Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080642

An Efficient Threshold Signature Scheme Resistible to Conspiracy Attack

Yu-Fang Chung[1,*], *Tzer-Shyong Chen*[2,*] *and Tzer-Long Chen*[3,*]

[1] Department of Electrical Engineering, Tunghai University, Taiwan
[2] Department of Information Mangement, Tunghai University, Taiwan
[3] Department of Technological Product Design, Lingtung University, Taiwan

Received: 12 Nov. 2013, Revised: 10 Feb. 2014, Accepted: 11 Feb. 2014
Published online: 1 Nov. 2014

Abstract: The study presents a threshold signature scheme. While developing threshold cryptography, the concept of threshold signature can accomplish a tradeoff between efficiency in use and dependability of security. The presented threshold signature scheme can resist conspiracy attack by controlling the right of issuing group signature, and the performance of constructing group signature is also enhanced by simplifying keys.

Keywords: Threshold Signature; Digital Signature; Public Key; Discrete Logarithm Problem.

1 Introduction

The first threshold cryptosystem [9] was proposed by Desmedt and Frankel in 1990. Since then, threshold cryptosystems have been gradually attracting attention from cryptographers. Research results of numerous international studies [5,7,8,10,14,15]were published, and considerable research [1,2,3,4,11] has been dedicated to threshold cryptography. Threshold cryptography is considered to have good future prospects. Consequently, the standardization organization IEEE P1363 has listed it as a part of its plan for future work and research [13]. Threshold signature cryptosystem is an important aspect of threshold cryptography; it relatively represents the core of threshold cryptography research. Other than the RSA-based threshold signature cryptosystem proposed by Desmedt and Frankel [10], another significant influence was the system proposed by Harn [5] that laid the foundation for the El Gamal system. However, a conspiracy attack that could damage the threshold system [10] was demonstrated by C. M. Li et al. [1]. Ever since, conspiracy attack has become a tough problem for threshold systems. The threshold signature cryptosystem [10] proposed by Desmedt and Frankel was a (t,n) threshold signature method with untraceable signers. Related research [1] revealed that $t+1$ or t sub secret shareholders could conspire to obtain system secrets and a conspiracy attack from the participants enabled conspirators to easily generate a group signature.

Subsequently, Li et al. proposed two (t,n) threshold signature methods [2] for withstanding conspiracy attack. One of the methods required a trusted distribution center. While both methods were able to resist conspiracy attack by attaching a random number to the sub-keys of all participants to prevent the signatures from being traced from the sub-key, the said methods failed to resist forgery attack from internal members, as pointed out by Michels and Horster [6]. In 1998, Wang et al. [3] proposed two new (t,n) threshold signature methods to resist conspiracy attacks. Signers could be traced in the newly proposed methods, but the association of random numbers to sub-keys could not be made. Nevertheless, Tseng and Jan forged an attack [11] to demonstrate insecurities in the methods by Wang et al.; they summarized the concepts of the attack, and then created yet again a new threshold signature system withstanding conspiracy attacks [4]. Group signature presents the accessible authority and the representativeness of group members. The threshold scheme is utilized in this study for a threshold being a group member. Majority decision is applied to standing for the group opinion. The used maximum computation loading of group signature is regarded as the required computation time when all

* Corresponding author e-mail: yfchung@thu.edu.tw, arden@thu.edu.tw, tlchen@teamail.ltu.edu.tw

members participate in. However, a threshold value needs to be set in the threshold scheme for the group effect. Although increasing members would increase computation loadings, the number of participants is normally restricted in the actual application in order to avoid the computation being too complicated. Meanwhile, the hardware computation ability has been enhanced that no specific loading would be caused. The new system was signer-untraceable; it required two sets of keys. One relied on the Discrete Logarithm Problem (DLP), while the other depended on the dissolution of the large integer problem. These two sets of keys were designed to protect the system signature key. In truth, this method, too, is unable to protect against sub-key holders conspiring to obtain system secrets. Thus, it, too, fails to withstand conspiracy attack [1].

2 The threshold signature scheme

2.1 System initialization

The method requires for a trusted SDC (Share Distribution Center) being responsible for establishing parameters. Assume that n members are involved in a group and let $A = P_1, P_2, ?, P_n$ represents the n-member set. For set A, P_i represents the ith participant given that $i \in n$ and $P_i \in A$. To sign a message, t or more participants must reach the agreement; so, they form a subset B, for $B \in A$. The SDC executes the procedure of system initialization as follows.

Step 1:Determine the system parameters.

1.Select two large prime numbers, denoted as p and q
2.Calculate $N = p^*q$.
3.Select the primitive root, denoted as g, where $g \in Z^*N$.
4.Select a one way hash function, denoted as $h(0)$.
5.Determine $a(t-1)$-order polynomial over $Z\varphi(N)$, represented as $f(x)$, as follows. $f(x) = a_{t-1}x^{t-1} + \ldots + a_1x + a_0 \bmod \phi(N)$, where $a_{t-1}, \ldots, a_1$, and $a_0 \in z_{\phi(N)}$
6.Determine the group private and public keys x and y.

$$x = f(0) = a_0$$

$$y = x^{-1} \bmod \phi(N)$$

Step 2:Declare the public parameters $N, g, h(0)$, and y.

Step 3:The SDC also generates the individual parameter for each member P_i in A. The procedure is as follows.

1.Assign P_i a public identity number ID_i.
2.Generate individual private and public keys x_i and y_i of P_i as follows.

$$x_i = \left(g^{f(ID)a}\right)^x \; mod\ N$$

$$y_i = \left(g^{f(ID)a}\right) \; mod\ N$$

$$a_i = \prod_{jeA.j\neq i} (ID_i - ID_j)^{-1} \; mod\ N$$

3.Send the individual private key x_i to P_i secretly and declare the individual public key y_i .
4.Destroy the secret parameters x, p, q, which are no longer required.

2.2 Signature generation

2.2.1 Suppose that t participants P_1, P_2,..., P_t are signing message m in behalf of group A. Each participant signs message m as follows.

Step 1:Select a random number k_i so as to calculate r_i.

$$r_i = g^{k,y} \mod N$$

Step 2:Broadcast the individual commitment value r_i to the other participants.

Step 3:Determine the continued product of r_j while collecting all r_j.

$$R = \prod_{e} r \mod N$$

Step 4:Calculate partial signature s_i using the individual private key x_i and the random number k_i.

$$S_i = (x_i)^{h(m,k)\prod(ID-ID)\prod(0-ID)} g^k \; mod\ N$$

Step 5:Send the partial signature (ri, si) to the signature generator SG.

After receiving (ri, si), the SG validates each of the t partial signatures as follows.

$$S_i^y = (y_i)^{h(m,k)\prod(ID-ID)\prod(0-ID)} r_i \; mod\ N$$

Proof:

$$\begin{aligned} S_i^y &= \left[(x_i)^{h(m,k)\prod(ID-ID)\prod(0-ID)} g^k\right]^y \; mod\ N \\ &= \left[\left(g^{f(ID)\alpha}\right)^{xyh(m,k)\prod(ID-ID)\prod(0-ID)} g^{ky}\right] \mod N \\ &= \left[(y^i)^{h(m,k)\prod(ID-ID)\prod(0-ID)} r_i\right] \; mod\ N \\ &= (y_i)^{h(m,k)\prod(ID-ID)\prod(0-ID)} r_i \; mod\ N \end{aligned}$$

Only when the equation above is satisfied will the SG believe that (r_i, s_i) is a valid partial signature by P_i. Once all individual signatures have been validated, the SG computes the group signature.

$$R = \prod_{jeB} r_j \; mod\ N$$

$$S = \prod_{ieB} s_j \; mod\ N$$

Afterwards, the SG sends the group signature (R, S) to the verifier.

2.2.2 To resist conspiracy attack, the SG can perform the following additional steps.

Step 1:Use the private key xSG to encrypt R and S, creating R' and S'.
Step 2:Send (m,R',S',R,S) to the verifier.

2.3 Signature verification

2.3.1 The verifier on acquiring message m, which is sealed with the group signature (R,S) of A, validates the group signature as follows.

$$S^{yy} \equiv g^{h(m,R)} R^{y} \ mod\ N$$

Proof:

$$\begin{aligned} S^{yy} &= \left(\prod_{ieB} S_i\right)^{yy} mod\ N \\ &= \left(\prod_{ieB} S_i\right)^{y} mod\ N \\ &= \left\{\prod_{ieB}\left[(y_i)^{h(m,R)\prod_{ee}(ID-ID)\prod_{ee}(0-ID)} r_i\right]\right\}^{y} mod\ N \\ &= \left\{\prod_{ieB}\left[\left(g^{f(ID)\alpha}\right)^{h(m,R)}\right]\prod_{ieB} r_i\right\}^{y} mod\ N \\ &= \left\{\left(g^{\sum_e f(ID)\alpha\beta}\right)^{h(m,R)} R\right\}^{y} mod\ N \\ &= \left\{(g^{x})^{h(m,R)} R\right\}^{y} \ \text{mod}\ N \\ &= g^{xyh(m,R)} R^{y}\ mod\ N \\ &= g^{xyh(m,R)} R^{y}\ mod\ N \end{aligned}$$

$$\begin{aligned} &\sum_e f(ID)\alpha\beta \\ &= \sum_e f(ID)\prod_e (ID-ID)^{-1}\prod_e (ID-ID)\prod_e (0-ID)\ mod\ \phi(N) \\ &= \sum_e f(ID)\prod_e \frac{(0-ID)}{(ID-ID)}\ mod\ \phi(N) \\ &= f(0)\ mod\ \phi(N) \\ &= x \end{aligned}$$

2.3.2 After receiving (m,R',S',R,S), the verifier carries out the verification as follows.

Step 1:The verifier uses the SG's public key ySG to decrypt R' and S', creating R'' and S''.
Step 2:Verify if $R'' = R$ and $S'' = S$. If both equations hold, meaning that the signature has been validated by the SG, it is then assumed to be resistible to conspiracy attack.

Step 3:Repeat the procedure in 2.3.1.

Example 2.1. Let the number of members in group A be $n = 7$ and the threshold value of participants who cooperatively generate a valid group signature in behalf of the whole group A be $t = 4$.

$$(t,n) = (4,7)$$
$$Group\ A = \{P_1,P_2,P_3,\ldots,P_1\}$$
$$Group\ B = \{P_1,P_3,P_4,P_7\}, for\ B \in A$$

The SDC executes the procedure of system initialization as follows.

Step 1:Determine the group private-and-public key pair.
1.Select two large prime numbers $p,q,i.e.,p = 11$ and $q = 19$.
2.Calculate $N = p*q = 209$.
3.Select $g = 17$.
4.Select a one way hash function $h(.)$.
5.Determine a 3-order polynomial $f(x)$.

$$f(x) = 1x^3 - 3x^2 - 1x + 7$$

6.Determine the group private and public keys x and y.
$x = f(0) = a_0 = 7$
$y = x^{-1} mod 180 = 103$

Step 2:Declare $N = 209,\ g = 17,\ h(.)$, and $y = 103$.
Step 3:Generate individual parameter for each member in group A.
1.Assign each member identity number.
$ID_1 = 1 \Rightarrow P_1$
$ID_2 = 2 \Rightarrow P_2$
$ID_3 = 3 \Rightarrow P_3$
$ID_4 = 4 \Rightarrow P_4$
$ID_5 = 5 \Rightarrow P_5$
$ID_6 = 6 \Rightarrow P_6$
$ID_7 = 7 \Rightarrow P_7$
2.Generate individual private and public keys x_i and y_i.

$$\begin{aligned} x_1 &= (17^{4*9})^7 \text{ mod } 209 = (17^{36})^7 \text{ mod } 209 = 58 \\ y_1 &= (17^{36}) \text{ mod } 209 = 115 \\ x_2 &= (17^{1*155})^7 \text{ mod } 209 = (17^{155})^7 \text{ mod } 209 = 120 \\ y_2 &= (17^{155}) \text{ mod } 209 = 175 \\ x_3 &= (17^{4*135})^7 \text{ mod } 209 = (17^{540})^7 \text{ mod } 209 = 1 \\ y_3 &= (17^{540}) \text{ mod } 209 = 1 \\ x_4 &= (17^{19*29})^7 \text{ mod } 209 = (17^{551})^7 \text{ mod } 209 = 63 \\ y_4 &= (17^{551}) \text{ mod } 209 = 61 \\ x_5 &= (17^{52*135})^7 \text{ mod } 209 = (17^{7020})^7 \text{ mod } 209 = 1 \\ y_5 &= (17^{7020}) \text{ mod } 209 = 1 \\ x_6 &= (17^{109*155})^7 \text{ mod } 209 = (17^{16895})^7 \text{ mod } 209 = 120 \\ y_6 &= (17^{16895}) \text{ mod } 209 = 175 \\ x_7 &= (17^{196*9})^7 \text{ mod } 209 = (17^{1764})^7 \text{ mod } 209 = 191 \\ y_7 &= (17^{1764}) \text{ mod } 209 = 20 \end{aligned}$$

3.Send x_i to P_i secretly and declare all y_i.
4.Destroy x, p, q.

Assume that the participant set $B = P_1, P_3, P_4, P_7$ *and* $B \in A$. *Each participant cooperatively generates the group signature, as follows.*

Step 1:Select a random number k_i, i.e., $k_1 = 11$, $k_3 = 13$, $k_4 = 14$, $k_7 = 17$.
Step 2:Calculate the individual commitment value r_i.

$$\begin{aligned} r_1 &= 17^{11*103} \bmod 209 = 161 \\ r_3 &= 17^{13*103} \bmod 209 = 24 \\ r_4 &= 17^{14*103} \bmod 209 = 80 \\ r_7 &= 17^{17*103} \bmod 209 = 6 \end{aligned}$$

Step 3:Broadcast r_i to other participants.
Step 4:Determine $R = 54$
Step 5:Calculate the partial signature s_i.

$$\begin{aligned} r_1 &= 17^{11*103} \bmod 209 = 161 \\ r_3 &= 17^{13*103} \bmod 209 = 24 \\ r_4 &= 17^{14*103} \bmod 209 = 80 \\ r_7 &= 17^{17*103} \bmod 209 = 6 \end{aligned}$$

Figure 1 illustrates an example of the presented threshold signature method in the study; there are seven members $P_1, P_2, P_3, P_4, P_5, P_6$, and P_7 in group A. Firstly, the SDC generates individual parameters for the members in group A. Then, some members in group A are denominated group $B = P_1, P_3, P_4, P_7$, who work as part of a team for signing message m in behalf of A. Members in group B send the generated individual signatures, P_1, P_3, P_4 and P_7, and then send them to the SG for the validation. Once all individual signatures have been approved, the SG computes the group signature and sends it to the verifier.

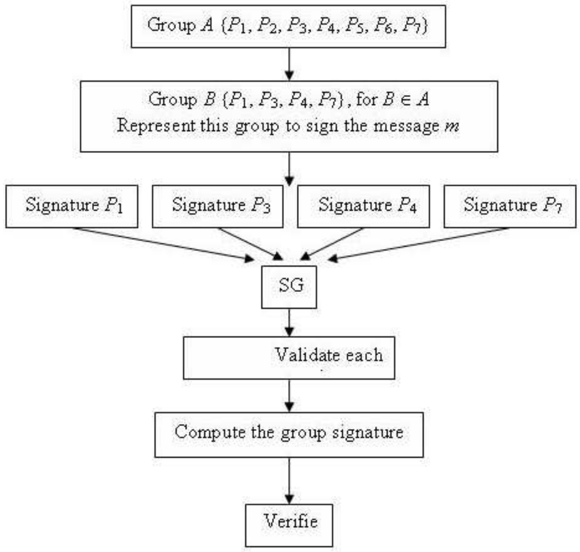

Fig. 1: Generation and verification of threshold group signature.

3 Analyses of security and performance

To prevent the leakage of system secretes by conspirators, Jan's method [4] changed the secret quota to the form $x_i = (g^{f(ID_i)l_i})^d \bmod N$ and applied the difficult of DLP to preventing conspiracy. However, the analyses have shown the method being unsatisfactory.

Therefore, a new combination consisting of the dissolution of the large integer problem and the difficult of DLP is used for constructing the group key and individual keys. To keep it efficient, the number of key sets needed for constructing the scheme is kept to a minimum. In the scheme, only the group public key x and corresponding private key y need to be determined. The individual private and public keys are generated by using the given ID of each participant in group A. As a result, there exists a relation between (x,y) and (x_i,y_i). For withstanding conspiracy attack, because of the SG, it is ensured that the signature is published by t or more group members. The scheme uses a new combination of RSA and DLP to construct the group key and individual keys. An attacker normally would attack the identity of a user participating in the computation during the signature computation process. Group signature represents the group right and application, which take protecting the user identity and applying cryptography into account in order to guarantee the user identity and group right. The mathematical difficulty in DLP is utilized in this study for the security when facing DLP difficulties. Moreover, the reference has been revised.

In addition, this study herein designs a threshold signature scheme that controls group signature issuance right to resist conspiracy attacks. Since the said scheme uses threshold signature, t or more members must be presented to establish a valid group signature and obtain the group secret key. Since an attacker may attempt to obtain group private key x from group public key y and further forge signature by $g^{xxh(m,R)}R^x$, an equitable SG is set up to prevent conspiracy attack. Following the generation of the group signature $S(m)$, the SG signs $S(m)$ with private key and obtains $S_1(m)$, where $(m, S(m), S_1(m))$ is taken to be the issued group signature for message m. Playing his role, the verifier confirms that $S(m)$ is a valid signature for m by using the group public key. Simultaneously, the issued group signature public key is utilized for verifying $S_1(m)$ being the valid signature for $S(m)$. The group signature is accepted when both signatures are validated. The signature scheme employs group signature issuance rights to restrict the *SG*. Furthermore, the *SG* controls only the right to issue group signatures, but no other system secrets. Since group members are unable to conspire to generate a valid signature without the participation of SG, the SG can be held wholly responsible in case of the forgery of valid signature. This will deter the SG from joining the conspirators. Hence, the proposition can successfully resist conspiracy attack. However, the requirement of a trusted SG might grow new concerns about its establishment cost and dependability, and the required operation cost at system initialization tends to be complex; fortunately, most of the complex calculations are one-time work.

For the application of signature, security problems need to be taken into account. Group signature shows the group member effect and the threshold scheme is applied to setting the majority decision. When setting the group, the member change might result in insecure application. The left members therefore became illegal ones. Such members might have old information and be able to access to the data that the data security is questioned. In this case, a newly generated signature should consider the legitimacy of members. Dynamic access would cause security problems because of the leaving or increase of members. To avoid the left members applying old information to accessing to the data and appended members not being able to access to the data, new signature should re-compute the members representing the new group so that the old members could not illegally use old information and insecurity problems could be avoided.

In general, users can use the signature very easily because most of the complex calculations are handled by the SDC. All they need to do is to follow the steps in 2.2 and 2.3. In summary, this paper successfully resists conspiracy attack and employs a new set of keys that make the scheme efficient. Nevertheless, not only does the proposed scheme need a trusted SDC and a trusted SG, but it actually makes the scheme safer than the others.

4 Conclusion

In reality, for a cryptosystem to be implemented successfully, full consideration must be given to conspiracy attacks. The method by Jan [4] was susceptible to conspiracy attack; it also had a lower level of resistance against conspiracy attacks than the initial methods [1, 10]. The proposed scheme is designed to resist conspiracy attacks by controlling the group signature issuance rights. The proposed method is advantageous in generating group signature through simplifying keys though it requires a dependable SG for attaining complete signatures.

Acknowledgement

This work was supported partially by National Science Council of Republic of China under Grants NSC 102-2410-H-275-013.

References

[1] C. M. Li, T. Hwang, and N. Y. Lee, "Remark on the Threshold RSA Signature Scheme," Advances in Cryptology-Proceedings of CRYPTO '93, LNCS, Springer-Verlag, **773**, 413-419 (1993).
[2] C. M. Li, T. Hwang, and N. Y. Lee, "Threshold Multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Shareholders," Advances in Cryptology-Proceedings of EUROCRYPT '94, LNCS, Springer-Verlag, **950**, 428-446, (1995).
[3] C. T. Wang, C. H. Lin, and C. C. Chang, "Threshold Signature Schemes with Traceable Signers in Group Communications," Computer Communications, **21**, 771-776 (1998).
[4] J. K. Jan, Y. M. Tseng, and H. Y. Chien,"A Threshold Signature Scheme Withstanding the Conspiracy Attack," Communications of Institute of Information and Computing Machinery, **2**, 31-38 (1999).
[5] L. Harn, "Group-oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature," IEE Proceeding-Computers and Digital Techniques, **141**, 307-313 (1994).
[6] M. Michels and P. Horster, "On the Risk of Disruption in Several Multiparty Signature Schemes," Advances in Cryptology-Proceedings of ASIACRYPT '96, LNCS, Springer-Verlag, **1163**, 334-345 (1997).
[7] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust Threshold DSS Signature," Advances in Cryptology-Proceedings of EUROCRYPT '96, LNCS, Springer-Verlag, **1109**, 354-371 (1996).
[8] S. Jarecki and A. Lysyanskaya, "Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures," Advances in Cryptology-Proceedings of EUROCRYPT 2000, LNCS, Springer-Verlag, **1807**, 221-242 (2000).
[9] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," Advances in Cryptology?Proceedings of CRYPTO '89, LNCS, Springer-Verlag, **435**, 307-315 (1990).
[10] Y. Desmedt and Y. Frankel, "Shared Generation of Authenticators and Signatures," Advances in Cryptology?Proceedings of CRYPTO ?91, LNCS, Springer-Verlag, **576**, 457-469 (1992).
[11] Y. M. Tseng and J. K Jan., "Attacks on Threshold Signature Scheme with Traceable Signers", Information Processing Letters, **71**, 1-4 (1999).
[12] Y. F. Chung, C. H. Liu, F. P. Lai, and T. S. Chen, "Threshold Signature Scheme Resistible for Conspiracy Attack," 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, Dec. 4-7, Taipei, Taiwan, 1-4, (2006).
[13] http://grouper.ieee.org/groups/1363/StudyGroup/index.html
[14] Y. F. Chang and C. C. Chang, "Robust t-out-of-n Proxy Signature Based on RSA Cryptosystems," Journal Innovative Computing, Information and Control, **4**, 425-431 (2008).

[15] X. Li, G. Liu, H. Ma, and L. Wang, "A Detection Method for the Illegal Copying of Digital Documents," Journal Innovative Computing, Information and Control, **4**, 681-688 (2008).

Yu Fang Chung received a B.A. degree in English Language, Literature and Linguistics from Providence University in 1994, an M.S. degree from Dayeh University in 2003, and a Ph.D. degree from National Taiwan University in 2007, both in Computer Science, Taiwan. She is currently an associateprofessor in the Departments of Electronic Engineering and Information Management at Tunghai University, doing research, i.e., Information Security and Cryptography.

Tzer Shyong Chen received the Ph.D. in the Department of Electrical Engineering (Computer Science) at National Taiwan University, Taiwan. He is currently a professor in the Department of Information Management at Tunghai University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.

Tzer Long Chen received thePh.D. in the Department of Information Management, National Taiwan University, Taiwan. He is currently an assistant professor in the Department of Technological Product Design at Lingtung University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.