A Novel Multistage Secret Sharing Scheme

Ting-Yi Chang[3], Min-Shiang Hwang[1,2], Shu-Chen Lin, and Wei-Pang Yang[4]

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan, R.O.C.
Department of Health Services Administration, China Medical University[2]
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan
Graduate Institute of e-Learning, National Changhua University of Education[3]
No.1, Jin-De Road, 500 Changhua City, Taiwan, R.O.C.
Department of Information Management, National Dong Hwa University[4]
No. 1, Sec. 2, Da Hsueh Rd., Shoufeng, Hualien 97401, Taiwan, R.O.C.

Abstract: There are two main security issues in a multistage (t, n) secret sharing scheme: 1) Multiple secrets cannot be reconstructed in predetermined order. 2) The secret holder cannot determine the values of the secrets. In this article, we propose a new multistage secret sharing to meet these security issues. There are two advantages in the proposed scheme: 1) the multiple secrets could be reconstructed in predetermined order. 2) The secret holder could determine the values of the secrets.

Keywords: Cryptography, multistage secret sharing, multi-secret sharing, secret sharing

1. Introduction

Secret Sharing is an important application in modern cryptography. Shamir [19] and Blakley [2] first proposed the threshold secret sharing schemes, which are separately based on Lagrange interpolating polynomial and linear projective geometry. In *(t, n)* secret sharing schemes, a secret is usually shared among *n* participants and each participant holds a secret value called shadow which is distributed by the secret holder (dealer) via a secure channel. At least *t* or more participants pool their shadows to collaboratively reconstruct the secret [12, 18, 19]. However, they are one-time-use schemes in most secret sharing schemes (See [14, 17] for a more detailed description). Thus, when some particular secrets have been reconstructed, it is required that the secret holder redistributes a fresh shadow over a secret channel to each participant. Obviously, to redistribute shadows is very inefficient and each user has to keep many secret shadows [1, 13, 21]. On the contrary, no matter what the number of the secret sharing is applied, the secret holder only distributes shadows once called multi-use scheme.

The first multistage secret sharing (MSS) scheme was proposed by He and Dawson [10], based on one-way function, in 1994. They used the public shift value technique to hide the true shadow and the successive applications of a one-way function to make the secrets are reconstructed in a stage-by-stage manner amongst *n* participants. The *k* secrets can be reconstructed one by one in a predetermined order, and the reconstruction of secrets at earlier stages does not reveal or weaken the secrecy of the remaining secrets. Later, He and Dawson proposed an alternative type secret sharing, which is called the dynamic multi-secret sharing scheme [11]. In a dynamic multi-secret sharing scheme, at least *t* participant should work in accordance with the secret holder's public information to reconstruct the secrets. However, *kn* public values are required in He and Dawson's scheme [10]. In order to reduce the public values, Harn [9] proposed another multistage secret sharing scheme with only *k(n-t)* public values.

However, Yang et al. [4] showed that He-Dawson and Harn's schemes are one-time-use schemes. Furthermore these schemes do not appear to offer a stage-by-stage reconstruction of the secret. On the other hand, Chien et al. [6] proposed a multi-secret scheme based on systematic block codes. In their scheme, the secret holder can determine the number of the distributed secrets dynamically and the secrets are reconstructed simultaneously.

In 2004, Yang et al. [22] proposed a *(t, n)* multi-secret sharing scheme, which has fewer public values and less storage as well as computing time than Chien et al.'s scheme. They pointed out that various secret sharing schemes have different approaches and further classify three types of secret sharing as follows.

1) Multi-secret sharing: the secrets are reconstructed simultaneously.
2) Dynamic multi-secret sharing: the secret are reconstructed according to the secret holder's public information.

(DOI: dx.doi.org/14.9831/1444-8939.2014/2-5/MAGNT.6)

3) Multistage secret sharing: the secrets are reconstructed stage-by-stage in predetermined order.

Both Chien et al.'s scheme and Yang et al.'s scheme used the two-variable one-way function *h()*. The two-variable one-way function has the following properties [6]:

1) Given *r* and *s*, it is easy to compute *h(r, s)*.
2) Given *s* and *h(r, s)*, it is hard to compute *r*.
3) It is hard to compute *h(r, s)* for any *r* without the knowledge of *s*.
4) Given *s*, it is hard to find two values r_1 and r_2 be satisfied $h(r_1, s) = h(r_2, s)$.
5) Give *r* and *h(r, s)*, it is hard to compute *s*.
6) Give pairs of r_i and $h(r_i, s)$, it is hard to compute $h(r', s)$ for $r' \neq r_i$.

The above-mentioned properties of the two-variable one-way function have been proven in [11]. Both of these schemes have the common characteristic that allows for parallel secret reconstruction, but the participants need not collaborate to reconstruct the secret by pass in sequence.

To be directed against in the multistage secret sharing schemes, Lee and Hwang [15] proposed a new multistage secret sharing scheme based on the intractability of the factorization (FAC) problem [16]. In their scheme, each participant only keeps one secret shadow, and two public values are required in this system. Their scheme has fewer the number of public values than He-Dawson and Harn's schemes [5, 7].

In this paper, we shall show that there are some weaknesses in their scheme as follows:

1) Multiple secrets cannot be reconstructed in predetermined order.
2) The secret holder cannot determine the values of the secrets, and their scheme is in fact a one-time-use scheme.

At the same time, we propose a new scheme to overcome the above weaknesses.

The remainder of this paper is organized as follows. In Section 2, we shall briefly review Lee-Hwang scheme and show that the weaknesses of their scheme. In Section 3, we shall propose a new multistage secret sharing. In Section 4, we shall analyze the security and properties of our scheme. In Section 5, we give the examples for application of multistage secret sharing and draw our conclusion.

2. The Weaknesses of Lee and Hwang's Scheme

(DOI: dx.doi.org/14.9831/1444-8939.2014/2-5/MAGNT.6)

We first review Lee and Hwang's scheme and then point out its weaknesses. Their scheme is composed of two phases as follows:

(1) The secrets and shadows generation phase:

The secret holder, called SD for short, computes $N=p \times q$, $p=2p'+1$ and $q=2q'+1$, where p, q, p' and q' are primes, and then SD defines $\lambda(N)=2p'q'$. Let α be a primitive element in both $GF(p)$ and $GF(q)$, and randomly choose an integer L with $\gcd(L, \lambda(N))=1$. Publish the parameters n and L, and keep the others secret. Choose some random odd integer d which satisfies $\gcd(d, \lambda(N))=1$. The k secrets S_i (for $I = 0, 1, \ldots, k-1$) are computed by the equation:

$$S_i = \alpha^{d \cdot L^i} \bmod N. \qquad (1)$$

Let A, $|A| = n$, be the set of all participants in the system and any subset B, $|B| = t$, in A. The SD randomly chooses a secret polynomial f(x) mod λ(n) of degree $t-1$ and f(0)=d. Then, SD distributes to each participant u_i, $i \in A$, a public odd integer x_i with an even $f(x_i)$ and a secret shadow K_i as follows:

$$K_i = \alpha^{S_i} \bmod N,$$

$$where\ S_i = \frac{f(x_i)/2}{\left[\prod_{\substack{j \in A \\ j \neq i}} (x_i, x_j)\right]/2} \bmod p'q'.$$

(2) The secrets reconstruction phase:

To reconstruct the secret S_l (for $l=k-1, k-2, \ldots, 0$), each u_i $(i \in B)$ must compute a value $K_{i,l}$ as follows:

$$k_{i,l} = k_i \, L^l \cdot \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \cdot \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j) \bmod N.$$

Then S_l can be reconstructed as follows:

$$\prod_{i \in B} K_{i,l} = S_l \bmod N. \qquad (2)$$

We shall describe some weaknesses in Lee and Hwang's scheme as follows:

1) In their scheme, S_0 can be easily reconstruct by Equation (2), when u_i $(i \in B)$ first provides his/her secret value $K_{i,0}$ $(i \in B)$. Then, they can compute other secrets $S_1, S_2, \ldots, S_{k-1}$ by the following equation $S_{i+1} = S_i^L \bmod N$ (for $i = 0, 1, \ldots, k-2$) without the preceding secrets. On the other hand, t participants collaborate to compute the first secret S_0, and then other secrets $S_1, S_2, \ldots, S_{k-1}$ can be revealed from S_0. Moreover, when S_0 is stolen by any adversary, he/she can obtain other secrets. Although d is

hard to compute in the equation $S_0 = a^d \bmod N$.

2) In the general secret sharing schemes of polynomial [19], the SD can arbitrarily determine the value of the secret. However, in Lee and Hwang's scheme, the SD computes the secrets in Equation (1), and S_i is determined by using the exponent dL_i of α. In other words, the SD cannot determine the value of S_i to follow his/her inclinations.
3) To analyze the computational complexity, the SD costs more computing time in the secrets generation phase. Each participant who generates a secret costs this phase at least one modular exponentiation.

To over the above weaknesses, we propose a new multistage secret sharing based on Shamir's secret sharing and use the two-variable one-way function to protect the shadows.

3. The Proposed Scheme

In order to ensure k secrets s_i be reconstructed in such special order as $s_0, s_1, \ldots, s_{k-1}$, and to make sure the SD can determine the value of secret s_i. Our scheme is composed of two phases as follows:

(1) The secrets generation phase:

The SD generates the secrets in the following steps:

Step 1. Determine the value of first secret s_0 to follow his/her inclination. Then, randomly choose a public prime number p, length is the same as s_0, and generate the $t-1$ degree polynomial $f_0(x) \bmod p$, where $f_0(0) = s_0 \bmod p$.

Step 2. Choose n secret shadows $d_1, d_2, \ldots, d_n$ called true shadows and distribute them to each participant over a secret channel. Publish a random number r and use a two-variable one-way function $h()$ to compute $y_{01}, y_{02}, \ldots, y_{0n}$, where $h(r, d_i)$ called fake shadows.

$$y_{0i} = f_0(h(r, d_i)), i = 1, 2, ..., n.$$

Step 3. Generate others secrets and continue to form the next $t-1$ degree polynomials $f_i(x) \bmod p$, where $f_i(0) = s_i$ for $i=1, 2, \ldots, (k-1)$.

Step 4. Compute and publish y_{ij} for $i= 1, 2, \ldots, k-1$ and $j=1, 2, \ldots, n$ as follows:

$$y_{ij} = f_i(h(s_{i-1}, d_j)).$$

After the above process, the SD can be revoked.

(2) The secrets reconstruction phase:

At least t or more pairs of secret shadows can only determine the $t-1$ degree polynomial $f(x)$ by using the Lagrange interpolation polynomial. The participants reconstruct the secrets in special order as follows:

Step 1. Collect t pairs of $(h(r, d_i), y_{0i})$ to obtain $f_0(0)$ by using the Lagrange interpolation polynomial as follows:

$$f_0(0) = \sum_{i=1}^{t} y_{0i} \prod_{j=1, j\neq i}^{t} \frac{-h(r, d_j)}{h(r, d_i) - h(r, d_j)} \bmod p$$
$$= s_0 \bmod p.$$

Then, they can collaborate to obtain the first secret s_0.

Step 2. In order to obtain the next secret s_i, the t participants must pool their fake shadows $h(s_{i-1}, d_j)$ for $j=1, 2, \ldots, n$. By using the Lagrange interpolation polynomial, $f_i(0)$ can be computed as follows:

$$f_i(0) = \sum_{i=1}^{t} y_{ij} \prod_{j=1, j\neq i}^{t} \frac{-h(s_{i-1}, d_j)}{h(s_{i-1}, d_i) - h(s_{i-1}, d_j)} \bmod p$$
$$= s_i \bmod p.$$

Repeating the Step 2, the remainder secrets can be computed.

To reconstruct the secret s_i, t participants should have the secret s_{i-1} first. Otherwise, they cannot use the value $h(s_{i-1}, d_j)$ to reconstruct the secret s_i by using the Lagrange interpolation polynomial successfully. Obviously, because our scheme is based on Shamir's secret sharing, there are many schemes [3, 8, 20] can be applied to detect cheating. Every participant can verify the validity of his/her own shadow distributed by the SD, which allows the honest participants to ensure that the secret to reconstruct is unique.

4. Discussions

In this section, we discuss the properties and security of our multistage secret sharing scheme as follows. After reconstructing all the secrets, the true shadow d_j is protected under the two-variable one-way function $h( )$. After sharing those secrets, the SD does not need to redistribute the new shadows d'_j to each participant for preparing the next secret sharing. Our scheme is multi-use scheme.

Each participant u_i, $i \in B$, want to reconstruct the secret s_1, he/she must to reconstruct the secret s_0 first, and s_0 on. The reconstruction of the current secret depends on that of the previous secret. Otherwise, they cannot reconstruct the secret. The secrets are reconstructed certainly in the special order $s_0, s_1, \ldots, s_{k-1}$. To reconstruct each secret in each stage, the protocol is based on Shamir's secret sharing scheme. At least t or more participants pooling their shadows will make it easy to reconstruct the secret, but only t-

(DOI: dx.doi.org/14.9831/1444-8939.2014/2-5/MAGNT.6)

1 or fewer shadows provide no more information about the secrets to an opponent than knowing no piece.

From the above discussions, the proposed scheme satisfies the requirements of the prescribed order multistage secret sharing scheme which the SD generates the k secrets $s_0, s_1, \ldots, s_{k-1}$ in sequence and at least *t* participants reconstruct the secrets by the same special order.

5. Application and Conclusion

We have presented an idea about how to use prescribed order multistage secret sharing scheme. For example, in a multistage secret sharing scheme for the security of bank vaults, one must pass thru k checkpoints before the vault can be opened. However, the checkpoints must be opened and passed in sequence by at least t participants together. The other example, in popular on-line game, role play game, the player cannot get into the second stage if he/she doesn't pass the first stage. Several players must cooperate to obtain the gem in this stage, then bring the gem and go to next stage. If he/she doesn't finish the requests, he/she cannot pass in the stage.

We have showed that the weaknesses in Lee-Hwang scheme and proposed a new scheme to make it qualified as a prescribed order multistage secret sharing scheme. In our scheme, the secret holder can arbitrarily determine the secret, at least t or more participants among n participants can collaborate to reconstruct the secret in special order, and it a multi-use scheme. Here, we didn't compare the performance with other multistage secret sharing schemes [9, 10, 15] because those schemes fails to satisfy the properties of multistage secret sharing.

Acknowledgment

This study was supported by the National Science Council of Taiwan under grant NSC 102-2221-E-468 -020; NSC 103-2622-E-468 -001 – CC2; and NSC 103-2622-H-468 -001 -CC2.

References

1. A. Basu, I. Sengupta, and J. K. Sing, ``Cryptosystem for secret sharing scheme with hierarchical groups," International Journal of Network Security, vol.15, no.6, pp.455--464, 2013.
2. G. Blakley, ``Safeguarding cryptographic keys," in Proc. AFIPS 1979 Natl. Conf., pp.313--317, New York, 1979.
3. T. Y. Chang, M. S. Hwang, and W. P. Yang, ``An improvement on the Lin-Wu (t, n) threshold verifiable multi-secret sharing scheme," Applied Mathematics And Computation, vol.163, no.1, pp.169--178, 2005.
4. T. Y. Chang, M. S. Hwang, and W. P. Yang, ``A new multi-stage secret sharing scheme using one-way function," ACM Operating Systems Review, vol.39, no.1, pp.48--55, 2005.
5. T. Y. Chang, M. S. Hwang, and W. P. Yang, ``An improved multi-stage secret sharing scheme based on the factorization problem," Information Technology and Control, vol.40, no.3, pp.246--251, 2011.
6. H. Y. Chien, J. K. Jan, and Y. M. Tseng, ``A practical (t, n) multi-secret sharing scheme," IEICE Transactions on Fundamentals, vol.E83-A, no.12, pp.2762--2765, 2000.
7. M. S. Hwang, C. T. Li, ``An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," International Journal of Innovative Computing, Information and Control, vol.6, no.5, pp.2181--2188, 2010.
8. R. Gennaro and S. Micali, ``Verifiable secret sharing as secure computation," in Advances in Cryptology, EUROCRYPT'95, pp.168--182, Lecture Notes in Computer Science, 1995.
9. L. Harn, ``Comment: Multistage secret sharing based on one-way function," Electronics Letters, vol.31, no.4, pp.262, 1995.
10. J. He and E. Dawson, ``Multistage secret sharing based on one-way function," Electronics Letters, vol.30, no.19, pp.1591--1592, 1994.
11. J. He and E. Dawson, ``Multisecret-sharing sceheme based on one-way function," Electronics Letters, vol.31, no.2, pp.93--95, 1995.
12. M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An efficient threshold decryption scheme without session keys," Computers & Electrical Engineering, vol.27, no.1, pp.29--35, 2000.
13. M. H. Ibrahim, ``Efficient dealer-less threshold sharing of standard RSA," International Journal of Network Security, vol.8, no.2, pp.139--150, 2009.
14. W. A. Jackson, K. M. Martin, and C. M. O'Keefe, ``On sharing many secrets," Asiacrypt'94, pp.42--54, 1994.
15. N. Y. Lee and T. Hwang, ``New multistage secret sharing scheme based on the factorization problem," Journal of Information Science and Engineering, vol.17, no.3, pp.525--529, 2001.
16. N. A. Moldovyan, ``Short signatures from difficulty of factorization problem," International Journal of Network Security, vol.8, no.1, pp.90--95, 2009.
17. J. Pieprzyk and X. M. Zhang, ``Ideal secret sharing schemes from permutations,"

International Journal of Network Security, vol.2, no.3, pp.238--244, 2006.

18. Y. V. S. Rao and C. Bhagvati, ``CRT based threshold multi secret sharing scheme," International Journal of Network Security, vol.16, no.4, pp.249--255, 2014.
19. A. Shamir, ``How to share a secret," Communications of the ACM, vol.22, pp.612--613, 1979.
20. M. Stadler, ``Publicly verifiable secret sharing," in Advances in Cryptology, EUROCRYPT'96, pp.190--199, Lecture Notes in Computer Science, 1996.
21. Y. Tian, C. Peng, and J. Ma, ``Publicly verifiable secret sharing schemes using bilinear pairings," International Journal of Network Security, vol.14, no.3, pp.142--148, 2012.
22. C. C. Yang, T. Y. Chang, and M. S. Hwang, ``A (t, n) multi-secret sharing scheme," Applied Mathematics and Computation, vol.151, no.2, pp.483--490, 2004.

(DOI: dx.doi.org/14.9831/1444-8939.2014/2-5/MAGNT.6)