A New Multi-stage Secret Sharing Scheme Using One-way Function*

Ting-Yi Chang[‡] Min-Shiang Hwang[†] Wei-Pang Yang[‡]

Department of Management Information Systems[†]
National Chung Hsing University
250 Kuo Kuang Road,
402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science[‡]
National Chiao Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.
Email: wpyang@cis.nctu.edu.tw

March 9, 2004

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

[‡]Responsible for correspondence: Prof. Min-Shiang Hwang

A New Multi-stage Secret Sharing Scheme Using One-way Function

Abstract

He and Dawson proposed a multi-stage secret sharing scheme based on one-way function. In that scheme, many secrets are reconstructed stage-by-stage in the dealer's predetermined order, and only one secret shadow is kept by every participant. When all the secrets have been reconstructed, the dealer needs not redistribute fresh shadows to every participant. Later, Harn further improved the He-Dawson scheme to reduce the total number of public values. However, in this paper, we will show that both the He-Dawson scheme and Harn's scheme are one-time-use schemes and that many secrets cannot in fact be reconstructed stage-by-stage. At the same time, we shall also modify the He-Dawson scheme to improve the drawbacks above and show the improved scheme can be applied.

Keywords: Cryptography, Multi-stage, One-way function, Secret sharing, Threshold scheme.

1 Introduction

In 1979, Shamir [20] and Backely [1] firstly proposed the (t, n) threshold secret sharing schemes which are separately based on the Lagrange interpolating polynomial and linear projective geometry. In a (t, n) threshold secret sharing scheme, the trusted dealer (secret holder) delivers the distinct secret values (called shares or shadows) to n participants. At least t or more participant can pool their shares and reconstruct the secret, but only $t-1$ or fewer shares cannot. Based on those properties, secret sharing is an important part of modern cryptography [4, 5, 13] (e.g., signing corporate cheques, opening bank vaults).

According to [16], when some particular secrets have been reconstructed, if it is required that the dealer redistribute fresh shares to every participant, then the scheme is called a one-time-use scheme. On the other hand, in case that every participant only needs to keep one share, then the scheme is called a multi-use scheme. As we all know, to redistribute shares is a very punctilious and costly process. For this reason, the property of multi-use is necessary in the secret sharing schemes.

In 1994, He and Dawson [10] proposed a multi-stage secret sharing scheme to share multiple secrets based on one-way function. They used the public shift technique to obtain the true shares and the successive applications of a one-way function to make the secrets reconstructed stage-by-stage in special order. Later, Harn [7] proposed an alternative scheme which has fewer public values than the He-Dawson scheme. They claimed that their schemes belongs to multi-use schemes.

On the other hand, the dynamic multi-secret sharing scheme were proposed [2, 9, 11, 21]. In a dynamic multi-secret sharing scheme, the dealer has the ability to publish some information about what secret she/he wants to share, and then at least t participants can use the information to reconstruct the secret. Obviously, if the dealer publishes these information in a special order, the dynamic multi-secret sharing schemes can easily be extended to the multi-stage secret sharing schemes. However, the different is that the dealer should participate in the reconstruction of each secret in the dynamic multi-secret sharing schemes.

In 1995, Harn [8] proposed another threshold multi-secret sharing scheme based on the Lagrange interpolating polynomial and the digital-signature algorithm proposed by NIST [12, 14, 17]. In 2000, Chien et al. [6] proposed a multi-secret sharing scheme based on the systematic block codes; at the same time, in their paper, they proved the Harn's scheme [8] is not appropriate for general multi-secret sharing applications but also showed several of its merits: (1) It allows parallel secret reconstruction; (2) The dealer can dynamically determine the number of distributed secrets; (3) To construct the generator matrix is easy and efficient; (4) It is a multi-use scheme; and (5) The computation is efficient. Compared with some pervious schemes [7, 10, 11], Chien et al.'s scheme has fewer public values.

However, in 2003, Yang et al. [23] pointed out that Chien et al.'s scheme belongs to a different type. No matter how the secrets are reconstructed stage-by-stage in predetermined order (multi-stage secret sharing), reconstructed according to the dealer's public information (dynamic multi-secret sharing), or reconstructed simultaneously (multi-secret sharing), various secret schemes have different approaches. Yang et al. further proposed a new multi-secret scheme that has fewer public values and less storage demand as well as shorter computing time than Chien et al.'s scheme.

In this article, we shall show that the He-Dawson scheme and Harn's scheme are one-time-use schemes and that many secrets cannot be reconstructed stage-by-stage. At the same time, we shall also modify with the He-Dawson scheme to improve the weaknesses.

The remainder of this paper is organized as follows. In Section 2, we shall briefly review the He-Dawson scheme and Harn's scheme. In Section 3, we shall show both the He-Dawson scheme and Harn's scheme are one-time-use schemes, and neither can reconstruct the secrets stage-by-stage. In Section 4, we shall propose a new multi-stage secret sharing by modifying the He-Dawson scheme. In Section 5, we discuss what goals our scheme can achieve and give a example of how our new multi-stage secret sharing scheme can be applied. Finally, we shall draw our conclusions in Section 6.

2 Review of Multistage Secret Sharing Schemes

In Shamir's secret sharing scheme, the trusted dealer chooses $a_1, a_2, \cdots, a_{t-1}$ from Z_p at random and forms the polynomial $P(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1}x^{t-1}$. Let $s = P(0)$ be the secret to be shared and $x_1, x_2, \cdots, x_n$ be n distinct numbers which are publicly known to everyone. Then the dealer delivers secret shares $y_i = P(x_i)$ (for $i = 1, 2, \cdots, n$) to every participant over a secret channel. At least t participants are enough to use the Lagrange interpolating polynomial to recover the secret. With the knowledge of the set of t points (x_i, y_i), the $t-1$ degree polynomial $P(x)$ can be uniquely determined as

$$P(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j}.$$

Since $s = P(0)$, the shared secret can be expressed as

$$s = P(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}.$$

With knowing only $t-1$ or fewer shares provides no information about s whatsoever in the information-theoretic sense to an opponent over knowing no piece.

2.1 The He-Dawson Scheme

He and Dawson wanted the dealer to be able to control the secrets and make them reconstructed stage-by-stage in special order. They would like their scheme to be a multi-use scheme. Their scheme notations are defined as follows. Let $f : Z_p \rightarrow Z_p$ be any one-way function while $f^k(m)$ denotes k successive applications of f to m; i.e., $f^0(m) = m$, and $f^k(m) = f(f^{k-1}(m))$. Assume the dealer wants to share k secrets s_i (for $i = 1, 2, \cdots, k$) and at least t participants can disclose the secrets. Then, the dealer chooses n distinct integers x_i (for $i = 1, 2, \cdots, n$) as the participants' public information and performs the following steps:

1. Randomly choose $y_1, y_2, \cdots, y_n$ as the shares.

2. For $i = 1, 2, \cdots, k$ execute the following steps:

   (a) Construct a polynomial $P_i(x)$ of degree $(t-1)$ and $P_i(0) = s_i$.

   (b) Compute $Z_{ij} = P_i(x_j)$, for $j = 1, 2, \cdots, n$.

   (c) Compute $d_{ij} = Z_{ij} - f^{i-1}(y_j)$ as the shift values and $f^{i-1}(y_j)$ as the pseudo shares, for $j = 1, 2, \cdots, n$.

3. Deliver y_i to each participant secretly and publish all d_{ij}, for $i = 1, 2, \cdots, k$ and $j = 1, 2, \cdots, n$.

At least t participants provide their pseudo shares in the special order: $f^{k-1}(y_j), f^{k-2}(y_j), \cdots, f^0(y_j)$ (for $j = 1, 2, \cdots, t$), to reconstruct the polynomials $P_i(x)$ for $i = k, k-1, \cdots, 1$. Then each secret is reconstructed through the following formula (for $i = k, k-1, \cdots, 1$):

$$s_i = P_i(0) = \sum_{a=1}^{t} (f^{i-1}(y_a) + d_{ia}) \prod_{b=1, b \neq a}^{t} \frac{0 - x_b}{x_a - x_b}.$$

The secrets are reconstructed in the special order: $s_k, s_{k-1}, \cdots, s_1$.

2.2 Harn's Scheme

In order to reduce public values, Harn proposed an alternative scheme as the following steps:

1. Randomly choose $y_1, y_2, \cdots, y_n$ as the shares.

2. For $i = 1, 2, \cdots, k$ execute the following steps:

   (a) Compute $f^{i-1}(y_j)$ as the pseudo shares, for $j = 1, 2, \cdots, n$.

   (b) Reconstruct an $(n-1)$th degree Lagrange interpolation polynomial $P_i(x)$ as follows:

   $$P_i(x) = \sum_{a=1}^{n} f^{i-1}(y_a) \prod_{b=1, b \neq a}^{n} \frac{x - x_b}{x_a - x_b}.$$

   And $P_i(0) = s_i$ is the secret to be shared.

(c) Compute $(n-t)$ values as $P_i(w)$ for $w = 1, 2, \cdots, (n-t)$.

3. Deliver y_i to each participant secretly and publish all $P_i(w)$ for $i = 1, 2, \cdots, k$ and $w = 1, 2, \cdots, (n-t)$.

At least t participants provide their pseudo shares in the special order: $f^{k-1}(y_j), f^{k-1}(y_j), \cdots, f^0(y_j)$ (for $j = 1, 2, \cdots, t$), to reconstruct the secrets. Then the secrets will be reconstructed in order as they are in the He-Dawson scheme.

3 The Weakness of He-Dawson's and Harn's Schemes

In this section, we shall offer some brief descriptions as to the He-Dawson scheme and Harn's scheme, showing that they are not multi-use schemes and that the dealer cannot make the secrets reconstructed in some special order.

To reconstruct the final secret s_1, at least t participants must provide their pseudo shares $f^0(y_i)$ for $i = 1, 2, \cdots, t$. Note that $f^0(y_i) = y_i$. So, after reconstructing all the secrets, the dealer must deliver y_i to each participant over a secret channel. Thus, their schemes belongs the one-time-use schemes.

When at least t participants provide their pseudo shares but not in the special order desired: $f^{k-1}(y_j), f^{k-2}(y_j), \cdots, f^0(y_j)$ for $j = 1, 2, \cdots, t$, the secrets will not be reconstructed in that special order. For example, when someone first provides her/his pseudo share $f^1(y_1)$, the other participants can easily obtain her/his pseudo shares $f^2(y_1), f^3(y_1), \cdots, f^{k-1}(y_1)$. Then, only $(t-1)$ participants can cooperate to reconstruct the secrets $s_2, s_3, \cdots, s_{k-1}, s_k$. Thus, the dealer cannot control the order because it is decided by the t participants. In other words, their schemes suffer from the conspire attack and cannot live up the requirements in some applications.

Besides, in Harn's scheme the dealer cannot arbitrarily determine the secrets because the dealer constructs the polynomials $P_i(x)$ for $i = 1, 2, \cdots, k$

after having the points $(x_j, f^i(y_j))$ for $j = 1, 2, \cdots, n$ and $i = 0, 1, \cdots, (k-1)$. If the secrets are messages (natural language) which are used to be shared, the secrets have to be determined by the dealer.

4 The Proposed Multi-stage Secret Sharing Scheme

In order to achieve the goal of making the secrets reconstructed stage-by-stage and making the scheme a real multi-use scheme, the dealer will perform the following steps:

1. Randomly choose $y_1, y_2, \cdots, y_n$ as the shares.

2. Construct a polynomial $P_k(x)$ of degree $(t-1)$ and $P_k(0) = s_k$.

3. Compute $Z_{kj} = P_k(x_j)$ for $j = 1, 2, \cdots, n$, and then compute $d_{kj} = Z_{kj} \oplus f^k(y_j)$ for $j = 1, 2, \cdots, n$, where d_{kj} stands for the shift values and $f^k(y_j)$ the pseudo shares.

4. For $i = k-1, k-2, \cdots, 1$, execute the following steps:

   (a) Construct a polynomial $P_i(x)$ of degree $(t-1)$ and $P_i(0) = s_i$.

   (b) Compute $Z_{ij} = P_i(x_j)$ for $j = 1, 2, \cdots, n$.

   (c) Compute $d_{ij} = Z_{ij} \oplus f^i(y_j) \oplus s_{i+1}$ for $j = 1, 2, \cdots, n$, where d_{ij} stands for the shift values and $f^i(y_j)$ as the pseudo shares.

5. Deliver y_i to each participant secretly and publish all d_{ij} for $i = 1, 2, \cdots, k$ and $j = 1, 2, \cdots, n$.

In our scheme, at least t participants must first provide $f^k(y_i)$ for $i = 1, 2, \cdots, t$ to reconstruct the secret s_k through the following formula:

$$s_k = P_k(0) = \sum_{a=1}^{t} (f^k(y_a) \oplus d_{ka}) \prod_{b=1, b \neq a}^{t} \frac{0 - x_b}{x_a - x_b}. \qquad (1)$$

Then they have to provide their pseudo shares in the following special order: $f^{k-1}(y_i), f^{k-2}(y_i), \cdots, f^1(y_i)$ for $i = 1, 2, \cdots, t$, to reconstruct the secrets via the following formula (for $i = k-1, k-2, \cdots, 1$):

$$s_i = P_i(0) = \sum_{a=1}^{t} (f^i(y_a) \oplus d_{ia} \oplus s_{i+1}) \prod_{b=1, b\neq a}^{t} \frac{0 - x_b}{x_a - x_b}. \qquad (2)$$

The secrets are reconstructed in the special order: $s_{k-1}, s_{k-2}, \cdots, s_1$. Here, we have no confer to detect cheating and identify the cheater. There are already numerous works on this issue [3, 15, 18, 19, 22] and can easily employed in our scheme. On the other hand, we can also modify Harn's scheme by using the method of modifying the He-Dawson scheme to have the property of multi-use and multi-stage secret sharing scheme. However, the dealer cannot arbitrarily determine the values of secrets.

5 Discussion

In this section, we shall prove that our scheme is a real multi-use scheme and that the secrets are reconstructed stage-by-stage, and we shall also analyze the security of our scheme.

- Multi-use Scheme:

  To reconstruct the final secret s_1, at least t participants must provide their pseudo shares $f^1(y_i)$ for $i = 1, 2, \cdots, t$. Because $f^1(y_i) \neq y_i$, the shares y_i (for $i = 1, 2, \cdots, t$) still stay un-disclosed. To share the next secret, the dealer only needs to publish a new value r and uses it together with participants' shares y_i (for $i = 1, 2, \cdots, n$) to compute their k-th pseudo shares; i.e., $f^k(y_i \oplus r)$. The dealer needs not deliver y_i (for $i = 1, 2, \cdots, n$) to every participant over a secret channel, which qualifies our scheme as a multi-use scheme. On the other hand, to share k secrets in our scheme, each participant only need to keep one secret share y_i.

- Multistage Feature:

Since s_k can be solved by Equation (1), at least t participants must provide their pseudo shares $f^k(y_i)$ (for $i = 1, 2, \cdots, t$) first. If they do not have s_k first, they cannot obtain the next secret by Equation (2). For this reason, they must forward $f^k(y_i), f^{k-1}(y_i), \cdots, f^1(y_i)$ to reconstruct the secrets. So the secrets certainly need to be reconstructed in this special order: $s_k, s_{k-1}, \cdots, s_2, s_1$.

- Determine the value of secret:

  As the same Shamir's secret sharing scheme, the dealer randomly chooses the coefficients of polynomial and determine the value of secret in a constant term. For the same reason, the dealer can arbitrarily determines the values of secrets in our scheme.

Obviously, our scheme is based on the Lagrange interpolating polynomial. At least t or more participants can pool their secret shares and easily reconstruct the secret, but only $t-1$ or fewer secret shares will not be enough. Knowing only $t-1$ or fewer secret shares provides no more information about the secret to an opponent than knowing no pieces. In the following, several possible attacks will be raised and fought against to demonstrate the security of our scheme.

Attack 1: A participant U_i tries to reveal other participants' shares y_j, where $1 \leq j \leq n$ and $j \neq i$.

Analysis of Attack 1: When the last secret has been reconstructed, every participant knows others' shares $f(y_j)$ by pooling or computing $P(x_j)$. However, no one can obtain the true share y_j from $f(y_j)$ under the protection of one-way function f.

Attack 2: A participant U_i tries to reveal other participants' pseudo shares $f^k(y_j)$.

Analysis of Attack 2: The secrets are reconstructed as $s_k, s_{k-1}, \cdots, s_2, s_1$. To reconstructed the secret s_k, t participants should pool their pseudo shares $f^k(y_j)$. However, no one can via $f^k(y_j)$ to obtain the participant's other pseudo shares $f^l(y_j)$ $(l < k)$. It is protected under the one-way function f.

Attack 3: t participants try to disintegrate the order by the dealer's determination to reconstruct the secrets.
Analysis of Attack 3: From the Equation (2), to reconstruct the secret s_i, they should reconstruct the secret s_{i+1} firstly. Thus, the conspire attack cannot work in our scheme.

In the following, let's discuss in what real-life situations our multi-stage secret sharing can be used. For example, there may be a security system of bank's confidential database where one must pass thru k checkpoints before the database can be accessed. To distribute the power of a single authority and the security policy, the checkpoints must be opened and passed in sequence by at least t participants together. If the number of paritipants is less than t or the checkpoints (secrets) do not follow the proper order, it will harm the security of the system. Form the above discussions of our scheme, the secrets are reconstruct by the dealer's predetermined order. It is more practical in real-world applications.

6 Conclusions

In this article, we have presented that both the He-Dawson scheme and Harn's scheme are one-time-use schemes and that many secrets cannot be reconstructed stage-by-stage. We have also proposed an improvement of the He-Dawson scheme which is based on the public shift technique and the successive applications of a one-way function. Moreover, the sample example was presented.

References

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

[2] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro, "Fully dynamic secret sharing schemes," in *Advances in Cryptology, CRYPTO'93*, pp. 110–125, 1994.

[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] Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang, "Threshold untraceable signature for group communications," *IEE Proceedings - Communications*, accepted (July 26, 2003) and to appear.

[5] Ting-Yi Chang, Chou-Chen Yang, and Min-Shiang Hwang, "Threshold signature for group communications without shared distribution center," *Future Generation Computer Systems*, accepted (June 20, 2003) and to appear.

[6] 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.

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

[8] L. Harn, "Efficient sharing (broadcasting) of multiple secret," *Proc. IEE-Comput. Digit. Tech.*, vol. 142, pp. 237–240, May 1995.

[9] L. Harn, T. Hwang, C. Laih, and J. Lee, "Dynamic threshold scheme based on the definition of cross-product in a n-dimensional linear space," in *Advances in Cryptology, Eurocrypt'89*, pp. 286–298, 1990.

[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] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

[13] Min-Shiang Hwang, Cheng-Chi Lee, and Ting-Yi Chang, "Broadcasting cryptosystem in computer networks using geometric properties of lines," *Journal of Information Science and Engineering*, vol. 18, no. 3, pp. 373–378, 2002.

[14] Min-Shiang Hwang, Cheng-Chi Lee, and Eric Jui-Lin Lu, "Cryptanalysis of the batch verifying multiple DSA-type digital signatures," *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287–288, 2001.

[15] 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.

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

[17] National Institute of Satndards and Technology (NIST), "The digital sinature standard proposed by NIST," *Communications of the ACM*, vol. 35, no. 7, pp. 36–40, 1992.

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

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

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

[21] H. U. Sun and S. P. Shieh, "On dynamic threshold schemes," *Information Processing Letters*, vol. 52, no. 4, pp. 201–206, 1994.

[22] 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.

[23] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics And Computation*, accepted (March 31, 2003) and to appear.