

$$r_i = g^{k_i \cdot e} \bmod N \tag{6}$$

Thus, U_i makes r_i publicly available through a broadcast channel. Once all r_i are available, U_i computes the product R as

$$R = \prod_{i \in B} r_i \bmod N. \tag{7}$$

Then, U_i uses his secret key x_i and the random number k_i to compute

$$s_i = (x_i)^{h(m,R) \prod_{j \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j}} \cdot g^{k_i} \bmod N. \tag{8}$$

The user U_i in B sends the partial signature, $\{s_i\}$, to a designated clerk responsible for collecting the partial signatures and producing the group signature. Since no secret information is kept, the clerk can be anyone in the system.

Phase 4 Group Signature Generation and Verification Phase

Upon receiving these t partial signatures, the clerk can compute the group signature

$$S = \prod_{i \in B} s_i \bmod N \tag{9}$$

$$= K \cdot g^{d \cdot x \cdot h(m,R)} \bmod N \tag{10}$$

where $K = \prod_{i \in B} g^{r_i} \bmod N$. Thus, $\{R, S\}$ is the group signature for the message m.

Any verifier can use the group public key y to authenticate the validity of the group signature $\{R, S\}$ for the message m by checking the following equation

$$S^e \equiv y^{h(m,R)} \cdot R \bmod N. \tag{11}$$

If the equation holds, the group signature $\{R, S\}$ on the message m is valid. The correctness of this equation can be easily seen as follows:

$$\begin{aligned} S^e &\equiv \left(\prod_{i \in B} s_i\right)^e \bmod N \\ &\equiv \prod_{i \in B} \left((x_i)^{e \cdot h(m,R) \prod_{i \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j}} \cdot g^{k_i \cdot e} \right) \bmod N \\ &\equiv \prod_{i \in B} \left(g^{f(ID_i)} \right)^{d \cdot e \cdot h(m,R) \prod_{j \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j}} \prod_{i \in B} r_i \bmod N \\ &\equiv \prod_{i \in B} \left(g^{h(m,R) \cdot f(ID_i) \cdot \prod_{j \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j}} \right) \cdot R \bmod N \\ &\equiv g^{h(m,R) \cdot \sum_{i \in B} \left(f(ID_i) \cdot \prod_{j \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j} \right)} \cdot R \bmod N \end{aligned}$$

According to the Lagrange interpolation formula, the above equation can be rewritten as

$$\begin{aligned} S^e &\equiv g^{f(0) \cdot h(m,R)} R \bmod N \\ &\equiv y^{h(m,R)} \cdot R \bmod N \end{aligned}$$

Therefore, $S^e \equiv y^{h(m,R)} \cdot R \bmod N$ and the group signature $\{R, S\}$ on the message m can be verified.

It is noted here that in Phase 3, the clerk does not have to verify the validity of the partial signature. If a faulty signature is presented, then the group signature cannot be successfully verified by the verifier. Tompa and Woll's (1988) scheme had been shown to effectively counter the cheating problem in practice.

The signers are anonymous to the verifier, because it is not possible to find out the identities of the t signers in B from the group signature. Moreover, if a new member is added to the system or an old member is removed from the system for some reasons, the system's secret parameters and others member's secret key will not be changed, because this scheme has the property of robustness and stability (the correctness of this scheme is shown in next Section).

SECURITY ANALYSIS

The security of the proposed scheme is based on well-known cryptographic assumptions: the intractability of reversing the one-way hash function (OWHF), solving the discrete logarithm (DLP) and achieving the factorization of a large integer. None of the following possible attacks against the proposed scheme can break this proposed scheme.

Attack 1 An adversary tries to reveal the group secret key x and the member's secret key x_i from the public key y and the public parameters e and N.

To derive the group secret key x from the group public key $y = g^x \bmod N$, the adversary has to solve the problem of computing a discrete logarithm modulo of the composite number N. Moreover since the modulus N is chosen to be infeasible to factor, specialized attacks applicable to the RSA scheme are ineffective (Gan and Li, 2003), e.g., it is infeasible to find d with the known e. This implies that an adversary cannot derive a member's secret key x_i if the

secret polynomial $f(x)$ and the secret parameter d are unknown.

Attack 2 t or more shareholders of the group, may cooperate to reveal the secret keys d and $x = f(0) \bmod v$.

Since each U_i is the group member, they have the corresponding secret key $x_i = (g^{f(ID_i)})^d \bmod N$. As for getting the secret keys, they might try the following two approaches: (i) revealing the secret key d of the mutually trusted center, (ii) revealing the value $f(ID_i)$ from x_i. In the first approach, since the modulus N is chosen to be infeasible to factor, specialized attacks applicable to the RSA scheme are ineffective, e.g., it is infeasible to find d with the known e. As for the other approach, to reconstruct the secret polynomial $f(x)$ of degree $t-1$, at least t distinct $(ID_i, f(ID_i))$ pairs have to be collected. Since the trusted center distributes $x_i = (g^{f(ID_i)})^d \bmod N$ instead of $f(ID_i)$ to the shareholder U_i, the problem for U_i in deriving $f(ID_i)$ from x_i is the difficult computation of the discrete logaithm modulo from the composite number N. That is, the proposed scheme can withstand the conspiracy attack stated by Tseng and Jan(1999) and Li *et al*.(2001).

Attack 3 The signer U_i colludes with the designated clerk to forge the valid signature for message m', but the signers $U_2, \ldots, U_t$ reject to sign a message m' with him.

In Michels and Horster's (1997) forgery attack on Harn's(1994) schemes, the signer U_i wants his victims, the signers $U_2, \ldots, U_t$ to sign a message m' with him. They reject the proposal, but agree to sign the innocent message m with him. In the proposed scheme, the partial signature is $s_i = (x_i)^{h(m,R)\prod_{j\in B, i\neq j}\frac{0-ID_j}{ID_i-ID_j}} \cdot g^{k_i} \bmod N$ and the message m is protected by the one-way hash function $h()$ with the value R. So, the proposed scheme can withstand the forgery attack.

Attack 4 An adversary may try to reveal the member's secret key x_i from the partial signature $x_i, i \in B$, of the message m.

To derive the member's secret key x_i from the partial signature s_i in Eq.(8), the adversary will not be successful, because there are two unknown values x_i and g^{k_i} in one equation. However, retrieving g^{k_i} from $r_i = g^{k_i \cdot e} \bmod N$ still faces the difficulty of breaking the RSA scheme.

Attack 5 An adversary may try to get the group secret key x from the group signature, $\{R, S\}$, of the message m.

The adversary will not succeed, because there are three unknowns K, x and d in Eq.(10). However retrieving K from R, and d from e still faces the difficulty of breaking the RSA scheme.

As stated in this section, the proposed scheme is secure against the Tseng and Jan's (1999) and Li *et al*.'s (2001) conspiracy attack, and the Michels and Horster's (1997) forgery attack.

PERFORMANCE ANALYSIS

Let us consider the performance of the proposed scheme. The performance evaluation of the proposed scheme concerns the size of the group signature and the time complexity for verifying the group signature. The size of the group signature $\{R, S\}$ is $2|N|$, and each partial signature $\{s_i\}$ is $|N|$, where $|N|$ is the bit-string length. As for the time complexity for verifying the group signature, two modular exponentiations are required. That is, the size of the group signature and the verification time of the group signature are equivalent to that of an individual signature.

EXTENSION SCHEME

The above scheme can be slightly modified so that it has the property that the original signers can prove that they are true signers. The System Initialization Phase, and Distribution of Secret Shadows and Verification Phase are the same as that the above scheme.

In the Partial Signature Generation Phase, each member U_i in B selects random integers k_i and $\bar{k}_i$ between 1 and $N-1$, and computes the values $r_i = g^{k_i \cdot e} \bmod N$ and $\bar{r}_i = g^{\bar{k}_i \cdot e} \bmod N$. r_i and $\bar{r}_i$ are broadcast to all members in B. Once all r_i and $\bar{r}_i$ are available, U_i computes the product R, and a new value $\bar{R}$ as

$$R = \prod_{i\in B} r_i \bmod N, \qquad (12)$$

$$\bar{R} = h(\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_t). \quad (13)$$

The partial signature s_i can then be generated by U_i:

$$s_i = (x_i)^{h(m,R,\bar{R}) \prod_{j \in B, i \neq j} \frac{0 - ID_j}{ID_i - ID_j}} \cdot g^{k_i} \bmod N. \quad (14)$$

In the Group Signature Generation and Verification Phase, S can be calculated by

$$S = \prod_{i \in B} s_i \bmod N, \quad (15)$$

and $\{R, \bar{R}, S\}$ is the group signature of m.

Verifier can authenticate the validity of the group signature $\{R, \bar{R}, S\}$ for the message m by checking the following equation

$$S^e \equiv y^{h(m,R,\bar{R})} \cdot R \bmod N. \quad (16)$$

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

If the original signers in B consent to expose their identities, they can show $\{\bar{k}_i, \bar{r}_i\}$ to an arbiter. The arbiter checks the following equation:

$$\bar{R} \stackrel{?}{=} h(\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_t), \text{and}$$
$$\bar{r}_i \stackrel{?}{=} g^{\bar{k}_i \cdot e} \bmod N.$$

If the above equations hold, the arbiter will believe that these users are the original signers.

The extension scheme is also untraceable, because the verifier cannot identify the original signers from the new value $\bar{R}$ in the group signature.

CONCLUSIONS

In this paper, the authors firstly proposed a verifiable (t, n) threshold untraceable signature scheme that is secure enough against the conspiracy attack and forgery attack; then demonstrated that the group signature verification process is simplified and that the group signature's size is equivalent to an individual signature's size; and then developed another threshold signature scheme wherein the original signers can prove that they are the true signers.

References

Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B., 1985. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. Proceeding of the 26th IEEE Symposium on Foundation of Computer Science, IEEE Computer Press, Washington, p.383 – 395.

Desmedt, Y. and Frankel, Y., 1992. Shared Generation of Authenticators and Signatures. *In*: Feigenbaum J. ed., Advances in Cryptology-Crypto' 91 Proceedings, Springer-verlag, Berlin, p.457 – 469.

Gan, Y.J. and Li, Q.H., 2003. A group oriented verifiable threshold signature scheme based on factorization. *Journal of the China railway society*, **25**(3): 69 – 72(in Chinese).

Harn, L., 1994. Group-oriented (t, n) threshold digital signature scheme and multisignature. *IEEE Proceedings, Computers and Digital Techniques*, **141**(5): 307 – 313.

Lee, N.Y., Hwang, T. and Li, C.M., 2000. (t, n)threshold untraceable signatures. *Journal of Information science and engingeering*, **16**(6): 835 – 846.

Li, C.M., Hwang, T. and Lee, N.Y., 1995. (t, n) threshold signature schemes based on discrete logarithm. *In*: Cryptogy procedings of Eurocrypt' 94, Springer-verlag, Berlin, p.191 – 200.

Li, Z.C., Hui, L.C.K., Chow, K.P., Chong, C.F., Tsang, W.W. and Chan, H.W., 2001. Security of Wang *et al.*'s group-oriented (t, n) threshold signature schemes with traceable signers. *Information Processing Letters*, **80**(6): 295 – 298.

Michels, M. and Horster, P., 1997. On the risk of disruption in several multiparty signature schemes. *In*: Cryptology-Crypto'96 Proceedings, Springer-verlag, Berlin, p.334 – 345.

Tompa, M. and Woll, H., 1988. How to share a secret with cheaters. *Journal of cryptology*, **1**(2): 133 – 138.

Tseng, Y.M. and Jan, J.K., 1999. Attacks on threshold signature scheme with traceable signers. *Information Processing Letters*, **71**(1): 1 – 4.

Wang, C.T., Lin, C.H. and Chang, C.C., 1998. Threshold signature schemes with traceable signers in group communications. *Computer Communications*, **21**(8): 771 – 776.

Wang, G.L. and Qing, S.H., 2000. The weaknesses of some threshold group signature schemes. *Journal of Software*, **11**(10): 1326 – 1332(in Chinese).

Wang, G.L., Wang M.S., Ji, Q.G. and Qing, S.H., 2001. Security limits of the LHL threshold group signature scheme. *Journal of Computers*, **24**(9): 897 – 902 (in Chinese).