Journal of Applied Mathematics and Physics, 2014, 2, 1196-1201
Published Online December 2014 in SciRes. http://www.scirp.org/journal/jamp
http://dx.doi.org/10.4236/jamp.2014.213140

Scientific Research

A Multi-Secret Sharing Scheme with Many Keys Based on Hermite Interpolation

Tomoko Adachi[1], Chie Okazaki[2]

[1]Department of Information Sciences, Toho University, Funabashi, Japan
[2]Kowa Electric Industry Co., Ltd., Kawasaki, Japan
Email: adachi@is.sci.toho-u.ac.jp

Received 10 November 2014; revised 1 December 2014; accepted 7 December 2014

Abstract

A secret sharing scheme is one of cryptographies. A threshold scheme, which is introduced by Shamir in 1979, is very famous as a secret sharing scheme. We can consider that this scheme is based on Lagrange's interpolation formula. A secret sharing scheme has one key. On the other hand, a multi-secret sharing scheme has more than one keys; that is, a multi-secret sharing scheme has $p(\geq 2)$ keys. Dealers distribute shares of keys among n participants. Gathering $t(\leq n)$ participants, keys can be reconstructed. In this paper, we give a scheme of a (t,n) multi-secret sharing based on Hermite interpolation, in the case of $p \leq t$.

Keywords

Secret Sharing Scheme, Multi Secret Sharing Scheme, Hermite Interpolation

1. Introduction

A secret sharing scheme is one of cryptographies. A secret sharing scheme was introduced by Shamir in 1979 [1] 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.

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 [1] introduced the secret sharing scheme which was based on 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 [4] applied a verifiable secret sharing scheme to Shamir's threshold scheme.

How to cite this paper: Adachi, T. and Okazaki, C. (2014) A Multi-Secret Sharing Scheme with Many Keys Based on Hermite Interpolation. *Journal of Applied Mathematics and Physics*, **2**, 1196-1201. http://dx.doi.org/10.4236/jamp.2014.213140

A secret sharing scheme has one key K. On the other hand, a multi-secret sharing scheme has more than one keys; that is, a multi-secret sharing scheme has $p(\geq 2)$ keys $K_1, K_2, \cdots, K_p$. Dealers 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.

Various schemes are proposed about a multi-secret sharing scheme. In 1994, Jackson *et al*. [5] studied a multi-secret sharing scheme for a matroid. A multi-secret sharing scheme by utilizing a one-way function is studied by He and Dawson [6] in 1994, and by Harn [7] in 1995. A multi-secret sharing scheme by utilizing a two variables one-way function is studied by He and Dawson [8] in 1995. A multi-secret sharing scheme by utilizing a linear block code is studied by Chien *et al*. [9] in 2000, and by Pang and Wang [10] in 2005. A multi-secret sharing scheme based on Lagrange's interpolation is studied by Yang *et al*. [11] in 2004, and by Pang and Wang [10] in 2005. Recently, Adachi [12] studies a secret sharing scheme with two keys based on Hermite interpolation.

In this paper, we give a scheme of a (t,n) multi-secret sharing based on Hermite interpolation, in the case of $p \leq t$. Here, p is the number of keys, n is the number of participants, and t is the number of gathering participants for secret reconstruction. In a (t,n) multi-secret sharing, we need to consider separately the cases where p is greater than t, equal to t, or less than t. In this paper, we give new scheme in the case of $p \leq t$. The goal of this paper is 1) to find system parameters, 2) to construct secret distribution, and 3) to complete secret reconstruction, for a multi-secret sharing, by utilizing Hermite interpolation.

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 $f_0 = f(x_0)$, $f_1 = f(x_1)$, $f_2 = f(x_2)$, $\cdots$, $f_n = f(x_n)$, we want to find an n dimensional polynomial $P(x)$ such that $P(x)$ satisfies $P(x_0) = f_0$, $P(x_1) = f_1$, $P(x_2) = f_2$, $\cdots$, $P(x_n) = f_n$. 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.

$$P(x) = \sum_{i=0}^{n} f_i k_i(x)$$

where an n dimensional polynomial $k_i(x)$ satisfies

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

Let $k_i(x) = \dfrac{(x-x_0)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}$, we can decide an unique n dimensional polynomial $P(x)$. This equation is called Lagrange's interpolation formula.

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 $x_0, x_1, x_2, \cdots, x_n$, ($a \leq x_i \leq b$, $x_i \neq x_j$ for $i \neq j$), and values $f_0 = f(x_0)$, $f_1 = f(x_1)$, $f_2 = f(x_2)$, $\cdots$,

$f_n = f(x_n)$, and their differential values $f_0' = f'(x_0)$, $f_1' = f'(x_1)$, $f_2' = f'(x_2)$, $\cdots$, $f_n' = f'(x_n)$, we want to find a $2n+1$ dimensional polynomial $P(x)$ such that $P(x)$ satisfies $P(x_0) = f_0$, $P(x_1) = f_1$, $P(x_2) = f_2$, $\cdots$, $P(x_n) = f_n$, and $P'(x_0) = f_0'$, $P'(x_1) = f_1'$, $P'(x_2) = f_2'$, $\cdots$, $P'(x_n) = f_n'$. 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 a $2n+1$ dimensional polynomial $P(x)$.

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

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

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

and

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

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

This is called Hermite interpolation.

3. A Multi-Secret Sharing Scheme Based on Lagrange's Interpolation

In this section, we describe a multi-secret sharing scheme based on Lagrange's interpolation, which is proposed by Yang *et al.* in 2004. We refer to [11]. We refer to the part of Yang's scheme in [10], too.

In Yang *et al.*'s scheme, for secret distribution, the secret are distributed in two separate cases, $p \leq t$ and $p > t$. In Yang *et al.*'s scheme, also, for secret reconstruction, the secret are reconstructed in two separate cases, $p \leq t$ and $p > t$. Since our scheme is treating in the case of $p \leq t$, we describe only the case $p \leq t$ for secret distribution and for secret reconstruction, 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 distinct integers, $s_1, s_2, \cdots, s_n$, as secret shadows of participants $P_1, P_2, \cdots, P_n$.

Here, we use $K_1, K_2, \cdots, K_p$ to denote p keys (secret values).

2) Secret distribution. In the case of $p \leq t$, the secret dealer executes the following steps:

2a) Construct a $(t-1)$-th degree polynomial $h(x) = K_1 + K_2 x + K_3 x^2 + \cdots + K_p x^{p-1} + a_1 x^p + \cdots + a_{t-p} x^{t-1} \ mod \ q$, where $K_1, K_2, \cdots, K_p$ are p keys and $a_1, a_2, \cdots, a_{t-p}$ 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. In the case of $p \leq t$, at least t participants pool their pseudo shadows $f(r, s_i)$. For example, t participants $P_1, P_2, \cdots, P_t$ pool their pseudo shadows $f(r, s_1), f(r, s_2), \cdots, f(r, s_i)$. 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 $K_1, K_2, \cdots, K_p$.

4. Our Scheme: A Multi-Secret Sharing Scheme Based on Hermite Interpolation

In this section, we describe our new scheme, that is, a multi-secret sharing scheme based on Hermite interpolation in the case $p \le t$, where p is the number of keys (secrets), and t is the number of necessary participants who can reconstruct keys (secrets).

In the case of $p = 2$, the following theorem is known.

Theorem 1. [12] *Suppose that we have two keys* (*secrets*), $n(\ge 2)$ *is the number of participants, and* t $(2 \le t \le n)$ *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.*

We expand this theorem. In our 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 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 $K_1, K_2, \cdots, K_p$ to denote p keys (secret values).

2) Secret distribution. In the case of $p \le t$, the secret dealer executes the following steps:

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

$$h(x) = K_1 + K_2 x + K_3 x^2 + \cdots + K_p x^{p-1} + a_1 x^p + \cdots + a_{t-p} x^{t-1} \quad mod \quad q$$

$$h'(x) = K_2 + 2K_3 x + 3K_4 x^2 + \cdots + (p-1)K_p x^{p-2} + p a_1 x^{p-1} + (p+1)a_2 x^p + \cdots + (t-1)a_{t-p} x^{t-2} \quad mod \quad q$$

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. In the case of $p \le t$, at least t 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 $i = 1,2,3,\cdots,t$.

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

$$d\ell_i(x) = \sum_{j \ne i} \frac{1}{f(r,s_i) - f(r,s_j)} \quad mod \quad q$$

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

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

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

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.

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

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

As stated above, we obtain the following theorem.

Theorem 2. *Suppose that* p *is the number of keys* (*secrets*), n *is the number of participants, and* $t(\le n)$ *is the number of necessary participants who can reconstruct keys (secrets). In the case* $p \le t$, *we can propose a scheme of a* (t,n) *multi-secret sharing scheme with many keys based on Hermite interpolation.*

Corollary 1. *Suppose that* n *is the number of participants, and* $t(\le n)$ *is the number of necessary participants who can reconstruct keys* (*secrets*). *Theorem* 2 *contains a scheme of a* (t,n) *secret sharing with one key based on Lagrange's interpolation, that is, Shamir's threshold scheme.*

Proof. In the case $p=1$ of Theorem 2, we obtain Corollary 1.

(Q.E.D.)

Corollary 2. *Theorem* 2 *contains Theorem* 1.

Proof. In the case $p=2$ of Theorem 2, we obtain Corollary 2.

(Q.E.D.)

5. Computational Complexity

In this section, we compare computational complexity of our scheme which we describe in Section 4, and that of Yang *et al.*'s scheme which we describe in Section 3.

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 $d_i = h'\left(f\left(r,s_i\right)\right)$ 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.

6. Conclusion

We can propose a new scheme of a multi-secret sharing scheme with many keys based on Hermite interpolation. Hermite interpolation is a higher precision analysis and needs more complex computation than Lagrange's interpolation. The merit on our scheme is that we can use many keys with fine distinctions. On the other hand, the demerit on our scheme is that its computation is complex for participants.

Acknowledgements

We thank the editor and the referee for their comments.

References

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. http://dx.doi.org/10.1145/359168.359176

[2] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. *AFIPS Conference Proceedings*, **48**, 313-317.

[3] Feldman, P. (1987) A Practical Scheme for Non-Interactive Verifiable Secret Sharing. *Proceedings of* 28*th IEEE Symposium on Foundations of Computer Science*, Los Angeles, 12-14 October 1987, 427-437.

[4] Pedersen, T.P. (1992) Non-Interacive and Information-Theoretic Secure Verifiable Secret Sharing. *Advances in Cryptology CRYPTO* '91, 129-140.

[5] Jackson, W.A., Martin, K.M. and O'Keefe, C.M. (1995) On Sharing Many Secrets. *Advances in Cryptology—ASIACRYPT*'94, **917**, 42-54.

[6] He, J. and Dawson, E. (1994) Multistage Secret Sharing Based on One-Way Function. *Electronics Letters*, **30**, 1591-1592. http://dx.doi.org/10.1049/el:19941076

[7] Harn, L. (1995) Comment: Multistage Secret Sharing Based on One-Way Function. *Electronics Letters*, **31**, 262. http://dx.doi.org/10.1049/el:19950201

[8] He, J. and Dawson, E. (1995) Multisecret Sharing Scheme Based on One-Way Function. *Electronics Letters*, **31**, 93-94. http://dx.doi.org/10.1049/el:19950073

[9] Chien, H.Y., Jan, J.K. and Tseng, Y.M. (2000) A Practical (*t*,*n*) Multi-Secret Sharing Scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E83**, 2762-2765.

[10] Pang, L.J. and Wang, Y.M. (2005) A New (*t*,*n*) Multi-Secret Sharing Scheme Based on Shamir's Secret Sharing. *Applied Mathematics and Computation*, **167**, 840-848. http://dx.doi.org/10.1016/j.amc.2004.06.120

[11] Yang, C.C., Chang, T.Y. and Hwang, M.S. (2004) A (*t*,*n*) Multi-Secret Sharing Scheme. *Applied Mathematics and Computation*, **151**, 483-490. http://dx.doi.org/10.1016/S0096-3003(03)00355-2

[12] Adachi, T. (Submitted) A Secret Sharing Scheme with Two Keys Based on Hermite Interpolation.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.