A (t, n) Multi-Secret Sharing Scheme*

Chou-Chen Yang‡ Ting-Yi Chang‡ Min-Shiang Hwang†

Graduate Institute of Networking and Communication Engineering†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Department and Graduate Institute of
Computer Science and Information Engineering‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.

March 31, 2003

*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 (t, n) Multi-Secret Sharing Scheme

Abstract

In the (t, n) multi-secret sharing scheme, there are n participants in the system. At least t or more participants can easily pool their secrets shadows and reconstruct p secrets at the same time. Chien et al. used $(n+p-t+1)$ public values, $(2(n+p)-t)\times(n+p)$ storages, and solved $(n+p-t)$ simultaneous equations to share p secrets [2]. In this article, we shall propose an alternative (t, n) multi-secret sharing based on Shamir's secret sharing. We shall use $(n+p-t+1)$ or $(n+1)$ public values, $2(t-1)$ or $2(p-1)$ storages, and employ the Lagrange interpolation polynomial to share p secrets. Our scheme will have exactly the same power as the Chien et al.'s scheme.

Keywords: Cryptosystem, Digital signature, Secret sharing, Threshold scheme

1 Introduction

In 1979, the first (t, n) threshold secret sharing schemes were proposed by Shamir [12] and Blakley [1] independently. Shamir's scheme [12] is based on the Lagrange interpolating polynomial, while Blakley's scheme [1] is based on linear projective geometry. In a (t, n) threshold secret sharing scheme, at least t or more participants can pool their secret shadows and easily reconstruct the secret, but only $t-1$ or fewer secret shadows cannot. In the information-theoretic sense, the Shamir's scheme [12] is a perfect threshold scheme where knowing only $t-1$ or fewer secret shadows provides no more information about the secret to an opponent than knowing no pieces.

Later, several multi-secret sharing schemes were proposed. In a multi-secret sharing scheme, there are multiple secrets to be shared during one secret sharing process [2]. Such a scheme is useful in several kinds of applications: Sometimes it is required that several secrets be protected with the same amount of data usually needed to protect one secret, and sometimes people need to partition one large secret into l pieces with each piece protected by a smaller amount of data than is needed to protect the entire secret.

In 1994, Jakson et al. [10] classified multi-secret sharing schemes into two types: the one-time-use scheme and the multi-use scheme. In a one-time-use-scheme, when some particular secrets have been reconstructed, the secret holder must redistribute fresh shadows to every participant. On the other hand, in a multi-use scheme, every participant only needs to keep one shadow. To distribute shadows to every participant can be a very punctilious and costly process. One common drawback shared by almost all known secret-sharing schemes is that they are one-time-use schemes.

In 1994, He and Dawson [6] proposed a multistage secret sharing (MSS) to share multiple secrets based on one-way function to solve this problem. They used the public shift technique to obtain the true shadows and the successive applications of a one-way function to make the secrets reconstructed stage-by-stage in predetermined order. In their scheme, the secret holder publishes pn public values. In order to reduce the number of public values, Harn [4] proposed an alternative scheme which has a smaller number of public values than He and Dawson's scheme [6]. In Harn's scheme [4], the secret holder publishes $p(n-t)$ public values.

In 1995, He and Dawson [7] proposed a dynamic multi-secret sharing scheme based on two-variable one-way function. The two-variable one-way function is a good method to avoid disclosing the secret shadows. In a dynamic secret-sharing scheme, the secret holder has the ability to publish some information about which secret he/she wants to share. All of the above schemes [4, 6, 7] use the one-way function and the polynomials of degree $(t-1)$ (in [6, 7]) or $(n-1)$

(in [4]) to distribute secrets. Harn [5] proposed another threshold multi-secret sharing scheme which is based on the Lagrange interpolating polynomial and the DSA-type digital signatures [8, 9].

In 2000, Chien et al. [2] proposed a multi-secret scheme based on the systematic block codes. In their paper, they showed that Harn's scheme [5] is not suitable for general multi-secret sharing application. To get more information, please refer to [2] for more details. Chien et al.'s scheme [2] has several merits: (1) it allows parallel secret reconstruction; (2) the secret holder can dynamically determine the number of the distributed secrets; (3) to construct the generator matrix is easy and efficient; (4) it is a multi-use scheme; (5) the computation is efficient.

Compared with pervious schemes [4, 6, 7], Chien et al.'s scheme [2] has fewer public values. The idea that the secrets are reconstructed simultaneously is beneficial to other applications of secret sharing. Although Chien et al.'s scheme [2] has a smaller number of public values, it belongs to a different type of secret sharing scheme. In fact, various secret sharing schemes have different approaches. In some schemes, the secrets are reconstructed stage-by-stage in predetermined order; in other schemes, the secret are reconstructed according to the secret holder's public information; and in still other schemes, the secrets are reconstructed simultaneously. In this article, we will propose a multi-secret sharing scheme based on Shamir's secret sharing [12], and we will compare the performance of our scheme only with that of Chien's scheme [2]. Our scheme has the same merits as Chien et al.'s scheme [2] and has fewer public values and less storages as well as computing time.

This rest of this paper is organized as follows. In Section 2, we shall briefly review Chien et al.'s multi-secret sharing scheme. In Section 3, we shall present our (t, n) multi-secret sharing scheme and make some discussions. In Section 4, there will be a comparison between the performance of our scheme and that of Chien et. al's scheme. Finally, we shall present our conclusions in Section 5.

2 Review of Chien et al.'s Scheme

In this section, we shall briefly review Chien et al.'s scheme [2]. We explain some notations of our scheme as follows. Function $f(r,s)$ denotes any two-variable one-way function that maps a secret shadow s and a value r onto a bit string $f(r,s)$ of a fixed length. The two-variable one-way function has the following properties [2]: (1) Given r and s, it is easy to compute $f(r,s)$. (2) Given s and $f(r,s)$, it is hard to compute r. (3) Having no knowledge of s, it is hard to compute $f(r,s)$ for any r. (4) Given s, it is hard to find two different values r_1 and r_2 such that $f(r_1,s) = f(r_2,s)$. (5) Given r and $f(r,s)$, it is hard to compute s. (6) Given pairs of r_i and $f(r_i,s)$, it is hard to compute $f(r',s)$, for $r' \neq r_i$. The properties of the two-variable one-way function have been proven in [5]. On the other hand, $G(N,K)$ denotes a special type of systematic block code generator matrix $\left[\begin{smallmatrix} G(N,K)=I \\ P \end{smallmatrix}\right]$, where I is a $K \times K$ identity matrix and P is a $(N-K) \times K$ matrix $[g^{(i-1)(j-1)}]$ with g being a primitive element in $GF(2^m)$ and $K < 2^m$. I and P can be depicted as follows:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & g^1 & g^2 & \cdots & g^{K-1} \\ 1 & g^2 & g^4 & \cdots & g^{2(K-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & g^{N-K-1} & g^{(N-K-1)2} & \cdots & g^{(N-K-1)(K-1)} \end{bmatrix}$$

Here, $(P_1, P_2, \cdots, P_p)$ denotes p secrets to be shared among n participants.

Before the secret sharing, the secret holder randomly chooses n secret shadows $s_1, s_2, \cdots, s_n$ and distributes them to every participant over a secret channel. Then the secret holder performs the following steps:

1. Randomly choose an integer r and compute $f(r, s_i)$, for $i = 1, 2, \cdots, n$.

2. Construct the generator matrix $G(2(n+p)-t, n+p)$ and $n+p < 2^m$.

3. Let $D = (P_1, P_2, \cdots, P_p, f(r, s_1), f(r, s_2), \cdots, f(r, s_n))^T$ be a vector and let the superscript T mean vector transposition.

4. Compute

$$
\begin{aligned}
V &= G \times D, \\
&= \begin{bmatrix} I \\ P \end{bmatrix} \times D, \\
&= \begin{bmatrix}
1 & 0 & 0 & 0 & \cdots & 0 \\
0 & 1 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
1 & 1 & 1 & 1 & \cdots & 1 \\
1 & g^1 & g^2 & g^3 & \cdots & g^{p+n-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
1 & g^{p+n-t-1} & g^{(p+n-t-1)2} & g^{(p+n-t-1)3} & \cdots & g^{(p+n-t-1)(p+n-1)}
\end{bmatrix} \\
&\quad \times \begin{bmatrix} P_1 \\ \vdots \\ P_p \\ f(r, s_1) \\ \vdots \\ f(r, s_n) \end{bmatrix}
\end{aligned}
$$

V can be expressed as

$$V = (P_1, P_2, \cdots, P_p, f(r, s_1), f(r, s_2), \cdots, f(r, s_n), c_1, c_2, \cdots, c_{n+p-t})^T, \quad (1)$$

where

$$c_i = \sum_{j=1}^{p} g^{(i-1)(j-1)} P_j + \sum_{j=p}^{n+p} g^{(i-1)(j-1)} f(r, s_{j-p}), 1 \leq i \leq p+n-t \quad (2)$$

5. Publish $(r, c_1, c_2, \cdots, c_{n+p-t})$ in any authenticated manner such as those in [3, 11] and so on.

If at least t participants pool their pseudo shadows $f(r, s_i)$ (for $i = 1, 2, \cdots, t$), then the $(n+p-t)$ equations in Equation (2) will contain only $(n+p-t)$ unknown symbols. Therefore, the secrets $(P_1, P_2, \cdots, P_p)$ and other participants' pseudo shadows $f(r, s_i)$ (for $i = t+1, t+2, \cdots, n$) can be obtained by solving $(n+p-t)$ simultaneous equations in Equation (2). According to the properties of the two-variable one-way function, the secret holder does not need to re-distribute fresh secret shadows to every participant in the next secret sharing session. The secret holder only has to publish another random integer r. In Chien et al.'s scheme, there are only $(n+p-t+1)$ public values required.

3 Our Scheme

Our scheme notations $(f(r, s_i), (P_1, P_2, \cdots, P_p))$ are the same as those of Chien's scheme. The secret holder first randomly chooses n secret shadows $s_1, s_2, \cdots, s_n$ and distributes them to every participant over a secret channel. Then the secret holder randomly chooses an integer r and computes $f(r, s_i)$ for $i = 1, 2, \cdots, n$. The secret holder then performs the following steps differently on different conditions. If $p \leq t$, the secret holder executes the following steps:

1. Choose a prime q and construct $(t-1)$th degree polynomial $h(x)$ mod q, where $0 < P_1, P_2, \ldots, P_p, a_1, a_2, \ldots, a_{t-p} < q$ as follows:

   $$h(x) = P_1 + P_2 x^1 + \cdots + P_p x^{p-1} + a_1 x^p + a_2 x^{p+1} + \cdots + a_{t-p} x^{t-1} \bmod q.$$

2. Compute $y_i = h(f(r, s_i)) \bmod q$ for $i = 1, 2, \cdots, n$.

3. Publish $(r, y_1, y_2, \cdots, y_n)$ in any authenticated manner such as those in [3, 11] and so on. The total of the public values is $(n+1)$.

If $p > t$, the secret holder executes the following steps:

1. Choose a prime q and construct $(p-1)$th degree polynomial $h(x)$ mod q, where $0 < P_1, P_2, \ldots, P_p < q$ as follows:

   $$h(x) = P_1 + P_2 x^1 + \cdots + P_p x^{p-1} \bmod q.$$

2. Compute $y_i = h(f(r, s_i)) \bmod q$ for $i = 1, 2, \cdots, n$.

3. Compute $h(i) \bmod q$ for $i = 1, 2, \cdots, p - t$.

4. Publish $(r, h(1), h(2), \cdots, h(p - t), y_1, y_2, \cdots, y_n)$ in any authenticated manner such as those in [3, 11] and so on. The total of the public values is $(n + p - t + 1)$.

Here, we show how to reconstruct the secret in two separate cases.

Case 1: $p \leq t$

At least t participants pool their pseudo shadows $f(r, s_i)$ (for $i = 1, 2, \cdots, t$). By using the Lagrange interpolation polynomial, with the knowledge of t pairs of $(f(r, s_i), y_i)$, the $(t - 1)$ degree polynomial $h(x) \bmod q$ can be uniquely determined as follows:

$$\begin{aligned} h(x) &= \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - f(r, s_j)}{f(r, s_i) - f(r, s_j)} \bmod q \qquad (3) \\ &= P_1 + P_2 x^1 + \cdots + P_p x^{p-1} + a_1 x^p + a_2 x^{p+1} + \cdots + a_{t-p} x^{t-1} \bmod q. \end{aligned}$$

Case 2: $p > t$

In addition to at least t participants pooling their pseudo shadows $f(r, s_i)$ (for $i = 1, 2, \cdots, t$), the secret holder publishes $h(i)$ (for $i = 1, 2, \cdots, p - t$). With the knowledge of t pairs of $(f(r, s_i), y_i)$'s and $p - t$ pairs of $(i, h(i))$'s, the $(p - 1)$ degree polynomial $h(x) \bmod q$ can be uniquely determined by using the Lagrange interpolation polynomial as follows:

$$\begin{aligned} h(x) &= \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - f(r, s_j)}{f(r, s_i) - f(r, s_j)} + \sum_{i=1}^{p-t} h(i) \prod_{j=1, j\neq i}^{p-t} \frac{x - j}{i - j} \bmod q \qquad (4) \\ &= P_1 + P_2 x^1 + \cdots + P_p x^{p-1} \bmod q. \end{aligned}$$

Because our scheme is based on Shamir's secret sharing, at least t or more participants pooling their secret shadows will make it easy to reconstruct the secrets, but only $t-1$ or fewer secret shadows will not do. In the information-theoretic sense, our scheme is a perfect threshold scheme in which knowing only $t-1$ or fewer secret shadows provides no more information about the secrets to an opponent than knowing no pieces. Besides, we also use the two-variable one-way function; the secret holder need not redistribute fresh secret shadows to every participant for the next secret sharing session.

4 Performance and Storage Analysis

Chien et al.'s scheme uses the systematic block codes to give a better performance and requires a smaller number of public values than pervious schemes [4, 6, 7]. Here, we shall compare our method with Chien et al.'s scheme in terms of the number of public values, the storages, and the computing time.

When the number of the secrets is smaller than the threshold value, it is obvious that $(n+1)$ public values, which our scheme needs, is less than $(n+p-t+1)$, which Chien et al.'s scheme needs. On the other hand, we have the same the number of public values as Chien et al.'s scheme. Moreover, the secrets reconstructed in Chien et al.'s scheme cost $(n+p-t)$ simultaneous equations in Equation (2), while in our scheme, the secrets are reconstructed only by using Lagrange interpolation polynomial in Equations (3) or (4). Using the Lagrange interpolation polynomial to reconstruct polynomial is easier than solving simultaneous equations. Besides, to store an $N \times K$ matrix needs $N \times K$ storages. So, to construct the generator matrix $G(2(n+p)-t, n+p)$ in Chien et al.'s scheme needs $(2(n+p)-t) \times (n+p)$ storages. If we use *link list* to store polynomials in Equations (3) and (4), we only need $2(t-1)$ and $2(p-1)$ separately.

5 Discussions and Conclusions

It is easily to realize the multi-secret sharing by using another method which chooses a larger module q. Then, the secret holder puts the secrets $P_1, P_2, \ldots, P_p$ together with an appropriate punctuation such as $P = P_1||P_2||\cdots||P_p$ and use ordinary secret sharing scheme [12] to share the integrated secret $h(0) = P \bmod q$. However, there are some drawbacks in the above method as follows. If the secret holder wants to share p secrets and each secret is in length of 512 bits, he/she should choose a larger module q in length of $p \times 512$ bits. The computational complexity and storage of reconstructing the integrated secret P will become more than that of our proposed scheme in Section 3. On the other hand, the published values $(y_1, y_2, \ldots, y_n)$ and $(h(1), h(2), \ldots, h(p-t), y_1, y_2, \ldots, y_n)$ separately in two cases will need to more spaces. Hence, in our proposed scheme, the secret holder only needs to choose a module q in length of 512 bits to share p secrets.

In this article, we have presented a (t, n) multi-secret sharing scheme based on Shamir's secret sharing. Our scheme has the same merits as Chien et al.'s scheme has: (1) It allows parallel secret reconstruction. (2) The secret holder can dynamically determine the number of the distributed secrets. (3) It is a multi-use scheme. Furthermore, our scheme needs fewer public values and less storage as well as computing time.

References

[1] G. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 Natl. Conf.*, pp. 313–317, New York, 1979.

[2] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals*, vol. E83-A, no. 12, pp. 2762–2765, 2000.

[3] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

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

[5] L. Harn, "Efficient sharing (broadcasting) of multiple secret," *IEE Proceedings - Computers and Digital Techniques*, vol. 142, no. 3, pp. 237–240, 1995.

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

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

[8] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *to appear in IEEE Transactions on Knowledge and Data Engineering.*

[9] 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.

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

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[12] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.