Multi secret sharing scheme based on Hermitian interpolation

Tomoko Adachi
Department of Information Sciences, Toho University, 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

Keywords: Secret sharing scheme, Two keys, Hermite interpolation.

Abstract A threshold scheme, which is introduced by Shamir in 1979, is very famous as a secret sharing scheme. Dealer distribute shares of a secret value among n participants. Gathering $t(\leq n)$ participants, a secret value can be reconstructed. This is called a (t, n) secret sharing scheme. This scheme is based on Lagrange's interpolation formula. As regard interpolation formula, it is known not only Lagrange's interpolation but also Hermite interpolation. In this paper, we give a scheme of a secret sharing scheme based on Hermite interpolation, in case of two secret values.

1. Introduction

A secret sharing scheme was introduced by Shamir in 1979 [6] and Blakley in 1979 [2] independently. A secret sharing scheme has been studied by many scientists until today. Now, a secret sharing scheme has some important application to several areas of the information security. In Japan, NRI (Nomura Research Institute) Secure Technologies which is one of the private sector in the area of the information security, has provided clients with some cloud computing product named Secure Cube, from October in 2010. This cloud computing product is utilized by a secret sharing scheme, and is one good example of the application to an external storage unit.

The secret sharing scheme is a method to distribute shares of a secret value — we call it a key, too — K among a set of participants P such a way that only the qualified subsets of P are able to reconstruct the value of K from their shares. In 1979, Shamir [6] introduced the secret sharing scheme which was based Lagrange's interpolation formula. This scheme is called Shamir's threshold scheme. In 1987, Feldman [3] studied a verifiable scheme in distributing system. In 1992, Pedersen [5] applied a verifiable secret sharing scheme to Shamir's threshold scheme.

A secret sharing scheme has one key K. On the other hand, a multi-secret sharing scheme has more than one key. Dealer distribute shares of keys among n participants. Let a set of participants $P = \{P_1, P_2, \cdots, P_n\}$. Gathering $t(\leq n)$ participants, keys can be reconstructed. A multi-secret sharing scheme based on Lagrange's interpolation is studied by Yang et. al. [7] in 2004, and by Pang and Wang [4] in 2005. In 2004, we give a scheme of a (t, n) secret sharing scheme based on Hermite interpolation [1].

In this paper, especially, we give a scheme of a secret sharing scheme with two keys based on Hermite interpolation. Moreover, we compare computational complexity of our scheme and that of Yang et. al. 's scheme.

2. Lagrange's interpolation and Hermite interpolation

In this section, we describe two famous interpolation formula, that is, Lagrange's interpolation and Hermite interpolation. In numerical analysis, Lagrange's interpolation and Hermite interpolation is a method of interpolating data points as a polynomial function.

2.1 Lagrange's interpolation

Suppose that a function $f(x)$ is defined on a closed interval $[a, b]$. Given $n+1$ data points x_0, x_1, x_2, $\cdots$, x_n, $(a \leq x_i \leq b,\ x_i \neq x_j$ for $i \neq j)$, and values

$$f_k = f(x_k), \qquad k = 0, 1, 2, \cdots, n, \tag{2.1}$$

we want to find an n dimensional polynomial $P(x)$ such that $P(x)$ satisfies

$$P(x_k) = f_k, \qquad k = 0, 1, 2, \cdots, n. \tag{2.2}$$

We call $P(x)$, an n dimensional interpolation polynomial for $f(x)$. In other words, I want to get an approximation of $f(x)$, for any variable x

except $n+1$ data points x_0, x_1, x_2, $\cdots$, x_n, by calculating the value of an n dimensional polynomial $P(x)$.

Here, we can get an n dimensional polynomial $P(x)$ by the following equation.

$$P(x) = \sum_{i=0}^{n} f_i \ell_i(x) \tag{2.3}$$

where an n dimensional polynomial $\ell_i(x)$ satisfies

$$\ell_i(x_k) = \begin{cases} 1 & k=i \\ 0 & k{\neq}i,\ k=0,1,\cdots,n. \end{cases} \tag{2.4}$$

Such an n dimensional interpolation polynomial for $f(x)$ which is expressed by equation (2.3), is called an n dimensional Lagrange's interpolation formula.

An interpolation polynomial can be decided uniquely, but its express is various. For example, letting

$$\ell_i(x) = \frac{(x-x_0)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}, \tag{2.5}$$

it is clear that the n dimensional polynomial $\ell_i(x)$ satisfies equation (2.4). Hence, we can decide an unique n dimensional polynomial $P(x)$ of equation (2.3).

2.2 Hermite interpolation

Hermite interpolation is an extension of Lagrange's interpolation. When using divided differences to calculate the Hermite polynomial of a function f.

Suppose that a function $f(x)$ is defined on a closed interval $[a,b]$. Given $n+1$ data points x_0, x_1, x_2, $\cdots$, x_n, ($a \le x_i \le b$, $x_i \neq x_j$ for $i \neq j$), and values

$$f_k = f(x_k), \quad f'_k = f'(x_k), \quad k = 0,1,2,\cdots,n, \tag{2.6}$$

we want to find a $2n+1$ dimensional polynomial $P(x)$ such that $P(x)$ satisfies

$$P(x_k) = f_k, \quad P'(x_k) = f'_k, \quad k = 0,1,2,\cdots,n. \tag{2.7}$$

The problem to find such a polynomial $P(x)$ is called Hermite interpolation.

Here, it is known that we can get an unique $2n+1$ dimensional polynomial $P(x)$ by the following equation.

$$P(x)=\sum_{i=0}^{n} f_i h_i(x)+\sum_{i=0}^{n} f_i' g_i(x)$$

where two $2n+1$ dimensional polynomial $h_i(x)$, $g_i(x)$ satisfy

$$h_i(x_j)=\begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}$$

$$g_i(x_j)=0 \quad \text{for any} \quad i,j$$

and

$$h_i'(x_j)=0 \quad \text{for any} \quad i,j$$

$$g_i'(x_j)=\begin{cases}1 & i=j\\ 0 & i\neq j.\end{cases}$$

This is called Hermite interpolation.

3. A secret sharing scheme with two keys based on Lagrange's interpolation

In this section, we describe a secret sharing scheme with two keys based on Lagrange's interpolation. We refer to [7]. We refer to the part of Yang's scheme in [4], too.

In 2004, Yang et al. [7] introduced a multi-secret sharing scheme. Since our scheme is treating in the case of two keys, we describe only the case of two keys in Yang et. al.'s scheme.

(1) System parameters. Let $f(r,s)$ be a two-variable one way function. Let q be a large prime and all the numbers are element in the finite field $GF(q)$. The trusted dealer randomly selects $n(\geq 2)$ distinct integers, $s_1, s_2, \cdots, s_n$, as secret shadows of participants $P_1, P_2, \cdots, P_n$.

Here, we use K_1, K_2 to denote two keys (secret values).

(2) Secret distribution. Let t be an integer such that $t \geq 2$. The secret dealer executes the following steps:

(2a) Construct a $(t-1)$-th degree polynomial $h(x)=K_1+K_2x+a_1x^2+a_2x^3+\cdots+a_{t-2}x^{t-1}$ *mod* q, where K_1, K_2 are two keys and $a_1, a_2, \cdots, a_{t-2}$ are randomly chosen from $GF(q)$.

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

(2c) Publish $(r, y_1, y_2, \cdots, y_n)$ in any authenticated manner such as those in digital signature scheme.

(3) Secret reconstruction. At least t $(2 \leq t \leq n)$ participants pool their pseudo shadows $f(r, s_i)$. For example, t participants $P_1, P_2, \cdots, P_t$ pool their pseudo shadows $f(r, s_1)$, $f(r, s_2)$, $\cdots$, $f(r, s_t)$. By Lagrange's interpolation polynomial, with the knowledge of t pairs of $(f(r, s_i), y_i)$, the $(t-1)$-th degree polynomial $h(x)$ can be uniquely determined. From the obtained polynomial $h(x)$, we can easily get the p keys K_1, K_2.

4. Our scheme : A secret sharing scheme with two keys based on Hermite interpolation

In this section, we describe our new scheme, that is, a (t, n) secret sharing scheme with two keys based on Hermite interpolation.

In this scheme, at first, we prepare system parameters which we need. Secondly, we describe secret distribution. Finally, we describe secret reconstruction.

(1) System parameters. Let $f(r, s)$ be a two-variable one way function. Let q be a large prime and all the numbers are element in the finite field $GF(q)$. The trusted dealer randomly selects $n(\geq 2)$ distinct integers, $s_1, s_2, \cdots, s_n$, as secret shadows of participants $P_1, P_2, \cdots, P_n$. The trusted dealer randomly selects an integer r, calculates $f(r, s_1)$, $f(r, s_2)$, $\cdots$, $f(r, s_n)$.

Here, we use K_1, K_2 to denote two keys (secret values).

(2) Secret distribution. Let t be an integer such that $t \geq 2$. The secret dealer executes the following steps:

(2a) He constructs a $(t-1)$-th degree polynomial $h(x)$ $mod\ \ q$ as follows, where the two keys K_1, K_2 are elements in $GF(q)$ and $a_1, a_2, \cdots, a_{t-2}$ are randomly chosen from $GF(q)$.

$$h(x) = K_1 + K_2 x + a_1 x^2 + a_2 x^3 + \cdots + a_{t-2} x^{t-1}$$

$$mod\ \ q,$$

$$h'(x) = K_2 + 2a_1 x + 3a_2 x^2 + \cdots + (t-1) a_{t-2} x^{t-2}$$

$$mod\ \ q.$$

(2b) He computes $b_i = h(f(r, s_i))$ and $d_i = h'(f(r, s_i))$ for $i = 1, 2, \cdots, n$.

(2c) He publishes $(r, b_1, b_2, \cdots, b_n, d_1, d_2, \cdots, d_n)$ in any authenticated manner such as those in digital signature scheme.

(3) Secret reconstruction. At least t $(2 \leq t \leq n)$ participants execute the following steps:

(3a) They pool their pseudo shadows $f(r, s_i)$. For example, t participants $P_1, P_2, \cdots, P_t$ pool their pseudo shadows $f(r, s_1)$, $f(r, s_2)$, $\cdots$, $f(r, s_t)$.

(3b) They compute $\ell_i(x)$ and $d\ell_i(x)$ for $i = 1, 2, 3, \cdots, t$.

$$\ell_i(x) = \Pi_{j \neq i} \frac{x - f(r, s_j)}{f(r, s_i) - f(r, s_j)} \quad mod \;\; q$$

$$d\ell_i(x) = \sum\nolimits_{j \neq i} \frac{1}{f(r, s_i) - f(r, s_j)} \quad mod \;\; q$$

(3c) They compute $h_i(x)$ and $g_i(x)$ for $i = 1, 2, 3, \cdots, t$ by utilizing the solution of (3b).

$$h_i(x) = \ell_i(x)^2(1 - 2(x - f(r, s_i))d\ell_i(x)) \quad mod \;\; q$$

$$g_i(x) = \ell_i(x)^2(x - f(r, s_i)) \quad mod \;\; q$$

(3d) By Hermite interpolation polynomial, with the knowledge of t triplets of $(f(r, s_i), b_i, d_i)$, the $(2t-1)$-th degree polynomial $h(x)$ *mod* q can be uniquely determined as follows.

$$h(x) = \sum\nolimits_{i=1}^{t} b_i h_i(x) + \sum\nolimits_{i=1}^{t} d_i g_i(x) \quad mod \;\; q$$

From the obtained polynomial $h(x)$ *mod* q, we can easily get the p keys K_1, K_2.

As stated above, we obtain the following theorem.

Theorem 4.1 . *Suppose that we have two keys (secrets), $n(\geq 2)$ is the number of participants, and t $(2 \leq t \leq n)$ is the number of necessary participants who can reconstruct two keys (secrets). We can propose a scheme of a (t, n) secret sharing scheme with two keys based on Hermite interpolation.*

5. Computational complexity

In this section, we compare computational complexity of our scheme and that of Yang et. al. 's scheme.

As regards phase (1) system parameters, the both schemes have the same amount of parameters.

As regards phase (2) secret distribution, computational complexity of our scheme is twice of that of Yang et. al. 's scheme. Since, in our scheme, there are $d_i = h'(f(r, s_i))$ for $i = 1, 2, \cdots, n$.

As regards phase (3) secret reconstruction, computational complexity of our scheme is twice of that of Yang et. al. 's scheme. Since, in (3b) of our scheme, there are $d\ell_i(x)$ for $i = 1, 2, \cdots, n$. In (3c) of our scheme, there are not only $h_i(x)$ but also $g_i(x)$ for $i = 1, 2, \cdots, n$. In (3d) of our scheme, there are not only $\sum_{i=1}^{t} b_i h_i(x)$ but also $\sum_{i=1}^{t} d_i g_i(x)$.

Hence, computational complexity of our scheme is twice of that of Yang et. al. 's scheme. This is suitable, since computational complexity of Hermite interpolation is twice of that of Lagrange's interpolation.

5. Conclusion

We can propose a new scheme of a secret sharing scheme based on Hermite interpolation. Hermite interpolation is higher precision analysis and need more complex computation than Lagrange's interpolation. The first merit on our scheme is that we can use distributed shadows with fine distinctions. The second merit is that we can have higher security, since its computation is complex for a wiretapper. On the other hand, the demerit on our scheme is that its computation is complex for participants.

References

[1] T. Adachi and C. Okazaki : A multi-secret sharing scheme with many keys based on Hermite interpolation. *Journal of Applied Mathematics and Physics*, vol. **2**, no. **13**, (2014), pp. 1196–1201.

[2] G. R. Blakley : Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, vol. **48** (1979), pp. 313–317.

[3] Paul Feldman : A practical scheme for non-interactive verifiable secret sharing. *SFCS' 87 Proceedings of 28th IEEE Symposium on Foundations of Computer Science*, (1987), pp. 427–437.

[4] Liao-Jun Pang, Yu-Ming Wang : A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing. *Applied Mathematics and Computation.*, vol. **167**, no. **2** (2005), pp. 840–848.

[5] Torben Pryds Pedersen : Non-Interacive and information-Theoretic Secure Verifiable Secret Sharing. *Advances in Cryptology CRYPTO '91*, (1992), pp. 129–140.

[6] Adi Shamir : How to share a secret. *Communications of the ACM*, vol. **22** (1979), pp. 612–613.

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