Dynamic and verifiable multi-secret sharing scheme based on Hermite interpolation and bilinear maps

Article *in* IET Information Security · October 2014

DOI: 10.1049/iet-ifs.2013.0558

Mohammad Hesam Tadayon
Iran Telecommunication Research Center

Mohammad Sayad Haghighi
University of Tehran

A New Dynamic and Verifiable Multi-Secret Sharing Scheme based on Hermite Interpolation and Bilinear Maps

Mohammad Hesam Tadayon*[1], Hadi Khanmohammadi†[2], and Mohammad Sayad Haghighi[1]

[1]Iran Telecom Research Center, Iran, [2]Tarbiat Modares University, Iran

Abstract

(t, n) threshold secret sharing is a cryptographic mechanism to divide and disseminate information among n participants in a way that at least t $(t \leqslant n)$ of them should be present for the original data to be retrieved. This has practical applications in the protection of secure information against loss, destruction and theft. In this paper, we propose a new multi-secret sharing scheme which is based on Hermite interpolation polynomials. Using the properties of discrete logarithm over elliptic curves and bilinear maps, we have created a verifiable scheme in which there is no need for a secure channel and every participant chooses his own share. This feature does not let the dealer cheat. The proposed method is dynamic to the changes in the number and value of the secrets as well as the threshold. In addition, it has the multi-use property which reduces the cost of secret distribution in multiple rounds of operation. The public values used in the proposed scheme are less than those of schemes providing similar features and the computations are also less complex. At the end of the paper, we have compared our scheme with the similar ones against a comprehensive set of key features used in secret sharing.

Index Terms: Multi-secret Sharing, Lagrange Interpolation, Hermite Interpolation, Elliptic Curve, Bilinear Map, Discrete Logarithm, Verifiable Scheme

1 Introduction

Secret sharing is an important topic in modern cryptography whose goal is to break one (or more) secret(s) into pieces called shares and distribute them among persons called participants in a way that whenever a predetermined subset of these participants pool their shares, the secret(s) can be recovered. This method of cryptography has many applications in the protection of secure information against loss, destruction and theft [1, 2]. One of the famous members of this family is (t, n) threshold secret sharing [3–9]. In this method, t or more participants who pool their shares can reconstruct the secret(s), but any subset with less than t participants cannot. In 1979 Shamir [3] and Blakley [4] proposed the first two (t, n) threshold secret sharing schemes independently. Shamir's scheme was based on interpolation polynomial and Blakley's was based on linear projective geometry. Studies have shown that both Shamir's and Blakley's schemes have some deficiencies. Among them, we can point to these: 1. Only one secret can be shared

*North Karegar St., Tehran, Iran, P.O.Box 14155-3961, Emails: tadayon@itrc.ac.ir, haghighi@itrc.ac.ir

†Jalal Ale Ahmad Highway, Tehran, Iran, P.O.Box 14115-111, Email: hadi.khanmohammadi@modares.ac.ir

at a time. 2. There is a need for secure channel to distribute the shares. 3. When participants pool their shares, they are disclosed to every participant. Therefore each share can be used only once. 4. If some of the participants cheat and do not pool the correct shares, the value of reconstructed secrets will be incorrect. Alternatively, the dealer might cheat and send one or some of the participants wrong shares. 5. If the dealer decides to change either the threshold value, the secret or the value of participants' shares, he/she must change the whole system including the shares of participants and reload it. This implies going through many computational steps and further accesses to the secure channel.

Over the years each of these problems has been addressed separately by researchers. The schemes supporting multiple secrets in each distribution are now called multi-secret schemes. Those which allow the shares to be re-used in several rounds are referred to as multi-use methods. Dynamism attribute allows the dealer to change the threshold, number or value of the secrets without having to touch the private shares of participants. And finally, verifiability feature allows revealing any fraudulent person in a scheme operation.

In this paper, we aim to introduce a new threshold multi-secret sharing scheme using properties of Hermite interpolation. We have provided multi-use feature by taking advantage of the hardship of solving the discrete logarithm problem over elliptic curves. Moreover, through the aforementioned approach we let the participants choose their shares themselves and leave no room for the dealer to cheat through manipulating the shares. In the secret reconstruction phase, the share of each participant is checked using bilinear map properties and in case of any fraudulent activity, the identity of the cheating participant is disclosed to the others. Hence, the proposed scheme is verifiable. By investigating the process of interpolation and reconstruction one can easily verify that the scheme is dynamic too. To the best of our knowledge, this work is the first one founded on the basis of Hermite interpolation polynomials and is providing the above features altogether. A table is given at the end of the paper which summarizes the attributes of the proposed scheme and compares them to those of similar schemes.

The rest of the paper is organized as follows: Section 2 reviews the related works and gives a more clear definition of features such as verifiability, multi-usability, and dynamism. In Section 3, some mathematical concepts which have been used in our scheme are given. In Section 4, the proposed scheme is presented which is followed by its security analysis in Section 5. Section 6 explains some of the features of our scheme and also compares it to the previous schemes serving similar features. An application of our scheme is presented too. Finally the conclusion given in Section 7.

2 Related Work

In 2000, Chien *et al.* [5] proposed a new (t, n) secret sharing scheme based on systematic block codes which could support multiple secrets. Participants could reconstruct m secrets when they pooled their shares together. One of the most important applications of such schemes is sharing big secrets since when the secret is very big, it can be divided into m pieces $s_1, s_2, \ldots, s_m$ and be shared by these schemes among participants. The problem with Chien *et al.*'s scheme was that it required solving simultaneous equations which was computationally complex.

In 2004, Yang *et al.* [6] proposed another (t, n) multi-secret sharing method based on Shamir's idea which could reduce the computational complexity of Chien *et al.*'s scheme. However, when the number of secrets was less than a threshold, it required publishing more public values than what Chien *et al.*'s did and therefore, was not efficient. In 2005, Pang *et al.* [7] presented a (t, n) threshold secret sharing method which was similar to Yang *et al.*'s in efficiency but required as many public values as Chien *et al.*'s did. Over the last few years, the research trend has been towards reduction of computational complexity as well as number of required public values [8].

Jackson *et al.* [10] classified multi-secret sharing schemes into two types: 1. One-time-use schemes and 2. Multi-use schemes. According to this classification, a scheme is called one-time-use if after the key (secret) recovery, the trusted dealer has to redistribute new shares to the participants. On the other hand, if the participants can construct new secrets based on the previous ones and the public values dealer has published, it will be called a multi-use scheme. Multi-use schemes are computationally efficient since the dealer does not need to send new shares to the participants after every secret reconstruction, thus, the calculations are reduced. In addition, due to the reduction of secure channel usage (to deliver the shares), the scheme's start-up cost decreases too.

In 1995, He and Dawson [11] proposed a multi-use secret sharing scheme using two variable one-way functions. In their scheme, the participants did not need to pool their private shares directly. Instead, they first had to put their secret shares in the pre-specified two-variable one-way function $f(r, s)$ and use the outputs as pseudo shares for secret reconstruction. This way, they always kept their shares private.

He and Dawson's scheme [11] was also dynamic. Dynamic property of a secret sharing scheme allows the dealer to change some of the main components such as the threshold value, the value or the number of secrets, the number of participants or the share values of some of them without having to change the shares of the others. Due to the high flexibility of these schemes, they can be started up quickly and the re-setup cost of them is very low [12, 13].

Chore *et al.* [14] were the first who built a verifiable secret sharing scheme. In verifiable methods, during the secret reconstruction phase, the combiner checks whether the shares that have been received by the participants are correct or not. Recently, a variety of multi-use verifiable methods have been proposed among which we may refer to [15] which takes advantage of RSA algorithm, [16] which uses discrete logarithm features, and also [9, 17] which use properties of elliptic curves and bilinear maps.

In 2005, Huang et al. [16] proposed a multi-secret sharing scheme utilizing discrete logarithm properties. Their proposal was inspired by Shamir's prominent work in this domain. Although it was verifiable, it lacked features such as multi-usability and required a secure channel to operate.

Tan and Wang [18] proposed a multi-use multi-secret dynamic secret sharing method based on Hermit interpolation and two-variable one-way functions in 2008. They assumed that every participant kept two private shares sent by the dealer via a secure channel. This of course left room for the dealer to cheat. Moreover, there was no way to prevent participants' cheating.

In the same year as Tan and Wang, Hadian and Mashhadi [19] presented another verifiable multi-use multi-secret sharing scheme based on Shamir's work. They employed discrete logarithm properties as well as RSA algorithm to achieve their goal.

Eslami and KabiriRad [9] proposed a dynamic verifiable secret sharing method in 2010 which was based on solving a system of linear equations. The effort in the paper was mainly to reduce the number of public values to enable the scheme to be updated quickly.

In 2011, Wang et al. [20] published another paper on verifiable multi-use multi-secret sharing methods. Similar to the above work, their approach was based on solving a set of linear equations. The number of secrets (m) was deemed be always less than the threshold (t) in their framework which limited the scheme's practicality.

In the next section, we give brief definitions for the components we have used in building up our scheme and familiarize the reader with the notations.

3 Definitions

3.1 Lagrange Interpolation Polynomial

Let (u_j, f_j) for $j = 0, \ldots, n$ be $n+1$ arbitrary pairs such that $u_i \neq u_k$ for $i \neq k$. $l_j(x)$ is defined as below [21]:

$$l_j(x) = \frac{(x-u_1)\ldots(x-u_{j-1})(x-u_{j+1})\ldots(x-u_n)}{(u_j-u_1)\ldots(u_j-u_{j-1})(u_j-u_{j+1})\ldots(u_j-u_n)}$$

where the degree of $l_j(x)$ is at most n; Then, the unique formula for Lagrange interpolation polynomial will be as follows:

$$g(x) = \sum_{j=0}^{n} f_j l_j(x) = \sum_{j=0}^{n} f_j \prod_{k=0,k\neq j}^{n} \frac{(x-u_k)}{(u_j-u_k)} \tag{1}$$

where,

$$g(u_j) = f_j; \;\; j = 0, \ldots, n.$$

The polynomial $g(x)$ found through Lagrange Interpolation is the only polynomial with a degree of maximum n whose curve passes through the points (u_j, f_j) ; $j = 0, ..., n$.

3.2 Hermite Interpolation Polynomial

Let $l(x)$ be a polynomial of degree n where $l(u_j) = 0$ for $j = 1, \ldots, n$. The Hermite interpolating polynomials of the first and second kinds are defined by [21][22]:

$$h_j^{(1)}(x) = [1 - \frac{l''(u_j)}{l'(u_j)}(x-u_j)][l_j(x)]^2,$$

and

$$h_j^{(2)}(x) = (x-u_j)[l_j(x)]^2,$$

for $j = 1, \ldots, n$. Moreover the Lagrange interpolation polynomials are defined by

$$l_j(x) = \frac{l(x)}{l'(u_j)\cdot(x-u_j)}$$

These polynomials have the following properties:

$$h_i^{(1)}(u_j) = \delta_{ij},$$
$$h_i^{(1)'}(u_j) = 0,$$
$$h_i^{(2)}(u_j) = 0,$$
$$h_i^{(2)'}(u_j) = \delta_{ij}$$

for $i, j = 1, \ldots, n$. Now let $f_1, \ldots, f_n$ and $f'_1, \ldots, f'_n$ be values. Then the expansion

$$g(x) = \sum_{j=1}^{n} f_j h_j^{(1)}(x) + \sum_{j=1}^{n} f'_j h_j^{(2)}(x) \tag{2}$$

gives the unique Hermite interpolating polynomial where

$$g(u_j) = f_j,$$
$$g'(u_j) = f'_j$$

3.3 Elliptic Curves

The elliptic curve E is defined over $GF(p)$ and is given by the equation: $y^2 = x^3 + ax + b$ where $a, b \in GF(p)$ and $\triangle = 4a^3 + 27b^2 \neq 0$. The points of E (plus the infinite point $\mathcal{O}$) together with the special operator ”+”, form a finite abelian group [23]. The elliptic curve discrete logarithm problem (ECDLP) can be summarized as follows: Given two points P and Q on $E(GF(p))$, find the integer k such that $kP = Q$ (if such a k exists). There is no polynomial time algorithm for solving ECDLP [24].

3.4 Bilinear Maps

Let G be a cyclic additive group of prime order q that is generated by P. The following problems for all $a, b, c \in Z_q^*$ are defined [25, 26]: a. Given (P, aP, bP), compute abP (Computational Diffie-Hellman Problem (CDHP)). b. Given (P, aP, bP, cP), decide whether $c = ab$ in Z_q^* (Decision Diffie-Hellman Problem (DDHP)).

If DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial time, then G is called a Gap Diffie-Hellman (GDH) group. Let G_1 be a cyclic additive group of prime order q that is generated by P, and let G_2 be a cyclic multiplicative group of the same order. Assume that the DDHP problem in G_1 and in G_2 is easy and hard, respectively and both the CDHP problem in G_1 and the discrete logarithm problem (DLP) in G_2 are hard. We say $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map if:

1. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and any $a, b \in Z_q^*$ (Bilinear property).
2. There exist $P, Q \in G_1$, such that $e(P, Q) \neq 1_{G_2}$, (non-degenerate property).
3. There is an efficient algorithm to compute $e(P, Q) \in G_2$ for all $P, Q \in G_1$ (Computable property).

4 The Proposed Scheme

In the proposed scheme, it is assumed that there are n participants and that the dealer is not one of them (i.e. he is not one of the participants). He just sets the scheme up and publishes the public values on a bulletin board. For secret reconstruction, participants will send their shares to the combiner who can even be one of the participants.

4.1 System Parameters Setup

Let p be a large prime number and also $G_1 = E(Z_p)$ be an elliptic curve with the large prime order q and P be a primitive element of it. Also, let G_2 be a multiplicative group of order q. Moreover, $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map so that the conditions of definition 3.4 are satisfied. In addition, the dealer chooses the function $h : G_1 \rightarrow Z_p^*$. The symbols $K_1, \dots, K_m$ stand for the secrets and $u_1, \dots, u_n$ are the public identities of participants which are selected from Z_p. The dealer publishes $< q, G_1, G_2, e, h, P, u_1, \dots, u_n >$ on the bulletin.

The arbitrary participant j randomly selects $s_j \in Z_q^*$ and computes $R_j = s_j P;\ \ j = 1, \dots, n$. Then keeps s_j as his/her private share and sends R_j to the dealer. If $R_i \neq R_j;\ \ i \neq j\ \ \&\ \ i, j = 1, \dots, n$, the dealer publishes them, otherwise asks those participants who have had equal shares to change their private shares.

4.2 Secret Distribution

The following steps shall be taken by the trusted dealer to distribute the secrets among the participants:

If the number of secrets is less than or equal to the number of participants ($m \leqslant n$):

1. Chooses an arbitrary $r \in Z_q^*$ and computes $R = rP$ and $R'_j = rR_j;\ j = 1, \dots, n$ then publishes R.

2. According to Eq. (2) (Hermite interpolation method), constructs the polynomial $g(x)$ of degree $n + m - 1$ over Z_p such that $g(u_j) = h(R'_j);\ j = 1, \dots, n$ and $g'(u_l) = K_l;\ l = 1, \dots, m$. The final $g(x)$ will have the following form:

$$g(x) = a_0 + a_1 x + \ldots + a_{n+m-1} x^{n+m-1} \tag{3}$$

3. Takes out the $n + m - t$ smallest integers d_i from the set $Z_p - \{u_1, \dots, u_n\}$ such that $d_i \neq d_j;\ i \neq j\ \&\ i, j = 1, \dots, n + m - t$ and publishes the tuple $(g(d_1), \dots, g(d_{n+m-t}))$.

If the number of secrets is greater than the number of participants ($m > n$):

1. Chooses an arbitrary $r \in Z_q^*$ and computes $R = rP$ and $R'_j = rR_j;\ j = 1, \dots, n$ then publishes R.

2. Since ($m > n$), he/she selects the smallest integers $u_{n+1}, \dots, u_m$ from $Z_p - \{u_1, \dots, u_n\}$ so that $u_i \neq u_j;\ i \neq j\ \&\ i, j = 1, \dots, m$.

3. According to Eq. (2), constructs the polynomial $z(x)$ of degree $n + m - 1$ over Z_p so that $z(u_l) = K_l;\ l = 1, \dots, m$ and $z'(u_j) = h(R'_j);\ j = 1, \dots, n$ and then publishes $z(0)$. The constructed polynomial will be of the following form:

$$z(x) = b_0 + b_1 x + \ldots + b_{n+m-1} x^{n+m-1} \tag{4}$$

4. Takes out the $n + m - t - 1$ smallest integers $d_i\ ;\ i = 1, ..., n + m - t - 1$ from the set $Z_p - \{u_1, \dots, u_m\}$ and publishes $(z'(d_1), \dots, z'(d_{n+m-t-1}))$.

4.3 Secret Reconstruction

Assume that at least t participants $U_1, \dots, U_t$ pool their pseudo shares R'_j to recover the m secrets; they should take the following steps:

1. Each participant U_j, using R and his/her private share s_j, computes $R'_j = s_j R$ and sends it to the combiner. The combiner puts the shares in the following equation for verification purpose:

$$e(P, R'_j) = e(R, R_j). \tag{5}$$

   If the equality holds, it goes to the next step, otherwise requests another value.

2. When $m \leq n$, with the pairs $(d_i, g(d_i));\ i = 1, \dots, n + m - t$ and also t pairs of $(u_j, h(R'_j))$ as the shares of participants, there will be $n + m$ points of $g(x)$ available and by Eq. (1), the combiner can uniquely reconstruct $g(x)$ (as in Eq. (3)) through Lagrange interpolation. $g'(u_l)$ can be computed easily afterwards and thus he/she obtains $K_l;\ l = 1, \dots, m$.

When $m > n$, using the pairs $(d_i, z'(d_i))$; $i = 1, \ldots, n+m-t-1$ and also t pairs of $(u_j, h(R'_j))$; $j = 1, \ldots, t$ as the participants shares, $n+m-1$ points of $z'(x)$ will be available and by Eq. (1), the combiner can reconstruct $z'(x)$ uniquely. By using $z(0)$ and taking the integral of $z'(x)$, he/she can obtain $z(x)$ (as in Eq (4)) and $z(u_l) = K_l$; $l = 1, \ldots, m$ will be found.

4.4 Numerical Example

Here we give a numerical example of how a secret is distributed and reconstructed in our scheme. We assume that the number of participants is five (i.e. $n = 5$), the threshold is three ($t = 3$) and the number of secrets is two ($m = 2$). The computations are done over Z_{11}, therefore, $p = 11$ and $G_1 = E(Z_{11})$. The elliptic curve parameters a and b (as in the definition 3.3), are set to 1 and 6 respectively. We have:

$$y^2 = x^3 + x + 6 \tag{6}$$

$$G_1 = \{(2,7), (5,2), (8,3), (10,2), (3,6), (7,9), (7,2), (3,5), (10,9), (8,8), (5,9), (2,4), (0,0)\} \tag{7}$$

in the above set, (2,7) is the primitive element whose order is 13. So in this example, P=(2,7) and $G_1 = E(Z_{11}) \cong Z_{13}$ which means there is isomorphism between these two sets. Now $e = G_1 \times G_1 \rightarrow G_2$ is defined according to the definition 3.4 and $h = G_1 \rightarrow Z^*_{11}$ can be given as in Table 1.

Table 1: Demonstration of h(x) function

x	(2,7)	(5,2)	(8,3)	(10,2)	(3,6)	(7,9)	(7,2)	(3,5)	(10,9)	(8,8)	(5,9)	(2,4)	(0, 0)
Meaning	P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	13P
h(x)	1	2	3	4	5	6	7	8	9	10	1	2	3

Assume that $K_1 = 0$ and $K_2 = 7$ are the two secrets and that the participants have chosen their private shares to be $s_1 = 4$, $s_2 = 2$, $s_3 = 12$, $s_4 = 6$ and $s_5 = 10$. The dealer assigns 1,...,5 to u_j ; $j = 1, ..., 5$ respectively and publishes them along with the other public values (refer to Section 4.1).

For secret sharing, assume the dealer sets $r = 1$. Then R, $R^{'}_1$,...,$R^{'}_5$ are found to be $(2,7)$, $(10,2)$, $(5,2)$, $(2,4)$, $(7,9)$ and $(8,8)$ respectively. Now, since $m \leqslant n$, the polynomial $g(x)$ will be of order 6 (which is n+m-1 as in Eq. (3)) and is given as below:

$$g(x) = 5 + 3x + 7x^5 + x^6 \tag{8}$$

Since $n + m - t = 5 + 2 - 3 = 4$, the dealer chooses d_1,...,d_4 from the set $Z_{11} - \{u_1, ..., u_5\}$ as 0, 6, 7, 8 respectively. Then he publishes $g(0) = 5$, $g(6) = 10$, $g(7) = 1$ and $g(8) = 3$.

For secret reconstruction, imagine that the participants U_1, U_2 and U_3 send their shares to the combiner. Having verified their shares through *Eq.* (5), the combiner finds seven points of the polynomial $g(x)$ as in Table 2.

Table 2: The seven points recovered from $g(x)$ polynomial

x	0	1	2	3	6	7	8
g(x)	5	5	2	2	10	1	3

Through Eq. (1), the polynomial $g(x)$ is reconstructed. Its derivation can be calculated easily then.

$$g'(x) = 3 + 35x^4 + 6x^5 \tag{9}$$

Finally, the secrets can be recovered as $g'(1) = K_1 = 0$ and $g'(2) = K_2 = 7$.

5 Security Analysis of the Proposed Scheme

In this section we analyze the security of our scheme by presenting three theorems.

Theorem 5.1. *Any sub-group of the participants with $t-1$ members (or less) cannot reconstruct the secrets.*

Proof. Suppose that $t-1$ participants send their shares (u_j, R'_j); $j = 1, \dots, t-1$. If $m \leq n$, with the $n + m - t$ points $(d_i, g(d_i))$; $i = 1, \dots, n + m - t$ published by the dealer, by definition 3.1, the combiner only needs one more point to uniquely determine the polynomial $g(x)$. So, the combiner has to choose the missing point randomly from the set $G_1 - \{0, R'_1, \dots, R'_{t-1}\}$. However, for each random choice, the constructed polynomial will be different. Therefore, the probability of achieving construction of the correct polynomial is $\frac{1}{q-t}$. By choosing a large value for q, the probability will be almost zero. One can prove the theorem for $m > n$ in a similar way.

Theorem 5.2. *The secret share s_j cannot be extracted from R_j; $j = 1, \dots, n$. Also the dealer's secret information r cannot be inferred from R.*

Proof. If someone wants to extract s_j from R_j; $j = 1, \dots, n$, he/she must solve the elliptic curve discrete logarithm problem in G_1, which is hard with our choice of G_1. Also, finding s_j via solving the equation $e(s_jP, P) = e(P, P)^{s_j}$ is hard too; because he/she has to solve discrete logarithm problem in G_2 this time. Similarly, we can prove one cannot extract r from R.

This property, along with the fact that with every reconstruction by the combiner, the dealer chooses a new value for r and updates the scheme, makes the old shares worthless and thwarts potential replay attacks.

Theorem 5.3. *Assume one of the participants (let us say the j^{th} one) sends his/her R'_j to the combiner. If Eq. (5) holds, R'_j is correct, otherwise, the participant is dishonest.*

Proof. by using bilinear map properties we have:

$$\begin{aligned} e(P, R'_j) &= e(P, s_jR) \\ &= e(P, s_jrP) \\ &= e(P, P)^{s_jr} \\ &= e(rP, s_jP) \\ &= e(R, R_j) \end{aligned}$$

If the j^{th} participant sends the true value R'_j, the above equation will hold. If someone cheats and does not send the correct value, his/her identity can be revealed to others.

6 Critical Comparison of Schemes

In this section we describe the features of our scheme and compare them with those of some similar distinguished schemes. We will summarize all the comparative information in a table at the end. The works referred to in this section have been briefly described in Section 2 before.

Huang et al.'s [16] proposal was a verifiable multi-secret sharing scheme utilizing discrete logarithm properties. However, it lacked features such as multi-usability and also required a rather high number of private shares (three for each participant). A secure channel was also required and verifiability feature came at the cost of excessive number of public values.

Tan and Wang 's [18] scheme was a multi-use multi-secret dynamic secret sharing method based on Hermit interpolation and two-variable one-way functions. In their proposal, every participant had to keep two private shares sent by the dealer via a secure channel. This of course left room for the dealer to cheat. Moreover, there was no way to prevent participants' cheating. The polynomial interpolated by the dealer was of degree $n+m+t-1$ which is larger than ours by t units. This results in a surplus in computations during secret distribution and re-construction.

Hadian and Mashhadi's [19] work came out as another verifiable multi-use multi-secret sharing scheme. They employed the discrete logarithm properties as well as RSA algorithm mainly for verification purpose. Compared to the previous two, a substantial improvement can be seen, however, the number of public values used is far more than what is proposed in the paper at hand. We denote this difference in the number of public values with Δ. When $m \leqslant t$ (i.e when the number of secrets is less than the threshold), there will be $2n+1$ public values in Hadian and Mashhadi's scheme. We may write:

$$\Delta = (2n+1) - (n+m-t+1) = n-m+t \xrightarrow{m \leqslant t\ ,\ n>1} \Delta > 0 \tag{10}$$

When $m \geqslant t$, the mentioned scheme requires $2n+m$ public values. In a comparison with ours, we can write the difference as:

$$\Delta = (2n+m) - (n+m-t+1) = n+t-1 \xrightarrow{t \geqslant 1\ ,\ n>1} \Delta > 0 \tag{11}$$

It is clear that with the increase in the number of participants or the threshold, the difference gets larger.

Wang et al.'s [20] scheme was a verifiable multi-use multi-secret sharing method. According to [9], it needs more than $n+m-t+1$ public values i.e. it uses more public values than the proposed scheme. Furthermore, the number of secrets (m) must be less than the threshold (t) in Wang et al.'s framework, otherwise, the scheme should be run multiple times. The scheme proposed in this paper requires only one run in either cases.

To the best of our knowledge, our proposal is the only one taking advantage of Hermite interpolation polynomials and is providing a comprehensive set of features at low costs. It is both multi-use and verifiable. It does not require a secure channel and participants choose their shares themselves. The number of public values is merely $n+m-t+1$ which is the lowest amongst similar multi-secret sharing schemes. Table 3 summarizes the above discussions and gives the reader a detailed feature-oriented view of the approaches.

Secret sharing schemes have many applications among which we may refer to electronic voting (e-voting). Although e-voting does not solely rely on secret sharing, it is usually one of the key building blocks. For example, Chen et al.'s e-voting scheme [27] combines the RSA blind signature scheme and secret sharing cryptosystem, to provide a fair and practical election. Eligibility (only eligible voters can vote), efficiency (the computations can be done in a reasonable time), robustness (the voters cannot stop or interfere with the election), mobility (voting can be done from any place at anytime) and practicability (no especial equipment or skill should be required for voting) are some of the important indices e-voting schemes are evaluated with. Our secret sharing scheme can be well embedded into e-voting schemes due to its rich features. Since it is verifiable, the participants’ shares are checked for integrity and correctness before secret reconstruction by the combiner. Hence, voters’ eligibility can be verified and because of this feature, no voter can stop or tamper with the election either. This gives the scheme designer the robustness feature as well. Multi-usability, low number of public values and the encryption methods employed, altogether, have made our secret sharing scheme computationally low-complex. This makes the e-voting system built upon our secret sharing scheme more efficient. Moreover, since our scheme is of low complexity and does not require a secure channel, e-voting can be done over the Internet and with regular devices available to the public. Therefore, it makes the e-voting system practicable too.

7 Conclusion

In this paper, we proposed a new (t, n) verifiable multi-secret sharing scheme based on Hermite and Lagrange interpolations. It uses discrete logarithm properties over elliptic curves as well as bilinear maps. In this scheme, since the participants choose their shares themselves, the dealer cannot cheat. It is also dynamic to the changes in the number and value of the secrets as well as the threshold i.e. the number of secrets, their values or the threshold can be changed without needing to touch participants’ private shares. Moreover, key features such as multi-usability have been embedded into the proposed scheme.

References

[1] Fouque, PA., Poupard G., Stern J.: ’Sharing decryption in the context of voting or lotteries’, Financial Cryptography (LNCS), 2001, 1962, (1), pp. 90-104

[2] Brickell, EF., Daveport, DM.: ’On the classification of ideal secret sharing scheme’, Journal of Cryptology, 1991, 4, (2), 123-134

[3] Shamir, A.: ’How to share a secret’, Communications of the ACM, 1979 , 22, (11), 612-613

[4] Blakley, GR.: ’Safeguarding cryptographic keys’, Proc. AFIPS National Computer Conference, 1979, pp. 313-317

[5] Chien, HY., Jan, JK., Tseng, YM.: ’A practical multi-secret sharing scheme’, IEICE Transactions on Fundamentals of Electronics, 2000, E83-A, (12), pp. 2762-2765

[6] Yang, CC., Chang, TY., Hwang, MS.: ’A (t, n) multi-secret sharing scheme’, Applied Mathematics and Computation, 2004, 151, (2), pp. 483-490

[7] Pang, LJ., Wang, YM.: ’A new (t,n) multi-secret sharing scheme based on shamir’s secret sharing’, Applied Mathematics and Computation, 2005, 167, (2), pp. 840-848

[8] Zhou, Y., Wang, F., Luo, S., et al.: ’A secret sharing scheme based on Near-MDS codes’, Proc. IEEE International Conference on Network Infrastructure and Digital Content, China, 2009, pp. 833-836

[9] Eslami, Z., Kabiri-Rad, S.: ’A new verifiable multi-secret sharing scheme based on bilinear maps’, Wireless Personal Communication, 2012, 63, (2), pp. 459-467

[10] Jackson, WA., Martin, KM., O'Keefe, CM.: 'On sharing many secrets', Proc. Advances in Cryptology (ASIACRYPT'94), 1995, pp. 42-54

[11] He, J., Dawson, E.: 'Multisecret-sharing scheme based on one-way function', Electronics Letters, 1995, 31, (2), pp. 93-95

[12] Wei, C., Xiang, L., Yuebin, B., Xiaopeng, G.: 'A new dynamic threshold secret sharing scheme from bilinear maps', Proc. Int. Conference on Parallel Processing Workshops, China, 2007, pp. 19-22

[13] Qu, J., Zou, L., Zhang, J.: 'A practical dynamic multi-secret sharing scheme', Proc. IEEE Int. Conference on Information Theory and Information Security, China, 2011, pp. 629-631

[14] Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: 'Verifiable secret sharing and achieving simultaneity in the presence of faults', Proc. 26th Annual Symposium on Foundations of Computer Science, USA, 1985, pp. 383-395

[15] Zhao, J., Zhang, J., Zhao, R.: 'A practical verifiable multi-secret sharing scheme', Computer Standards and Interfaces, 2007, 29, (1), 138-141

[16] Huang, MJ., Zhang, JZ., Xie, SC.: 'A secure and efficient (t, n) threshold verifiable multi-secret sharing scheme', Proc. Computational Intelligence and Security, Springer, 2005, pp 532-537

[17] Hua, S., Aimin, W.: 'A multi-secret sharing scheme with general access structures base on elliptic curve', Proc. 3rd Int. Conf. on Advanced Computer Theory and Engineering, 2010, pp. 629-632

[18] Tan, XQ., Wang, ZQ: 'A new (t, n) multi-secret sharing scheme', Proc. Int. Conference on Computer and Electrical Engineering, Thailand, 2008, pp. 861-865

[19] Dehkordi, MH., Mashhadi, S.: 'An efficient threshold verifiable multi-secret sharing', Computer Standards and Interfaces, 2008, 30, (3), pp. 187-190

[20] Wang, SJ., Tsai, YR., Shen, CC.: 'Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ECC', Wireless Personal Communications, , 2011, 56, (1), pp. 173-182

[21] Szego, G.: 'Orthogonal Polynomials' (AMS Bookstore; 1992)

[22] Hildebrand, F.B.,: 'Introduction to numerical analysis' (Courier Dover Publications, 2nd edn. 1987)

[23] Koblitz, N.: 'Introduction to elliptic curves and modular forms' (Springer-Verlag, 1993)

[24] Hankerson, D., Menezes, AJ., Vanstone, S.: 'Guide to elliptic curve cryptography' (Springer, 2004)

[25] Washington, LC.,: 'Elliptic curves: Number theory and cryptography' (CRC Press, 2nd edn. 2008)

[26] Lee, HS.,: 'Self-pairing map and its applications to cryptography', Applied Mathematics and Computation, 2004, 151, (3), pp. 671-678

[27] Chen, Y., Jan, J., Chen, C.,: 'The design of a secure anonymous Internet voting system', Computers and Security, 2004, 4, (23), pp. 330-337

Table 3: Feature comparison of multi-secret sharing schemes

Feature	Huang et al.'s [16]	Tan and Wang's [18]	Hadian and Mashhadi's [19]	Wang et al.'s [20]	The Proposed Scheme
Multi-usability	No	Yes	Yes	Yes	Yes
Verifiability	Yes	No	Yes	Yes	Yes
Dynamism	Yes	Yes	Yes	Yes	Yes
Polynomial Degree	t	$n+m+t-1$	$\begin{cases} t & m \leqslant t \\ m & m > t \end{cases}$	NA[a]	$n+m-1$
Public Values to be Refreshed/Round	$n+4m+t$	$n+m-t+1$	$\begin{cases} 2n+1 & m \leqslant t \\ 2n+m-1 & m > t \end{cases}$	$\begin{cases} n+1 & m \leqslant t \\ \left[\frac{m}{t}\right] n+1 & m > t \end{cases}$	$n+m-t+1$
Private Shares	3	2	1	1	1
Participants Freedom to Choose Their Own Shares	No	No	Yes	Yes	Yes
Secure Channel Requirement	Yes	Yes	No	No	No
Encryption Algorithm Used in Verifiability	DL[b]	Linear OWF[b]	DL & RSA	DL over EC[b] & BM[b]	DL over EC & BM

[a] This scheme uses a set of linear equations instead of polynomials. The secrets are retrieved by solving the linear equations system.

[b] DL (Discrete Logarithm), OWF (One-Way Function), EC (Elliptic Curve), BM (Bilinear Map)