ISSN 1392–124X INFORMATION TECHNOLOGY AND CONTROL, 2010 Vol. 0, No. 0, 1–7

An Improved Multi-stage Secret Sharing Scheme Based on the Factorization Problem

Ting-Yi Chang

National Changhua University of Education, Graduate Institute of e-Learning
No.1, Jin-De Road, Changhua City, Taiwan, R.O.C.

Min-Shiang Hwang

National Chung Hsing University, Department of Management Information Systems
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Corresponding author: e-mail: mshwang@nchu.edu.tw

Wei-Pang Yang

National Dong Hwa University, Department of Information Management
1, Sec. 2, Da Hsueh Rd., Shou-Feng,
Hualien, Taiwan, R.O.C.

Abstract. Lee and Hwang proposed a multi-stage (t, n) secret sharing scheme which has fewer public values than pervious schemes. In their scheme, a group of participants share multiple secrets stage-by-stage, and only one secret share should been kept by each participant. However, in this article, the authors will show that multiple secrets cannot in fact be reconstructed stage-by-stage by the secret holder's determination and that the secret holder cannot determine the values of the secrets in Lee and Hwang's scheme. Moreover, their scheme belongs to the family of one-time-use schemes. At the same time, we shall also modify their scheme to improve the above weaknesses and show the improved scheme can be applied. The security of the proposed scheme is based on the factorization problem which provides higher security confidence than using the hash function in Harn's and Chang et al.'s multi-stage secret sharing schemes.

Key words: Cryptography, multi-stage, secret sharing, threshold scheme.

1. Introduction

The first secret sharing schemes based on the Lagrange interpolating polynomial and linear projective geometry were proposed by Shamir [24] and Blakley [2], respectively. In (t, n) secret sharing schemes, a secret is usually shared among n participants, and at least t or more participants can collaborate to reconstruct the secret, but only $t - 1$ or fewer participants will not be enough [24]. Based on those properties, secret sharing plays an important role in the modern cryptography [5–8, 17, 21] (e.g., opening bank vaults, signing corporate cheques). However, there is a common drawback in most secret sharing schemes: they belong to the family of one-time-use schemes (See [19] for a more detailed description). Thus, when some particular secrets have been reconstructed, it is required that the secret holder redistributes a fresh share over a secret channel to each participant. Obviously, to redistribute shares is a very costly process.

In 1994, He and Dawson [15] proposed a multi-stage secret sharing scheme based on one-way function. They used the public shift value technique to hide the true share and the successive applications of a one-way function to make the secrets reconstructed stage-by-stage among 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 [16]. 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. In order to reduce the public values, Harn [13] proposed another multi-stage secret sharing scheme with only $k(n - t)$ public values.

In 2000, Chien et al. [11] proposed a multi-secret scheme based on systematic block codes. In their scheme, the secrets are reconstructed in parallel with each other. Though their scheme has fewer public values than previous schemes [13, 15, 16], Yang et al.

[26] pointed out that their scheme belongs to a different type. Each type of secret sharing has a different approach. For some computer games, a treasure map is a variation of a map to help track progress and mark the location of buried treasure swords. One must pass thru k checkpoints before the treasured swords can be obtain. The restriction is that the checkpoints must be opened and passed to reveal a part of treasure map in sequence by at least t participants' cooperations. At the same time, Yang et al. further proposed a new multi-secret sharing scheme that has fewer public values and less storage demand as well as shorter computing time than Chien et al.'s scheme.

In 2004, Chang et al. [9] showed that the schemes in [13] and [15] have the common weakness, which is that the secrets cannot be reconstructed in special order dominated by the secret holder. Any t participants can arbitrarily destroy the order. Moreover, Chang et al. also pointed out that the secret holder cannot determine the values of the secrets in [13]. As we know, if the secret are messages (natural language) which are used to be shared, the secrets have to be determined by the secret holder. Simultaneously, they proposed a multi-stage secret sharing scheme using one-way function. Obviously, a hash function is considered as a black-box that contains an ideally random function in the random oracle model [1]. However, in a "real-world", random oracles do not exist. In other words, the random oracle assumption is more stronger than practical and available cryptographic problems such as the factorization problem and the discrete logarithm problem. Therefore, to design a provable secure multi-stage secret sharing scheme without random oracles is necessary.

Lee and Hwang [20] proposed a new multi-stage secret sharing scheme based on the intractability of the factorization problem. Lee and Hwang 's scheme provided higher security confidence than using the hash function in Harn's [13] and Chang et al's [9] multi-stage secret sharing schemes. In their scheme, each participant only keeps one secret share, and two public values are required in the system. In this paper, we shall show that multiple secrets cannot be reconstructed in predetermined order, and 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 shall also modify Lee and Hwang 's scheme to improve the above weaknesses. Here, we first present the requirements that we reckon a (t, n) multi-stage secret sharing scheme should meet as follows. We assume that there are k secrets S_i ($i = 0, 1, \cdots, k-1$) to be shared among n participants.

- *Threshold feature.* Any t out of n share holders can collaborate to reconstruct S_i, but it is impossible to reconstruct S_i with the knowledge of $t-1$ or fewer secret shares.
- *Determine the values of secrets.* The secret holder can arbitrarily determine the value of S_i.
- *Multi-stage feature.* The secrets will be reconstructed in such predetermined order as $S_{k-1}, S_{k-2}, \cdots, S_0$ by the secret holder's domination, and the reconstruction of secrets at earlier stages does not reveal or weaken the secrecy of the remaining secrets.
- *Multi-use feature.* When some particular secrets have been reconstructed, it is not required that the secret holder redistribute a fresh share over a secret channel to each participant.
- *Efficient.* Each participant only has to keep one secret share.

The proposed scheme satisfies the above features and its security is based on the factorization problem. The remainder of this paper is organized as follows. In Section 2, we shall briefly review Lee and Hwang's scheme. At the same time, we shall also show that the weaknesses of their scheme. In Section 3, we shall propose a new multi-stage secret sharing by modifying Lee and Hwang's scheme. In Section 4, we shall analyze the security and properties of our scheme. Finally, we shall draw our conclusion in Section 5.

2. The Weaknesses of Lee and Hwang's Scheme

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

(1) The secrets and shares generation phase:
The trusted *Secret Holder* (SD) 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 $\mathbb{GF}(p)$ and $\mathbb{GF}(q)$, and randomly choose an integer L with $\gcd(L, \lambda(n)) = 1$. The parameters n and L are public, and the others are secret. The k secrets S_i (for $i = 0, 1, \cdots, k-1$) are computed by the following equation:

$$S_i = \alpha^{d \cdot L^i} \bmod n, \tag{1}$$

where d is a random odd integer with $\gcd(d, \lambda(n)) = 1$. Let A ($|A| = n$) be the set of all participants in the system and any subset B ($|B| = t$) in A. SD randomly chooses a secret polynomial $f(x) \bmod \lambda(n)$ 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 $f(x_i)$ [12] and a secret share K_i as:

$$\begin{aligned} K_i &= \alpha^{s_i} \bmod n, \quad \text{where} \\ s_i &= \frac{[f(x_i)/2]}{\left[\left(\prod_{\substack{j\in A \\ j\neq i}} (x_i - x_j)\right)\right]/2} \bmod p'q'. \end{aligned} \quad (2)$$

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

$$K_{i,l} = K_i^{L^l \cdot \prod_{\substack{j\in A \\ j\notin B}} (x_i - x_j) \cdot \prod_{\substack{j\in B \\ j\neq i}} (0 - x_j)} \bmod n. \quad (3)$$

Then S_l can be reconstructed as:

$$\begin{aligned} \prod_{i\in B} K_{i,l} &= \prod_{i\in B} K_i^{L^l \cdot \prod_{\substack{j\in A \\ j\notin B}} (x_i - x_j) \cdot \prod_{\substack{j\in B \\ j\neq i}} (0 - x_j)} \bmod n \\ &= \alpha^{\sum_{i\in B} s_i \cdot L^l \cdot \prod_{\substack{j\in A \\ j\notin B}} (x_i - x_j) \cdot \prod_{\substack{j\in B \\ j\neq i}} (0 - x_j)} \bmod n \\ &= \alpha^{f(0)\cdot L^l} \bmod n \\ &= S_l \bmod n. \end{aligned} \quad (4)$$

In the next multi-stage secret sharing, the SD only needs to choose a new public value L' with $\gcd(L', \lambda(n)) = 1$. In the following, we show that the SD cannot determine the values of secrets and their scheme does not satisfy multi-stage feature and multi-use feature, respectively.

Determine the values of secrets:
In the general secret sharing schemes of polynomial [24], the SD chooses the polynomial one of whose constant terms is the secret. So 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 what the value of S_i is.

Multi-stage feature:
When u_i $(i \in B)$ provides the pseudo share in Equation (3) but not in the special order desired: $K_{i,k-1}, K_{i,k-2}, \cdots, K_{i,0}$ $(i \in B)$, the secrets will not be reconstructed in that special order: S_{k-1}, S_{k-2}, $\cdots$, S_0. For example, when u_i $(i \in B)$ first provides his/her secret value $K_{i,0}$ $(i \in B)$, S_0 can be easily reconstruct by Equation (4). Then, they need not provide other pseudo shares $K_{i,k-1}$, $K_{i,k-2}$, $\cdots$, $K_{i,0}$, and the remaining secrets $S_1, S_2, \cdots, S_{k-1}$ can be revealed form knowing S_0 by computing the following equation (for $i = 0, 1, \cdots, k-2$):

$$S_{i+1} = S_i^L \bmod n.$$

Multi-use feature:
When $S_0 = \alpha^{dL^0} = \alpha^d \bmod n$ is reconstructed, every u_i $(i \in B)$ has the knowledge of value $\alpha^d \bmod n$. In the next multi-stage secret sharing, the SD publishes a new L' such that $\gcd(L', \lambda(n)) = 1$ and prepares the secret S_i' (for $i = 0, 1, \cdots, k-1$) as follows.

$$S_i' = \alpha^{dL'^i} \bmod n.$$

Therefore, every u_i $(i \in B)$ can use $S_0 = \alpha^d \bmod n$ to obtain any secret by the SD's computation in the above equation without other $t-1$ participants' cooperation. Hence, SD should choose another polynomial $f'(x)$ where $f'(0) = d'$ and a fresh share K_i' in Equation (4) for each u_i $(i \in A)$. I thinks that this error is only one typo or careless in preparing the secrets in Equation (1). If the last secret S_0 is removed, no one can obtain $\alpha^d \bmod n$ from $\alpha^{dL} \bmod n$ if the factors of n are unknown.

3. The Proposed Scheme

To ensure k secrets S_i be reconstructed in such special order as $S_{k-1}, S_{k-2}, \cdots, S_0$, and to make sure the SD can determine the value of S_i without redistributing K_i, we only modify in Lee and Hwang's scheme a bit. Our scheme is also composed of two phases as follows:

(1) The secrets and shares generation phase:
The parameters $(n, p, q, p', q', \lambda(n), \alpha, L, d, f(x))$ in our new scheme are the same as those in Lee and Hwang's scheme. The SD first chooses the secrets S_i $(i = k-1, k-2, \cdots, 0)$ and computes a value $\widehat{S}_{k-1}$ as:

$$\widehat{S}_{k-1} = \alpha^{d\cdot L} \bmod n.$$

The SD computes a public value P_{k-1} as:

$$P_{k-1} = \widehat{S}_{k-1} \oplus S_{k-1}.$$

Then, the SD computes $\widehat{S}_i$ and public values P_i (for $i = k-2, k-3, \cdots, 0$) as:

$$\begin{aligned} \widehat{S}_i &= \alpha^{d \cdot L \cdot S_{i+1}} \bmod n \\ P_i &= \widehat{S}_i \oplus S_i. \end{aligned}$$

The public odd integer x_i and secret share K_i in Equation (2) for each participant u_i $(i \in A)$ are the same as those in Lee and Hwang's scheme.

(2) The secrets reconstruction phase:
To reconstruct the secrets, each participant u_i $(i \in B)$ first computes $K_{i,k-1}$ as:

$$K_{i,k-1} = K_i^{L \cdot \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \cdot \prod_{j \neq i} (0 - x_j)} \bmod n. \tag{5}$$

Then, $\widehat{S}_{k-1}$ can be computed as:

$$\begin{aligned} \prod_{i \in B} K_{i,k-1} &= \alpha^{\sum_{i \in B} s_i \cdot L \cdot \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \cdot \prod_{j \neq i} (0 - x_j)} \\ &\quad \bmod n \\ &= \alpha^{f(0) \cdot L} \bmod n \\ &= \alpha^{d \cdot L} \bmod n \\ &= \widehat{S}_{k-1} \bmod n. \end{aligned}$$

The secret S_{k-1} can be derived as:

$$S_{k-1} = P_{k-1} \oplus \widehat{S}_{k-1}.$$

When each participant $u_i (i \in B)$ obtains S_{k-1}, they can use it to reconstruct $S_{k-2}, S_{k-3}, \cdots, S_0$ stage by stage (for $l = k-2, k-3, \cdots, 0$) as follows:

$$K_{i,l} = K_i^{L \cdot S_{l+1} \cdot \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \cdot \prod_{j \neq i} (0 - x_j)} \bmod n. \tag{6}$$

Then, $\widehat{S}_l$ can be computed as:

$$\begin{aligned} \prod_{i \in B} K_{i,l} &= \alpha^{\sum_{i \in B} s_i \cdot L \cdot S_{l+1} \cdot \prod_{\substack{j \in A \\ j \notin B}} (x_i - x_j) \cdot \prod_{j \neq i} (0 - x_j)} \\ &\quad \bmod n \\ &= \alpha^{f(0) \cdot L \cdot S_{l+1}} \bmod n \\ &= \alpha^{d \cdot L \cdot S_{l+1}} \bmod n \\ &= \widehat{S}_l \bmod n. \end{aligned} \tag{7}$$

The secret S_l can be derived as:

$$S_l = P_i \oplus \widehat{S}_l.$$

After reconstructing all secrets, the SD needs not redistribute a fresh share for the next secret sharing. The SD only chooses a new public value L' with $\gcd(L', \lambda(n)) = 1$. Because there are already numerous works to detect cheating and identify the cheater [3, 10, 14, 18, 22, 23, 25], we does not reiterate this issue here.

4. Discussions

Here are some discussions to show the properties and security of our multi-stage secret sharing scheme as follows:

- *Threshold feature.* According to the property of Shamir's secret sharing scheme, we know that any t out of n participants can easily reconstruct the secrets by using the Lagrange interpolating polynomial, but $t-1$ or fewer participants are not enough.
- *Determine the values of secrets.* In our scheme, we make use of the exclusive-OR operation to enable the SD to determine the values of the secrets. Then, each participant works according to the public values P_i $(i = k-1, k-2, \cdots, 0)$ to obtain the corresponding secrets S_i $(i = k-1, k-2, \cdots, 0)$.
- *Multi-stage feature.* Each participant u_i $(i \in B)$ has to reconstruct the secret S_{k-1} first and then uses it to reconstruct the next secret S_{k-2}, and so on and so forth. In other words, the reconstruction of the current secret depends on that of the previous secret. Otherwise, they cannot reconstruct the secret. The secrets are certainly reconstructed in such special order $S_{k-1}, S_{k-2}, \cdots, S_0$. To derive d from $\alpha^{d \cdot S_{l+1}}$ $(l = k-2, k-3, \cdots, 0)$ is difficult because $\alpha^{d \cdot S_{l+1}}$ is a primitive element in both $\mathbb{GF}(p)$ and $\mathbb{GF}(q)$. For the same reason, it is difficult to derive d form $\alpha^{d \cdot L}$. In addition, the parameter α is secret in the system.
- *Multi-use feature.* After reconstructing all the secrets, the secret share K_i is still unknown, and $S_i \neq \alpha^d \bmod n$. The SD needs not distribute a fresh share to each participant any more. If two secrets S_{i+1} and S_i are reconstructed, the adversary can obtain the following equations:

$$\begin{cases} \widehat{S}_i = \alpha^{d \cdot L \cdot S_{i+1}} \bmod n \\ \widehat{S}_{i-1} = \alpha^{d \cdot L \cdot S_i} \bmod n \end{cases}$$

If $\gcd(L \cdot S_{i+1}, L \cdot S_i) = 1$, the value $\alpha^d \bmod n$ can be revealed by the Euclidean algorithm. However, since the values $L \cdot S_{i+1}$ and $L \cdot S_i$ have the common factor L, $\gcd(L \cdot S_{i+1}, L \cdot S_i) \neq 1$. For the same reason, if $\gcd(S_{i+1}, S_i) = 1$, the value $\alpha^{d \cdot L} = \widehat{S}_{k-1} \bmod n$ can be revealed. However, the secret $\widehat{S}_{k-1}$ has been reconstructed before.
On the other hand, if an adversary tries to obtain K_i form Equations (5) and (6), the adversary has to face the intractability of the factorization of n. However, it is difficult to obtain $(L)^{-1} \bmod \lambda(n)$ and $(S_{l+1})^{-1} \bmod \lambda(n)$ if the factors of n are unknown.

- *Efficient.* Each participant only keeps one secret share K_i to reconstruct k secrets.

From the above discussions, the proposed scheme satisfies the requirements of the multi-stage secret sharing scheme which stated in Section 1. We have no confer to detect cheating and identify the cheater. There are already numerous works on this issue [3, 10, 14, 18, 22, 23, 25] and can easily employed in our scheme.

5. Conclusion

In this paper, we have given some modifications to Lee and Hwang's scheme to make it qualified as an ideal multi-stage secret sharing scheme, and the secret holder can arbitrarily determine the secret to conform to the requirements in practice. Further, the security of the proposed scheme is based on the factorization problem which provides higher security confidence than using the hash function in Harn's and Chang et al.'s multi-stage secret sharing schemes.

References

[1] M. Bellare, "Practice-oriented provable-security," in *Lectures on Data Security (Modern Cryptology in Theory and Practice)*, pp. 1–15, Lecture Notes in Computer Science 1561, 1999.

[2] G. R. Blakley, "Safeguarding cryptograhic keys," in *AFIPES 1797 Natl. Comput. Conf.*, vol. 48, pp. 165–172, New York, 1979.

[3] C. C. Chang and R. J. Hwang, "Efficient cheater identification method for threshold schemes," *IEE Proc. Comput. Digit. Tech.*, vol. 144, no. 1, pp. 23–27, 1996.

[4] 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.

[5] T. Y. Chang, C. C. Yang, and M. S. Hwang, "Threshold signature for group communications without shared distribution center," *Future Generation Computer Systems*, vol. 20, no. 6, pp. 1013–1021, 2004.

[6] T. Y. Chang, C. C. Yang, and M. S. Hwang, "Threshold untraceable signature for group communications," *IEE Proceedings - Communications*, vol. 151, no. 2, pp. 179–184, 2004.

[7] Ting-Yi Chang, "An computation-efficient generalized group-oriented cryptosystem," *accepted (May 23, 2009) to appear in Informatica*.

[8] Ting-Yi Chang, "A convertible multi-authenticated encryption scheme for group communications," *Information Sciences*, vol. 178, pp. 3426–3434, May 2008.

[9] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang, "A new multi-stage secret sharing scheme using one-way function," *ACM SIGOPS Operating Systems Review*, vol. 39, no. 1, pp. 45–55, 2004.

[10] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang 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.

[11] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE TRANS. FUNDAMENTALS*, vol. E83-A, pp. 2762–2765, DECEMBER 2000.

[12] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Advances in Cryptology, CRYPTO'91*, pp. 457–469, 1991.

[13] L. Harn, "Comment: Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 31, no. 4, p. 262, 1995.

[14] L. Harn and C. Lin, "Strong (n, t, n) verifiable secret sharing scheme," *Information Sciences*, vol. 180, no. 16, pp. 3059–3064, 2010.

[15] J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1994.

[16] J. He and E. Dawson, "Multisecret-sharing scheme based on one-way function," *Electronics Letters*, vol. 31, no. 2, pp. 93–95, 1995.

[17] Min-Shiang Hwang and Ting-Yi Chang, "Threshold signatures: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 3, pp. 123–137, 2005.

[18] R. J. Hwang, W. B. Lee, and C. C. Chang, "A concept of designing cheater identification methods for secret sharing," *The Journal of Systems and Software*, vol. 46, no. 1, pp. 7–11, 1999.

[19] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe, "On sharing many secrets," *Asiacrypt'94*, pp. 42–54, 1994.

[20] Narn-Yih Lee and Tzonelih 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.

[21] Jaume Martí-Farré, "A note on secret sharing schemes with three homogeneous access structure," *Information*

Processing Letters, vol. 102, no. 4, pp. 133–137, 2007.

[22] T. P. Pedersen, "Non-interactive and information-theoretic verifiable secret sharing," in *Advances in Cryptology, CRYPTO'91*, pp. 129–140, 1991.

[23] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Advances in Cryptology, CRYPTO'91*, pp. 522–526, 1991.

[24] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[25] T. C. Wu and T. S. Wu, "Cheating detection and cheater identification in secret shairng schemes," *IEE Proc. Comput. Digit. Tech.*, vol. 142, no. 5, pp. 367–369, 1995.

[26] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics And Computation*, vol. 151, no. 2, pp. 483–490, 2004.

An Improved Multi-stage Secret Sharing Scheme Based on the Factorization Problem

Ting-Yi Chang, Min-Shiang Hwang, Wei-Pang Yang

Lee and Hwang proposed a multi-stage (t, n) secret sharing scheme which has fewer public values than pervious schemes. In their scheme, a group of participants share multiple secrets stage-by-stage, and only one secret share should been kept by each participant. However, in this article, the authors will show that multiple secrets cannot in fact be reconstructed stage-by-stage by the secret holder's determination and that the secret holder cannot determine the values of the secrets in Lee and Hwang's scheme. Moreover, their scheme belongs to the family of one-time-use schemes. At the same time, we shall also modify their scheme to improve the above weaknesses and show the improved scheme can be applied. The security of the proposed scheme is based on the factorization problem which provides higher security confidence than using the hash function in Harn's and Chang et al.'s multi-stage secret sharing schemes.

Received July 2010