Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 4470 – 4475

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Analysis and Improvement of a Threshold Signature Scheme Based on the General Access Structure

Cai Yongquan[a,*], Zhang En[a,b] Cheng Fula[ia]

[a]College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China.

[b]College of Computer and Information Technology, Henan Normal University, Xinxiang 453007, China.

Abstract

Hua-wang Qin et al. proposed a novel threshold signature scheme based on the general access structure in order to break the applied limitation of the conventional threshold signature schemes. The security of the scheme was analyzed in this paper, and it is pointed out that the scheme is insecure because it cannot withstand conspiracy attacks and what's more, the identity of signer cannot be investigated. To overcome these security vulnerabilities, this paper proposed an improved threshold signature scheme, and the security analysis results show that the improved scheme can not only resist the conspiracy attack, but also have the properties of anonymity and traceability simultaneously.

Keywords: threshold signature; access structure; conspiracy attacks; anonymity; traceability

1. INTRODUCTION

The concept of the threshold signature scheme was firstly introduced by Desmedt and Frankel, and they proposed the first (t, n) threshold signature scheme based on RSA cryptosystem [1] in 1991. In the (t, n) threshold signature scheme, a signature can be generated when the number of participators is equal to or more than the threshold value t, but any less than t players cannot generate a valid one. A secure threshold signature scheme should not only satisfy the properties including threshold characteristics, traceability, anonymity and robustness, but also can withstand the conspiracy attack and the forgery attack. The threshold signature schemes have been discussed widely and many threshold signature schemes [3-8] have been proposed, but no scheme meets all of those properties.

In many practical applications, the signing power of the signature players is differentiated according to the importance of the message which needs to be signed. Some important message must to be signed by several players and some others by less players even one. In this case, the conventional (t, n) threshold signature scheme is helpless. So the scholars proposed changeable threshold signature schemes [2, 3] and threshold signature schemes with privilege subsets [9] to this problem. But all of those schemes cannot be used to solve the situation [10] put forward by Hua-wang Qin et al. It is that the power of signing belongs

* Corresponding author. Tel.:+8613910303218

E-mail address:cyq@bjut.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.

doi:10.1016/j.proeng.2011.08.840

to some specified subsets, and the group of any *t* or more players has no right to sign if the subset they formed is not a specified subset.

Hua-wang Qin et al. referenced the secret sharing scheme with general access structures and proposed a novel threshold signature scheme [10] based on the general access structure for this problem. Their scheme has a wide range of applications and the players just need to preserve and maintain a few private keys. Unfortunately, according to our security analysis, their scheme cannot resist the player's conspiracy attack. And moreover, the signers cannot be traced when a dispute on the signature arises. To overcome these security weaknesses, we propose an improved scheme and the security analysis result shows that the improved scheme can not only resist the conspiracy attack, but also have the properties of anonymity and traceability simultaneously.

The rest of this paper is organized as follows. In Section II, we review Qin et al.'s threshold signature scheme based on the general access structure and analyze its weaknesses. In Section III, we present an improved threshold signature scheme. In Section IV, we prove the correctness of the improved scheme and analyze it. Finally, we draw our conclusions in Section V.

2. Review of the Qin et al.'s scheme and its weaknesses

In this section, we review Qin et al.'s threshold signature scheme and then present the weaknesses of their scheme.

A. Initialization phase

The system parameters are defined as follows: *n* players are denoted by $U_1, U_2, \cdots, U_n$ and let Γ_0 be the minimal access structure set of the signature system. Γ_0 contains α authorized subsets and be defined by $\Gamma_0 = \{P_i | i=1, 2, \cdots, \alpha\}$.

1) The Key Distribution Center (KDC) chooses two large prime numbers *p* and *q*, such that $q \mid (p-1)$. Then let *g* be an element of order *q* in *GF* (*p*) and *p*, *q*, *g* are opened.

2) The KDC selects randomly an integer *X* and divides *X* into *n* different sub-secrets, such that $X = x_1+x_2+\cdots+x_n$ and $x_j (j=1, 2, \cdots, n)$ must be an integer. Afterwards, KDC sends x_j secretly to the corresponding player U_j by using a secure channel.

3) For each authorized subset $P_i (i= 1, 2, \cdots, \alpha)$, KDC computes and broadcasts $G_i = {}_{X-\sum_{U_j \in P_i} x_j}$.

4) Each player $U_j (j=1, 2, \cdots, n)$ selects randomly an integer k_j over $[1, p-1]$ and computes and broadcasts $y_j = g^{r_j k_j} \bmod p$, $r_j = g^{k_j} \bmod p$.

5) The KDC computes and broadcasts $R = {}_{\prod_{j=1}^{n} r_j \bmod p}$, then computes $E = g^x R \bmod p$ and keeps *E* in secret.

B. Generation of partial signature and verification

1) Assume that the authorized subset P_i want to sign a message *m*. Each player U_j belongs to P_i chooses randomly an integer t_j over $[1, p-1]$ and computes and broadcasts $T_j = g^{t_j} \bmod p$ and $z_j = g^{t_j k_j^{-1}} \bmod p$. 2) U_j computes $Z = \prod_{U_c \in P_i} z_c \bmod p$. 3) U_j computes the partial signature: $S_j = [x_j h(Z,m) - Z t_j k_j^{-1}] \bmod q$, and sends it to the Designated Clerk (DC). And *h*() is a secure one-way hash function. 4) The DC confirms the validity of S_j by checking if the equation $r_j^{s_j} T_j^{Z} = y_j^{h(Z,m)} \bmod p$ holds.

C. Generation of threshold signature and verification

1) If all S_j is valid, the DC computes $S = \sum_{U_j \in P_i} S_j + G_j h(Z, m)$, and the threshold signature on m is $\{m, S, Z, R, E\}$.

2) Any verifier can verify the validity of the threshold signature $\{m, S, Z, R, E\}$ by checking if the equation $g^S Z^Z = (ER^{-1})^{h(Z,m)} \bmod p$ holds.

D. The weaknesses of Qin et al.'s scheme

1) The Qin et al.'s scheme cannot resist the conspiracy attack

In Qin et al.'s scheme, all players of any an authorized subset P_i in the minimal access structure set Γ_0 can cooperate to compute the system secret key. Then, they conspirators can sign any message they like without taking responsibility. The reasons are as follows. The system secret key X is computed as follow: $X = x_1 + x_2 + \cdots + x_n$, where x_j is the player's secret key. The players in the authorized subset P_i can show their secret key to each conspirator, and they just need to figure out the rest $X - \sum_{U_j \in P} x_j$. Unfortunately, the rest part can be fond directly from the public information, that's the G_i. Now they get the $X = G_i + \sum_{U_j \in P} x_j$.

Afterwards, conspirators can sign any message. The right of the threshold signature verification equation can be rewrite like this:

$(ER^{-1})^{h(Z,m)} = (g^x RR^{-1})^{h(Z,m)} = (g^x)^{h(Z,m)} \bmod p$. X is known and they can select a random number instead of Z because Z contains random number t_j. Assume conspirators take a random number v as $\sum_{U_j \in P_i} t_j k_j^{-1} \bmod p$, then Z is replaced by $Z' = g^v \bmod p$. So, the threshold signature is $S' = Xh(Z', m) - Z'v \bmod q$ and $\{m, S', Z', R, E\}$. Check the new threshold signature using the verification equation. Left is

$g^{S'} Z'^{Z'} \bmod p = g^{Xh(Z',m) - Z'v} g^{vZ'} \bmod p = g^{Xh(Z',m)} \bmod p$.

Obviously, it's equal to the right and the equation holds. So, this attack works.

2) The signers in Qin et al.'s scheme are untraceable

Traceability is the main security notion of the threshold signature, since it is related to unforgeability: nobody (even a collusion of players) should be able to produce a valid signature that cannot be open in a convincing way. Lack of traceability makes the Qin et al.'s scheme useless.

In Qin et al.'s scheme, the parameters which can be used to trace the signers are the players' private key x_j and the random number k_j chose by player U_j in the initialization phase. The last valid threshold signature is $\{m, S, Z, R, E\}$, where m, R, E have no relation to do with the signers. Though k_j^{-1} is needed when we compute Z, we cannot calculated k_j or any information about k_j from Z because it contains another random number t_j. So we cannot trace the signers by using Z. According to the discussion above, all players of any an authorized subset P_i can cooperate to compute the system secret key and forge a valid threshold signature. Obviously, we also cannot trace the signers from S. In addition, the DC's responsibility in this scheme is just synthesizing the threshold signature, and anyone who got the partial signatures can do it. As a result, the Qin et al.'s scheme has no the property of traceability, which means that we cannot trace adversarial signers if forgery is suspected.

Therefore, Qin et al.'s scheme is insecure.

3. AN IMPROVED THRESHOLD SIGNATURE SCHEME BASED ON THE GENERAL ACCESS STRUCTURE

To overcome the weaknesses of Qin et al.'s scheme, we propose an improved scheme in this section.

A. Initialization phase

1) The KDC selects two large prime numbers p and q, such that $q \mid (p-1)$. Then let g be an element of order q in $GF(p)$ and p, q, g are opened. The KDC chooses and broadcasts a secure one-way hash function $h()$. 2) The KDC selects randomly an integer X and divides X into n different sub-secrets, such that $X = x_1 + x_2 + \cdots + x_n$ and $x_j (j = 1, 2, \cdots, n)$ must be an integer. Afterwards, KDC sends x_j secretly to the

corresponding player U_j by using a secure channel. Then KDC computes and broadcasts $Y = g^X \bmod p$, the public key, and $y_j = g^{x_j} \bmod p$ (j=1, 2,⋯, n). 3) For each authorized subset P_i (i= 1, 2,⋯, α), KDC computes as follows: KDC chooses a random integer s_i in the range [1, p-1] and computes $R_i = g^{s_i} \bmod p$. Next, he calculated A_i in accordance with the congruence equation $X - \sum_{U_j \in P_i} x_j = s_i R_i + A_i \bmod q$.

Finally, KDC opens each (R_i, A_i). 4) The player U_j accepts x_j from KDC if the equation $g^{x_j} = y_j \bmod p$ holds.

B. Generation of partial signature and verification

1) Assume that the authorized subset P_i want to sign a message m. Each player U_j belongs to P_i chooses randomly an integer k_j in the range [1, p -1] and computes and broadcasts $K_j = g^{k_j} \bmod p$.

2) After receiving all K_j, each player U_j computes $K = \prod_{U_c \in P_i} K_c \bmod p$.

3) Each player U_j generates his partial signature on message m: (1)

$$S_j = [x_j h(K,m) - K k_j] \bmod q \tag{1}$$

And U_j sends it to the DC.

4) The DC verifies the partial signature by checking the equation:

$$(K_j)^K g^{S_j} = y_j^{h(K,m)} \bmod p \tag{2}$$

If it holds, DC accepts. Otherwise, DC asks the player to re-compute the partial signature.

C. Generation of the threshold signature and verification

1) If all partial signatures are valid, the DC chooses the corresponding (R_i, A_i) and selects a random integer l in the range [1, p-1]. Let $R = R_i^{R_i h(K,m)} g^l \bmod p$. Then DC generates the threshold signature:

$$S = \sum_{U_j \in P_i} S_j + A_i h(K,m) - l \bmod q \tag{3}$$

And {m, S, K, R} is the final threshold signature on the message m.

2) Any verifier can verify the validity of the threshold signature {m, S, K, R} by checking the following equation:

$$g^S R K^K \equiv (Y)^{h(K,m)} \bmod p \tag{4}$$

If it holds, the verifier accepts the signature, otherwise it's rejected.

D. Anonymity and traceability of the improved scheme

Given two sets of honest players P_1 and P_2, the adversary should not have any significant advantage in guessing which one of them have issued a valid signature. Surely, the improved scheme has the anonymity property. The verifier can check the valid of the threshold signature {m, S, K, R} and cannot reveal any useful information about the secret key or the signers. Because K is a random number and S and R are parameters contain random numbers, they are useless for identifying the signers. So the improved scheme provides anonymous.

When there is a dispute on a signature, the KDC can trace the signers who participated in making the threshold signature. (1) If DC acts in concert with KDC, then DC shows the random integer l which he used in the phase of generation of threshold signature to KDC when the KDC asked. The KDC computes $r = R \cdot g^{-l} \bmod p$, which is equal to $r = R_i^{R_i h(K,m)} \bmod p$. Because all ($R_i$, A_i) are generated by KDC, he knows the relationship between (R_i, A_i) and the authorized subset P_i. And KDC can computes $r_i' = R_i^{R_i h(K,m)} \bmod p$ for i= 1, 2,⋯,α. The (R_i, A_i) makes r_i' equal to r is the right one and the corresponding authorized subset is the signers' set signed the message. (2) If DC doesn't act in concert

with KDC, then KDC need to compute $-l_i - K\sum_{U_j \in P_i} k_i \mod p$, obviously, it's equal to $S - \sum_{U_j \in P_i} x_i h(K,m) - A_i h(K,m) \bmod q$. Then KDC can compute the value r which is mentioned earlier and $r = Rg^{-l_i - K\sum_{U_j \in P_i} k_i} K^K \bmod p$. Now the remaining steps is described in part one. So the KDC can trace the signers.Therefore, the improved threshold scheme satisfies the properties of the signers' anonymity and traceability.

4. ANALYSIS OF THE IMPROVED SCHEME

The correctness and security of the improved scheme will be discussed in this section.

A. Correctness

1) If $(K_j)^K g^{S_j} = y_j^{h(K,m)} \bmod p$, then S_j is the valid partial signature produced by U_j.

Proof:

$$\begin{aligned}&(K_j)^K g^{S_j} = g^{k_i K} g^{x_j h(K,m) - Kk_j} \bmod p\\ &= g^{x_j h(K,m)} \bmod p = y_j^{h(K,m)} \bmod p\end{aligned}$$

2) If $g^S RK^K \equiv (Y)^{h(K,m)} \bmod p$, then $\{m, S, K, R\}$ is the valid threshold signature of m.

Proof:

$$\begin{aligned}&g^S RK^K = g^{\sum_{U_j \in P_i} S_j + A_i h(K,m) - l} \cdot R_i^{R_i h(K,m)} g^l \cdot g^{K\sum_{U_j \in P_i} k_i} \bmod p\\ &= g^{\sum_{U_j \in P_i} [x_j h(K,m) - Kk_j]} g^{A_i h(K,m)} \cdot R_i^{R_i h(K,m)} \cdot g^{K\sum_{U_j \in P_i} k_i} \bmod p\\ &= g^{\sum_{U_j \in P_i} [x_j h(K,m)]} g^{A_i h(K,m)} \cdot R_i^{R_i h(K,m)} \bmod p\\ &= g^{\sum_{U_j \in P_i} [x_j h(K,m)] + A_i h(K,m)} g^{s_i R_i h(K,m)} \bmod p\\ &= g^{[\sum_{U_j \in P_i} (x_j) + A_i + s_i R_i] h(K,m)} \bmod p\\ &= g^{Xh(K,m)} \bmod p\\ &= (Y)^{h(K,m)} \bmod p\end{aligned}$$

Therefore, the threshold signature $\{m, S, K, R\}$ can be verified.

B. Security analysis of the improved scheme

1) The adversary cannot forge a valid partial signature satisfying Eq. 2.

Suppose an attacker tries to imitate a player U_i and generate a legitimate partial signature. According to the Eq. 1, the attacker needs to get the player's secret key x_i. However, solving x_i from the public information is more difficult than solving discrete logarithm problem (DLP). Even if the attacker got a valid partial signature, he cannot get x_i because there are two unknown parameters x_i and k_i in Eq. 1. Moreover, parameter substitution attack is useless for this scheme because of the secure one-way hash function h (). So the adversary cannot forge a valid partial signature satisfying Eq. 2.

2) The adversary cannot forge a valid threshold signature of message m satisfying Eq. 4.

Suppose an attacker tries to forge a valid threshold signature, then the forged signature needs to make the Eq. 4 hold, which means that attacker got all players private keys of at least one authorized subset. We know that it is impossible. Another way is getting the secret key X, but it's also impossible because the attacker cannot get the players' private keys and (R_i, A_i) is useless because of the lack of s_i. From the Eq.3 and 4, the improved scheme is secure against substitution attacks under the DLP and one-way hash function assumptions. So this attack cannot work successfully.

3) No matter how many players are in collusion, they cannot cooperate to release non-conspirator's private keys, let alone the group's secret key.

To against the conspiracy attack, the KDC doesn't broadcast the $G_i = X - \sum_{U_j \in P} x_j$, computes (R_i, A_i) for each authorized subset as a substitute and $G_i = X - \sum_{U_j \in P} x_j = s_i R_i + A_i \bmod q$. Then the conspirators cannot get the secret key X because s_i is a secret kept by KDC. As the KDC divided the X into n pieces randomly,

nobody can deduce a non-conspirator's private key no matter how much keys he knows from other conspirators. So the players' private keys cannot be released by the conspirators from the public information. As a result, in the improved scheme, the conspirators cannot get more useful information then a player does. Therefore the improved scheme withstands conspiracy attack and overcomes the weakness in the previously Qin et al.'s scheme.

5. Conclusion

The purpose of proposed threshold signature scheme based on the general access structure is breaking the applied limitation of the conventional threshold signature schemes based on the general access structure. In this paper, we pointed out the security weakness of the Qin et al.'s threshold signature scheme. Furthermore, we proposed an improved scheme which overcomes its weakness. And the security analysis result shows that the improved scheme can withstand the conspiracy attack and has the properties of the signers' anonymity and traceability. It is still an interesting problem to develop or analyze threshold signature schemes based on the General Access Structure.

Acknowledgements

This work was supported by the Beijing Municipal Natural Science Foundation (Grant No.1102003) and the National Basic Research Program of China (Grant No. 2007CB311106).

References

[1] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In: Proceedings of Crypto'91, Santa Barbara, California, USA, 1991: 457 – 469.
[2] Lee N Y. Threshold signature scheme with multiple signing policies. IEE Proc-Compute Digit Tech, 2001, 148(2): 95 – 99.
[3] PANG Liao-jun, JIAO Li-cheng. Changeable Threshold Signature Scheme without a Trusted Center. ACTA ELCTRONICA SINICA, 2008, 36(8): 1559-1563.
[4] Ham L. Group-oriented (t, n) threshold digital signature scheme and digital multi-signature. IEEE Proceedings of Computers and Digital Technique, 1994, 141(5): 307-313.
[5] Chang T.Y., Yang C.C., Hwang M.S. A threshold signature scheme for group communications without a shared distribution center. Future Generation Computer Systems, 2004, 20(6): 1013-1021.
[6] XIE Qi, YU Xiu-Yuan. A (*t, n*) Threshold Group Signature Scheme Based on Block Secret Sharing. Chinese Journal of Computers, 2005, 28(2): 209-213.
[7] Yu J., Kong F.Y., Hao R. A Note on a Forward Secure Threshold Signature Scheme from Bilinear Pairing. Journal of Computer Research and Development, 2010, 47(4): 605-612.
[8] Yang X.D., Wang C.F.. Threshold Proxy Re-signature Schemes in the Standard Model. CHINESE JOURNAL OF ELECTRONICS, 2010, 19(2): 345-350.
[9] Chen Wei-dong, Feng Deng-guo. A group of threshold group-signature schemes with privilege subsets. Journal of Software, 2005, 16(7): 1289-1295.
[10] QIN Hua-wang, DAI Yue-wei and WANG Zhi-quan. Threshold Signature Scheme Based on the General Access Structure. Journal of Beijing University of Posts and Telecommunications, 2009，32(6)：102-105.