中華民國八十六年全國計算機會議

秘密分享系統之另一種公平重建方法

Yet Another Fair Reconstruction Method for Secret Sharing Schemes

黃裕峰 吳宗成 吳宗杉
Huang Yu-Feng Wu Tzong-Chen Wu Tzong-Sun

國立台灣科技大學資訊管理系
Department of Information Management
National Taiwan University of Science and Technology
tcwu@cs.ntust.edu.tw

摘要

在大部份以往所提出的秘密分享系統中，最後一位拿出次金鑰（shadow）的參與者總是有能夠成功地欺騙其他秘密分享者的優勢。在本文中，我們將提出解決上述欺騙問題的公平秘密重建（fair secret reconstruction）方法。在此方法中，系統需要信賴中心參與解密，然而，它並不需要知道分享之秘密內容。在信賴中心的協助之下，本方法可保證僅在所有的參與者均拿出真正的次金鑰之後，這些參與者才可解出分享的秘密。反之，若有欺騙者存在，則該欺騙者必定會被其他參與者指認出來，而且任何人都無法得到共享的秘密。本方法可以修改應用於順序式或是廣播式之系統架構。另外，它也可以套用於任何種類的秘密分享系統，以達到秘密重建的公平性。

關鍵字：門檻方法、秘密分享、公平秘密重建、欺騙者指認。

Abstract

In most of the previously proposed secret sharing schemes, the participant who is the last one to present his shadow for secret reconstruction always has the advantage to plot a cheating trick and could cheat successfully. In this paper, we propose a fair secret reconstruction method to resolve the problem stated above. In the proposed method, a trusted server is required, however the trusted server does not know the secret throughout the secret reconstruction stage. With the assistance of the trusted server, the proposed method assures that the secret can be fairly reconstructed only when all participants present their true shadows. On the other side, any cheater will be deterministically identified by the other participants and no one can obtain the true secret alone. The proposed method can be easily adopted to the sequential and the broadcasting architectures. Moreover, we can employ the proposed method to any kind of secret sharing schemes to realize its fairness for secret reconstruction.

Keywords: threshold scheme, secret sharing, fair secret reconstruction, cheater identification.

1. Introduction

A (t, n) threshold scheme provides a flexible and reliable method to share a secret among n participants suspicious with each other such that at least t participants are required to construct the secret. In a (t, n) threshold scheme, the shared secret is divided into n shadows and each is possessed by one participant, such that the following conditions are satisfied:

1. Any t or more shadows can be used to reconstruct the secret.

2. Any $t-1$ or less shadows cannot be used to reconstruct the secret.

In 1979, two novel (t, n) threshold schemes for secret sharing were independently introduced by Shamir [15] and Blakley [1]. Since then, researches on secret sharing schemes and their applications have been extensively studied in the past decade [5, 8, 9, 10].

Suppose t out of n participants want to reconstruct the secret protected in a (t, n) threshold scheme. These t participants could reconstruct the secret if they present their own shadows and follow the predetermined secret reconstruction procedure. However, if there exists a dishonest participant (i.e., cheater) who presents a fake shadow to the other $t-1$ honest participants, then only the cheater can obtain the true secret alone, whereas all the other participants will obtain the false one. The cheating problem has a negative impact on the righteousness for secret sharing schemes. Many researches are focused on how to detect cheating or identify cheaters for secret sharing schemes [2, 4, 13, 17].

Tompa and Woll [16] demonstrated the weakness of Shamir's scheme [15] and proposed an elegant method against cheating tricks. With a small modification of Shamir's scheme, the Tompa-Woll scheme dramatically reduces the probability of a successful cheating to $1/w$, where w is the number of subshadows distributed to each participant. However, in the Tompa-Woll scheme, participants should pool their subshadows simultaneously in the secret reconstruction stage; otherwise the participant who is the last one to present his subshadows would have the advantage to plot a successful cheating during the secret construction stage.

Recently, Lin and Harn [12] proposed a fair secret reconstruction method for resolving the cheating

problem inherent in secret sharing schemes. In the Lin-Harn scheme, participants do not require to pool their subshadows simultaneously. Unfortunately, the participant who is the last one to present his subshadows still could plot the same cheating trick as in the Tompa-Woll scheme, although the probability of a successful cheating is $1/w$. Even if the cheater cannot succeed in obtaining the secret alone, his fake subshadow may fool the other participants by mistaking some value as the secret.

For most of the previously proposed (t, n) secret sharing schemes, the dishonest participant, who is the last one and presents a fake shadow (or subshadow) during the secret reconstruction stage, may have very high probability to obtain the secret alone, even he is identified at last. In such case, all the other honest participants will obtain the false secret. Hence, the fairness of secret reconstruction collapses. We say that a (t, n) secret sharing scheme is fair if its secret reconstruction procedure meets the following properties:

Completeness: All t out of n participants can obtain the secret if they are honest.

Robustness: No participant can obtain the secret alone if there exists any cheater.

It will see, as discussed in Section 2, that the Tompa-Woll and the Lin-Harn secret sharing schemes are not truly fair, since both of these two schemes do not satisfy the completeness property stated above.

In this paper, we intend to propose a fair secret reconstruction method for secret sharing schemes. In the proposed method, a trusted server involves in the secret reconstruction stage, however the trusted server does not know the secret throughout the secret reconstruction stage. With the assistance of the trusted server, the proposed method assures that the secret can be fairly reconstructed only when all participants present their true shadows. On the other side, any cheater will be deterministically identified by the other participants and no one can obtain the secret alone. We also show that the proposed method is indeed fair, i.e., it meets the robustness and the completeness properties. Moreover, we can employ the proposed method to any kind of secret sharing schemes to realize its fairness for secret reconstruction.

2. Review of previous researches

To facilitate the understanding of the cheating tricks taken in the secret sharing schemes, three well-known secret sharing schemes (Shamir's scheme [15], the Tompa-Woll scheme [16] and the Lin-Harn scheme [12]) are briefly reviewed in the following.

Assume that n participants, say U_1, U_2, ..., and U_n, share a secret $D < q$, for q is a large prime, and let t out of n participants can reconstruct D. In Shamir's scheme, the secret dealer (SD) initially constructs a polynomial $f(x)$ of degree $t-1$ over GF(q):

$$f(x) = D + a_1 x + \ldots + a_{t-1} x^{t-1} \bmod q, \qquad (1)$$

where $a_i \in Z_q$. Then, SD computes a shadow $s_i = f(i)$ and distributes it to U_i (for $i = 1, 2, \ldots, n$) via a secure channel. When any t or more $t-1$'s want to recover D, they present their own shadows s_i's to the others, reconstruct $f(x)$ by interpolating on points (i, s_i)'s, and then obtain the secret $D = f(0)$.

Tompa and Woll [16] demonstrated a weakness of Shamir's scheme that a dishonest participant could fool the others and obtain D alone in the secret reconstruction stage by presenting a fake shadow. Suppose that U_1, U_2, ..., and U_t want to reconstruct D and U_1 is a cheater. U_1 may first construct a polynomial $g(x)$ of degree at most $t-1$, such that $g(0) = -1$ and $g(i)=0$, for $i=2, 3, \ldots, t$. After that, he presents $s_1 + g(1)$ as his shadow to the others. In such case, all participants will construct an interpolating polynomial $f(x) + g(x)$. However, only U_1 (the cheater) can obtain the true D alone by subtracting $g(0)$ from $f(0) + g(0)$, whereas the other participants will get a false secret $f(0) + g(0) \neq D$.

To overcome the weakness of Shamir's scheme, Tompa and Woll [16] suggested a (t, n) threshold protecting policy to safeguard the secret. Their protecting policy is described as follows. Let F be never used as the value of a real secret and be published to all participants. Initially, SD constructs two distinct $(t-1)$-degree polynomials $f(x)$ and $g(x)$, such that $f(0) = D$ and $g(0) = F$. Then, SD hides D in the sequence D_1, D_2, ..., D_w for some w, such that $D = D_a$ for some a randomly chosen and $D_j = F$ for $j \neq a$. Afterwards, SD divides each D_j (for j=1, 2, ..., w) into n subshadows $D_j^{(1)}$, $D_j^{(2)}$, ..., $D_j^{(n)}$ by applying Shamir's scheme, and dispatches a sequence of subshadows $D_1^{(i)}$, $D_2^{(i)}$, ..., $D_w^{(i)}$ to U_i (for i=1, 2, ..., n) via a secure channel. To reconstruct D, any t out of n participants pool their subshadows, one by one, to reconstruct a $(t-1)$-degree polynomial $h(x)$ and check whether $h(0) = F$. If the equation holds, then these t participants discard the used subshadows from their subshadow sequences and do the reconstruction procedure again. Otherwise, the $h(0)$ in the current round shall be the secret. It is to see that the cheater should guess at which position the true subshadow is located in the subshadow sequence before plotting a cheating trick. Hence, the cheater who is not the last one to present his subshadows could cheat successfully with the probability $1/w$; whereas the cheater who is the last one to present his subshadow can always cheat successfully. Even if the cheater cannot cheat successfully, he can fool the others to regard $h(0)$ as the final result, which is a false secret.

The Tompa-Woll scheme is difficult to be implemented in real applications, because t out of n participants must simultaneously present their subshadows in the secret reconstruction stage. Lin and Harn [12] proposed a modified Tompa-Woll scheme that any t out of n participants can fairly reconstruct the secret without simultaneously presenting their subshadows. The Lin-Harn scheme is described as follows. Like the Tompa-Woll scheme, SD publishes an randomly chosen $F \neq D$ and hides D in the sequence D_1, D_2, ..., D_w for some w, such that $D_{a-1} = D$, $D_a = F$ and $D_j \neq F$ for some a randomly chosen and $j \neq a-1$ and $j \neq a$. Afterwards, SD divides D_j (for j=1, 2, ..., w) into n subshadows $D_j^{(1)}$, $D_j^{(2)}$, ..., $D_j^{(n)}$ by applying Shamir's scheme, and dispatches a

sequence of subshadows $D_1^{(i)}$, $D_2^{(i)}$, ..., $D_w^{(i)}$ to U_i (for i=1, 2, ..., n). To reconstruct D, any t out of n participants pool their subshadows (not in a simultaneous manner), one by one, to reconstruct a $(t-1)$-degree polynomial $h(x)$ and check whether $h(0) = F$. If the equation holds, then the secret shall be the $h(0)$ in the previous round. It is to see that in the Lin-Harn scheme the cheater who is the last one to present his subshadow still can cheat successfully with the probability $1/w$, if he could guess at which position the true subshadow is located in the subshadow sequence before plotting a cheating trick.

3. The proposed method for fair secret reconstruction

In this section, we shall present a fair secret reconstruction method for secret sharing schemes with respect to the sequential and the broadcasting architectures. The proposed method is divided into three stages: the system initialization stage, the shadow generation stage and the secret reconstruction stage. In our system, a trusted server (TS) is required. The role of TS is somewhat like the legitimate agency in real life, i.e., he is trusted by all participants. As pointed out in [12, 16], any dishonest participant who is the last one to present his shadow always has the advantage for plotting a cheating trick in the secret reconstruction stage. It is reasonable to assume that TS should never conspire with any participant to plot a cheating trick, or else the achievement of the fairness of secret reconstruction will be impossible. However, TS does not know the secret throughout the secret reconstruction stage. These three stages are described in the following.

The System Initialization Stage -- First of all, secure communication channels for communicating entities should be provided in advance. In the sequential architecture, one can use a public key distribution system (PKDS), for instance, the Diffie-Hellman PKDS [6], to establish secure channels between SD and participant (for issuing a shadow to the dedicated participant in the shadow generation stage), and between participant and participant (for presenting shadows in the secret reconstruction stage). As to the broadcasting architecture, one can use a conference key distribution system (CKDS), for instance, the Burmester-Desmedt CKDS [3] and the Hwang-Yang CKDS [11], to establish a secure channel among participants for presenting shadows in the secret reconstruction stage. For identifying cheaters in the secret reconstruction stage, SD selects a signature generation key K and publishes signature verification key P, an available signature generation function Sig, and the corresponding signature verification function Ver such that $Ver(P,s,Sig(K,s))$ = TRUE if the shadow s is signed with the secret key K by SD, otherwise $Ver(P,s,Sig(K,s))$ = FALSE. The functions Sig and Ver could be easily implemented by some well-known signature schemes, such as the RSA scheme [14] and the ElGamal scheme [7].

The Shadow Generation Stage -- Let D be the secret that can be reconstructed by any t out of n participants U_1, U_2, ..., and U_n. First, SD uses a $(t+1, n)$ threshold scheme, e.g., the Shamir's scheme [15], to divide D into $n+1$ shadows s_1, s_2, ..., s_n, and s_T, and computes their corresponding signatures $Sig(K,s_1)$, $Sig(K,s_2)$, ..., $Sig(K,s_n)$, and $Sig(K,s_T)$. Next, SD issues $\{s_i, Sig(K,s_i)\}$ to U_i (for i = 1, 2, ..., n) and $\{s_T, Sig(K,s_T)\}$ to TS via pre-established secure channels.

The Secret Reconstruction Stage -- Without loss of generality, suppose that U_1, U_2, ..., and U_t want to collaboratively reconstruct the secret D. For simplicity of describing how to identify a potential cheater, we assume that the established secure channels are resistant to any natural or man-made noise when proceeding communications in this stage. The secret reconstruction procedures for the sequential and the broadcasting architectures are separately described in the following.

Secret Reconstruction for Sequential Architecture:

Step 1. For $a = 0$ to $t-2$, do the following:

(1-1). U_i (for i = 1, 2, ..., t) presents $\{s_i, Sig(K,s_i)\}$ to $U_{((i+a) \bmod t)+1}$.

(1-2). $U_{((i+a) \bmod t)+1}$ checks whether $Ver(P,s_i,Sig(K,s_i))$ = TRUE. If the equation does not hold, $U_{((i+a) \bmod t)+1}$ announces that U_i is a potential cheater and terminates the procedure.

Step 2. After receiving the true shadows sent from the other $t-1$ participants, U_i (for i = 1, 2, ..., t) sends an acknowledge to TS.

Step 3. Upon receiving the acknowledges sent from these t participants, TS publishes $\{s_T, Sig(K,s_T)\}$.

Step 4. U_i (for i = 1, 2, ..., t) checks whether $Ver(P,s_T,Sig(K,s_T))$ = TRUE. If the equation holds, U_i uses the shadows s_1, s_2, ..., s_t, and s_T to reconstruct D alone. Otherwise TS may be impersonated by some malicious adversary.

Secret Reconstruction for Broadcasting Architecture:

Step 1. Each U_i (for i = 1, 2, ..., t) broadcasts $\{s_i, Sig(K,s_i)\}$ to the others via the pre-established secure channel.

Step 2. Upon receiving $\{s_i, Sig(K,s_i)\}$, each U_j, for $j \neq i$, checks whether $Ver(P, s_i, Sig(K,s_i))$ = TRUE. If the equation does not hold, U_j announces that U_i is a potential cheater and terminates the procedure.

Step 3 to Step 5. As Step 2 to Step 4 in the sequential architecture.

In both the sequential and the broadcasting architectures, TS does not have any knowledge of D throughout the secret reconstruction stage, since the shadows s_1, s_2, ..., and s_t are presented via the pre-established secure channel among participants and are never seen to him. A simple example for illustrating the secret reconstruction procedure in the sequential architecture is given. From this example, the reader can

easily sketch the secret reconstruction procedure in the broadcasting architecture.

Example: Assume that a secret D is shared by a set of n participants, $\{U_1, U_2, ..., U_n\}$, such that any five out of n participants can reconstruct it. In the shadow generation stage, SD uses a $(6, n)$ threshold scheme to divide D into $n+1$ shadows and then issues $\{s_i, Sig(K,s_i)\}$ to U_i (for $i = 1, 2, ..., n$) and $\{s_T, Sig(K,s_T)\}$ to TS. Suppose that U_1, U_2, U_3, U_4 and U_5 want to reconstruct D in the sequential architecture. Table 1 shows the shadows received by U_i (for $i = 1, 2, ..., 5$) in each sequential round after the presentation of shadows. It is to see that each U_i (for $i = 1, 2, ..., 5$) will obtain five verified shadows, i.e., s_1, s_2, ..., and s_5, after four sequential rounds. Upon receiving five acknowledges sent from U_1, U_2, U_3, U_4 and U_5, TS publishes $\{s_T, Sig(K,s_T)\}$. Afterwards, each U_i (for $i = 1, 2, ..., 5$) can individually reconstruct D by using s_1, s_2, ..., s_5 and s_T. On the other hand, if any one of these participants has identified a potential cheater and does not send an acknowledge to TS, TS will not publish $\{s_T, Sig(K,s_T)\}$. Therefore, no participant can reconstruct D, because one true shadow, i.e., s_T, is lacking.

4. Fairness of the proposed method

In the following, we will show that the proposed secret reconstruction method is fair in both the sequential and the broadcasting architectures.

Security Issue 1. (Completeness property) All t out of n participants can obtain the secret if they are honest.
Justification of Security Issue 1: Consider a t out of n secret sharing scheme. In both the sequential and the broadcasting architectures, the honest participant will send an acknowledge to TS if he has received the other $t-1$ verified shadows. TS will publish his dummy shadow s_T only when he has received the acknowledges sent from these t participants. Afterwards, each of these t participants can individually reconstruct the secret by using the shadow for himself, the $t-1$ shadows presented by the others, and the dummy shadow published by TS to reconstruct the secret. □

Security Issue 2. (Robustness property) No participant can obtain the secret alone if there exists any cheater.
Justification of Security Issue 2: The justification is based on the following two facts:

Fact 1: TS would never publish his dummy shadow unless he has received the acknowledges sent from these t participants.

Fact 2: The dishonest participant or the conspiratorial participants will be identified during the secret reconstruction stage, since the cheater(s) cannot forge a signature for a fake shadow without knowing the signature key, i.e., K for SD.

Consider the sequential architecture. If Fact 2 happens, then the secret reconstruction procedure will be forcedly terminated by the participant who has identified the cheater(s). Hence, no participant can get enough shadows to reconstruct the secret (including the cheater). As to the broadcasting architecture, the cheater may have the chance (if he is the last one to present his shadow) to get the other honest participants' shadows. The other honest participants will detect the cheating trick at last before sending their acknowledges to TS. However, by Fact 1, TS will not publish his dummy shadow to the participants. Thus, the cheater still does not have enough shadows to reconstruct the secret. □

5. Conclusions

We have presented a fair secret reconstruction method for secret sharing schemes. The proposed method can be easily adopted to the sequential and the broadcasting architectures. With the assistance of a trusted server, the proposed method assures that only participants present their shadows, the secret can be fairly reconstructed. On the other side, any cheater will be deterministically identified by the other participants and no one can obtain the true secret alone. Note that the trusted server does not know the secret throughout the secret reconstruction stage.

In the proposed method, each participant requires to possess one shadow and its signature, and not more than one cheaters can be deterministically identified, whereas in the Lin-Harn scheme [12], each participant requires to possess a sequence of w subshadows and the cheater has the probability $1/w$ to cheat successfully. Table 2 shows the comparison of capabilities for secret reconstruction provided in the proposed method and some well-known previously proposed secret sharing schemes.

References

[1] Blakley, G. R., "Safeguarding cryptographic keys", *Proceedings AFIPS 1979 National Computer Conference*, New York, Vol. 48, 1979, pp. 313-317.

[2] Brickell, E. F. and Stinson, D. R., "The detection of cheaters in threshold schemes", *Advances in Cryptology - CRYPTO '88*, Springer-Verlag, Berlin, 1989, pp. 564-577.

[3] Burmester, M. and Desmedt, Y., "A secure and efficient conference key distribution", *Advances in Cryptology - EUROCRYPT '94*, Springer-Verlag, Berlin, 1995, pp. 275-286.

[4] Carpentieri, M., "A perfect threshold secret sharing scheme to identify cheaters", *Designs, Codes and Cryptography*, Vol. 5, No. 3, 1995, pp. 183-187.

[5] Desmedt, Y. and Frankel, Y., "Shared generation of authenticators and signatures", *Advances in Cryptology - CRYPTO '91*, Springer-Verlag, Berlin, 1992, pp. 457-469.

[6] Diffie, W. and Hellman, M. E., "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976, pp. 644-654.

[7] ElGamal, T., "A public-key cryptosystem and a signature based on discrete logarithms", *Advances in Cryptology - CRYPTO '84*, Springer-Verlag, Berlin, 1985, pp. 10-18.

[8] Harn, L., "Efficient sharing (broadcasting) of multiple secrets", *IEE Proceedings - Computers and Digital Techniques*, Vol. 142, No. 3, 1995, pp. 237-240.

[9] Harn, L., "Group-oriented (t,n) threshold digital signature scheme and digital multisignature", *IEE Proceedings - Computers and Digital Techniques*, Vol. 141, No. 5, 1994, pp. 307-313.

[10] He, J. and Dawson, W., "Multisecret-sharing based on one-way function", *Electronics Letters*, Vol. 31, No. 2, 1995, pp. 93-95.

[11] Hwang, M.S. and Yang, W.P., "Conference key distribution schemes for secure digital mobile communications", *IEEE Journal on Selected Areas in Communications*, Vol. 13, No. 2, 1995, pp. 416-420.

[12] Lin, H.Y. and Harn, L., "Fair reconstruction of a secret", *Information Processing Letters*, Vol. 55, No. 1, 1995, pp. 45-47.

[13] Rabin, T. and Ben-Or, M., "Verifiable secret sharing and multiparty protocols with honest majority", *Proceedings 21st ACM Symposium on Theory of Computing*, 1989, pp. 73-85.

[14] Rivest, R.L., Shamir, A. and Adleman, L.M., "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.

[15] Shamir, A., "How to share a secret", *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 612-613.

[16] Tompa, M. and Woll, H., "How to share a secret with cheaters", *Journal of Cryptology*, 1988, Vol. 1, No. 2, 1988, pp. 133-138.

[17] Wu, T.C. and Wu, T. S., "Cheating detection and cheater identification in secret sharing schemes", *IEE Proceedings - Computers and Digital Techniques*, Vol. 142, No. 5, 1995, pp. 367-369.

Table 1. The shadows received by the participants in each sequential round.

round	U_1	U_2	U_3	U_4	U_5
1	s_5	s_1	s_2	s_3	s_4
2	s_4	s_5	s_1	s_2	s_3
3	s_3	s_4	s_5	s_1	s_2
4	s_2	s_3	s_4	s_5	s_1

Table 2. Comparison of capabilities for secret reconstruction.

Secret Sharing Scheme	cheating detection	cheater identification	coalition prevention	fair secret reconstruction
Shamir [15]	No	No	No	No
Brickell-Stinson [2]	Yes	Yes	Yes	No
Tompa-Woll [16]	No	No	No	No
Rabin-Ben-Or [13]	Yes	Yes	Yes	No
Carpentieri [4]	Yes	Yes	No	No
Wu-Wu [17]	Yes	Yes	Yes	No
Lin-Harn [12]	Yes	Yes	Yes	Yes*
Proposed method	Yes	Yes	Yes	Yes

* The cheater can cheat successfully with probability $1/w$, where w is the number of subshadows possessed by each participant.