Metadata of the chapter that will be visualized in SpringerLink

Book Title	Emerging Technology Trends in Internet of Things and Computing	
Series Title		
Chapter Title	A New Secret Sharing Scheme Based on Hermite Interpolation and Folded Magic Cube Rules	
Copyright Year	2022	
Copyright HolderName	Springer Nature Switzerland AG	
Author	Family Name	**Abdulaziz**
	Particle	
	Given Name	**Rafid**
	Prefix	
	Suffix	
	Role	
	Division	College of Education for Pure Sciences
	Organization	University of Anbar
	Address	Anbar, Iraq
	Email	Rafid.alhashimy@uoanbar.edu.iq
	ORCID	http://orcid.org/0000-0002-4783-0349
Author	Family Name	**Sagheer**
	Particle	
	Given Name	**Ali**
	Prefix	
	Suffix	
	Role	
	Division	Al-Qalam University College
	Organization	Dean of Al-Qalam University College
	Address	Kirkuk, Iraq
	Email	dean@alqalam.edu.iq
	ORCID	http://orcid.org/0000-0003-2589-5317
Corresponding Author	Family Name	**Dawood**
	Particle	
	Given Name	**Omar**
	Prefix	
	Suffix	
	Role	
	Division	College of Computer Science & IT
	Organization	University of Anbar
	Address	Ramadi, 31001, Iraq
	Email	omar-Abdulrahman@uoanbar.edu.iq
	ORCID	http://orcid.org/0000-0003-3276-602X

Abstract

In this paper, a modern secret sharing scheme has been proposed that deal with set of variables points along specific polynomial. The main idea is to establish the dimension of magic cube into a secret point at

a Lagrange polynomial equation. The secret value can be reconstructed from set of cooperated dealers or participants according to predefined threshold. The core idea is how to reconstruct a full magic cube of six dimensions across single key solution. The proposed method adopted Hermite mathematical comprehension that allows minimum number of participants with k-points under definition of a polynomial with degree $k - 1$ to reconstruct the secret properly. The proposed scheme supposed each dealer has his own share and any group of shareholders at the decided threshold together they can recover the secret. The proposed idea gave a good implementation and fast secret recovery with new mathematical orientation.

Keywords (separated by '-') Shamir's secret sharing - Magic square - Magic cube - Hermite interpolation - Lagrange

A New Secret Sharing Scheme Based on Hermite Interpolation and Folded Magic Cube Rules

Rafid Abdulaziz[1], Ali Sagheer[2], and Omar Dawood[3](✉)

[1] College of Education for Pure Sciences, University of Anbar, Anbar, Iraq
Rafid.alhashimy@uoanbar.edu.iq
[2] Al-Qalam University College, Dean of Al-Qalam University College, Kirkuk, Iraq
dean@alqalam.edu.iq
[3] College of Computer Science & IT, University of Anbar, Ramadi 31001, Iraq
omar-Abdulrahman@uoanbar.edu.iq

Abstract. In this paper, a modern secret sharing scheme has been proposed that deal with set of variables points along specific polynomial. The main idea is to establish the dimension of magic cube into a secret point at a Lagrange polynomial equation. The secret value can be reconstructed from set of cooperated dealers or participants according to predefined threshold. The core idea is how to reconstruct a full magic cube of six dimensions across single key solution. The proposed method adopted Hermite mathematical comprehension that allows minimum number of participants with k-points under definition of a polynomial with degree $k - 1$ to reconstruct the secret properly. The proposed scheme supposed each dealer has his own share and any group of shareholders at the decided threshold together they can recover the secret. The proposed idea gave a good implementation and fast secret recovery with new mathematical orientation.

Keywords: Shamir's secret sharing · Magic square · Magic cube · Hermite interpolation · Lagrange

1 Introduction

Secrets sharing is an important cryptographic principle to people ever since humans started to interact with each other. There are a lot of information which we do not want other people to know, while there is other information which we could not risk landing in the wrong hands. One example perhaps would be our ATM passwords [1]. In modern cryptography, the security of data is fully dependent on the security of the keys used. As most of the ciphers are public knowledge, one can easily encrypt and decrypt any message if they know the key involved. For some highly confidential data, it's not always good to have a single person in control of the key and to secure the data. This has led to the need for Secret Sharing Schemes, which allow keys to be distributed among a group of people, with a pre-specified number of them needing to input their share in order, to access the key [2].

In 1979 Shamir [3] and Blakley [4] introduced the concept of secret sharing through threshold schemes. Their models were based on polynomials and finite geometries.

P. Liatsis et al. (Eds.): TIOTC 2021, CCIS 1548, pp. 1–13, 2022.
https://doi.org/10.1007/978-3-030-97255-4_26

Since 1979 many researchers have taken the basic concept of a threshold scheme and used other mathematical structures to adapt threshold schemes to meet the needs of many practical situations [5]. Secret sharing plays an important role in protecting important information from getting lost, destroyed, or into wrong hands. A secret can be shared among n participants. At least t or more participants can reconstruct the secret, but (t -1) or fewer participants can obtain nothing about the secret. To share another secret, the secret dealer must redistribute every participant s secret shadow [6, 7]. 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. One of the famous members of this family is (t, n) threshold secret sharing. In this method, t or more participants who pool their shares can reconstruct the secret(s) [8].

2 Related Works

Muthukumar, K. A., & Nandhini, M in [9], have introduced the performance of two algorithms viz., secret sharing algorithm and information dispersal algorithm that are compared and modified secret sharing algorithm and which is proposed for medical data sharing. Phenomenon of secure medical data sharing in cloud environment is discussed with two algorithms Secret sharing algorithm and information dispersal algorithm and their concerns are analyzed with different complexities. This modified secret sharing algorithm is proposed to overcome the issues faced by the existing algorithms. Through this algorithm, medical data can be shared in secured way according to the data requested by the client. The existing drawbacks are overcome in this proposed one and it can be used for dynamic database without affecting the users. It is very well suited for sharing high sensitive data in multi cloud environment. Also Further work is recommended to improve the system performance and increase the flexibility of system.

Lan, Y., Wu, C., & Zhang, Y. in [10], have proposed a secret sharing-based key management (SSKM). SSKM utilizes the advantages of hierarchical architecture and adopt two-level key mechanism, which can efficiently enhance and protect the all over network security and survivability. Different from previous works, the SSKM distributes keys based on secret sharing mechanism by the clustered architecture, which not only localizes the key things but also keeps scalability. The SSKM provides various session keys, the network key for base station (BS) and cluster heads (CHs); the cluster key between the cluster head and member nodes. The SSKM dynamically generates different keys based on different polynomials from BS in different periods which can protect the network from the compromised nodes and reduce the high probability of the common keys. The SSKM can prevent several attacks effectively and reduce the energy consumption. The Salient advantage of this work is addressed challenging security issues by localizing key things based on secret sharing theory. This paper presents the network key and cluster key and generate new keys from various polynomials by Lagrange interpolation formula. Meanwhile, SSKM has an authentication mechanism to ensure the scalability, which can not only authenticate the new sensor but also can isolate the compromised node.

Diaconu, A. V., & Loukhaoukha, K. in [11], have proposed a newly designed image cryptosystem that uses the Rubik's cube principle in conjunction with a digital chaotic cipher. Thus, the original image is shuffled on Rubik's cube principle (due to its proven confusion properties), and then XOR operator is applied to rows and columns of the scrambled image using a chaos-based cipher (due to its proven diffusion properties). This work develops novel permutation—substitution image encryption architecture, based on Rubik's cube principle and digital chaotic cipher. The proposed encryption system includes two major parts, chaotic pixels substitution (in order to achieve desired diffusion factor) and Rubik's cube, principle based, pixels permutation (in order to achieve desired confusion factor). Different keys were used for shuffling and ciphering procedures, and while a tent map was used to generate image's ciphering matrices, each row's and column's intrinsic properties were used to compute the number of their circular shifts. Comprehensive experimental tests have been carried out, and numerical analyses have shown robustness of the proposed algorithm against several cryptanalytic attacks. Likewise, the performance assessment tests attest that the proposed image encryption scheme is fast and highly secure. Although a much smaller key space is used, but still large enough to face against exhaustive attack, with a smaller key size, the proposed encryption scheme presents better results, compared to those of previously proposed ones.

Feng, X., Tian, X., & Xia, S. in [12], have introduced a novel image encryption algorithm based on the discrete fractional Fourier transform and an improved magic cube rotation scrambling algorithm. Through fractional Fourier transform and position scrambling, the proposed algorithm can achieve double image encryption in the time-frequency domain. Compared the encrypted images and decrypted images, the proposed image encryption algorithm has better performance than only using fractional Fourier transform.

3 Hermite Interpolation Method

Hermite interpolation is an extension of Lagrange's interpolation. When using divided differences to calculate the Hermite polynomial of a function f [13, 14].

To suppose that a function f(x) is defined on a closed interval [a, b]. given n + 1 data points $x_0, x_1, x_2, \ldots, x_n$, ($a \leq x\_i \leq b, x\_i \neq x\_j \; for \; i \neq j$), and values.

$$F_k = f(x_k), f'_k = f'(x_k), k = 0, 1, 2, \ldots, n$$

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

$$P(x_k) = f_k, p'(x_k) = f'k, k = 0, 1, 2, \ldots, n$$

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

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

$$\mathrm{P(x)} = \sum_i^n f_i \, h_i(x) + \sum_i^n f'_i \, g_i(x)$$

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

$$h_i(x_j) = \begin{cases} 1 \; i = j \\ 0 \; i \neq j \end{cases}$$
$$g_i(x_j) = 0 \text{ for any } \quad \text{I, j}$$
$$\text{And}$$
$$h_i'(x_j) = 0 \text{ for any } \quad \text{I, j}$$
$$g_i'(x_j) = \begin{cases} 1 \; i = j \\ 0 \; i \neq j \end{cases}$$

This is called Hermite interpolation.

4 Magic Square and Magic Cube Rules

Magic squares have been studied for at least three thousand years, the earliest recorded appearance dating to about 2200 B.C., in china. In the 19th century, Arab astrologers used them in calculating horoscopes, and by 1300 A.D. magic square had spread to the west. An engraving by the German artist embedded the date, 1514, in the form of two consecutive numbers in the bottom row, because the concept of a magic square is so easily understood, magic squares have been particularly attractive to puzzles and an amateur mathematicians [15].

An n × n magic square is a permutation of n2 distinct numbers, 1, 2, 3,⋯, n^2 (each number is used once), in a square matrix, where the sums of the numbers in each row, each column, and the forward and backward main diagonals are equal. This sum is normally called the magic constant. According to whether size n is an even or odd number, a magic square can be called an even order or odd order one. Further, the even order magic squares can be classified into doubly even order and singly even order ones depending on whether or not n can be divided by 4 [16].

The magic constant (MC), magic vector or magic number, these terms are synonyms that can be calculated by the derivative formula (1).

$$\text{MC} = \frac{n^2(n^2+1)}{2} \tag{1}$$

Thus, 3 * 3 normal magic square must have its rows, columns and diagonals adding to MC = 15, MC = $3(3^2 + 1)/2 = 15$, 4 * 4 to MC = 34, 5 * 5 to MC = 65 and 8 * 8 to MC = 260, and so on. The Magic Sum (MS) is another significant term that includes the summation to all the numbers by (rows, columns and diagonals) in a magic square uses the following formula (2).

$$\text{MS} = \frac{n^2(n^2+1)}{2} \tag{2}$$

The MS for 3 * 3 = 45, MS for 4 * 4 = 136, MS for 5 * 5 = 325, MS for 8 * 8 = 2080 and so on, other method for calculating MS is by multiplying the MC by dimension of the magic square [17].

The following Fig. 1 below is a simple example of a magic square of order 3 with 9 values arranged consecutively in the magical order. So, suppose MC is the number that each row, column and diagonal must be add up to a vector numbers, and (P) is a pivot element for the numbers through which the magic square is determined and constructed. The pivot element in the magic square represents the center element in the middle square as it explained and mentioned with shaded central number, and through which can be determined some properties of the magic square.

8	1	6
3	5	7
4	9	2

Fig. 1. Magic square of order 3

The pivot element at any magic square of odd order with sequential numbers can be calculated with the following formula:

$$P = \frac{(n^2 + 1)}{2}$$

For example: the following two examples include pivot computing in magic square of order three and order five.

$$P = \frac{(n^2 + 1)}{2} = \frac{(3^2 + 1)}{2} = 5$$
$$P = \frac{(n^2 + 1)}{2} = \frac{(5^2 + 1)}{2} = 13$$

And so on Here, is another formula to determine the pivot element in non-sequential odd order numbers that might begin with indeterminate integer number, or have a period, in another word that have difference between the numbers greater than one. As stated below in Eq. (3). Where N = square order, A = starting number and D = difference number that represents the difference between the successive and the previous numbers. The Fig. 2 below states three of different examples a, b and c respectively that explains the whole notation [18].

$$P = \frac{(2 * A + D(n^2 - 1))}{2} \tag{3}$$

$$P = \frac{(2 * 54 + 3(3^2 - 1))}{2} = 66$$
$$P = \frac{(2 * 17 + 5(3^2 - 1))}{2} = 37$$
$$P = \frac{(2 * 3 + 2(3^2 - 1))}{2} = 11$$

75	54	69
60	66	72
63	78	57

(a) N=3, A=54, D=3

52	17	42
27	37	47
32	57	22

(b) N=3, A=17, D=5

17	3	13
7	11	15
9	19	5

(c) N=3, A=3, D=2

Fig. 2. Three magic square of order three with constant difference

A magic cube of order n is a 3-dimensional n * n * n matrix (cubical table)

$$Q_n = [q(i, j, k); 1 \leq i, j, k \leq n]$$

Containing the natural numbers 1, 2, 3,…, n3 in some order, and such that.

$$\sum_{x=1}^{n} q(x, j, k) = \sum_{x=1}^{n} q(i, x, k) = \sum_{x=1}^{n} q(i, j, x) = \frac{n\left(n^3 + 1\right)}{2} \text{ For all } i, j, k = 1,$$

(Note that in a magic cube we make no requirement about the sums of elements on any diagonal). The triple of numbers (i; j; k) called the coordinates of the element q(i; j; k) (Fig. 3).

AQ1

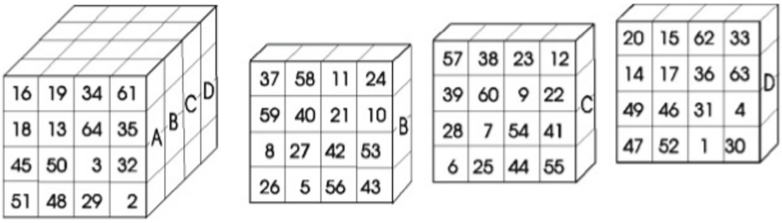

Fig. 3. Magic cube

A magic square of order 1 is a magic cube of order 1. Just as a magic square of order 2 does not exist a magic cube of order 2 does not exist either [19]. The basic feature of magic cube is that the sum of all numbers in each layers, each column, each row and main space diagonal is equal to single number, this number is called as magic constant of a cube, denoted by M3(n).

AQ2

$$M_3(n) = \frac{n\left(n^2 + 1\right)}{2}$$

According to the theorem stated by M. Trenkler, magic cube can be constructed from the combination of magic square and two orthogonal Latin squares [20].

5 The Proposed Secret Sharing Method

The main objective behind the adopted magic cube idea is to transfer the magic cube properties from the dealer to a group of trusted subscribers. The pivot element of one

of the six magic squares is selected from the magic cube and sent within a polynomial (secret) to the participants. In addition to sending another selected element (The element of G) to the subscribers through which will be obtained the characteristics of the magic cube and then reconstructed the original magic cube again. The following steps describe the main notations for the mixing of magic cube with secret sharing using Hermite interpolation.

- **First Step:** Build a magic cube of odd order from six magical squares, and the magic cube numbers start from a dedicated number with a specific difference value between the numbers.
- **Second Step:** The pivot element is selected from the first magic square of the Magic Cube to use it as a secret value in the polynomial to compute the main points (x_i, y_i) and its derivatives $(y\prime_i)$ and send them to the participants.

$$F(x) = (pivot) + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \ \text{mod} \ prime \tag{4}$$

$$F(x) = a_1 + 2 \cdot a_2 \mathrm{x} + \ldots + \mathrm{k} \cdot a_k \cdot x^{k-1} \ \text{mod} \ prime \tag{5}$$

- **Third Step:** Magic cube properties are sent to subscribers to be rebuilt again according to the some parameters likewise (Start value, Difference value, Pivot element and the cube order).
- **Forth Step:** The new selected element (G) is chosen under special conditions after the magic cube is built by the dealer. This element must be smaller than the pivot element (Pivot $>$ G) and greater than the cube's dimensions ($G > N$).
- **Fifth Step:** When the Modular operation is taken between the pivot element and the numbers smaller than it. We will choose the output that will equal the dimensions (N) of the magic cube (Pivot Mod $G = N$) accordingly. Also the product of dividing the (G) element on the dimensions of the magic cube will represent the difference (D) value according to (G Divide N = Difference).
- **Sixth Step:** After sending the points and (G) number to the participants. The Hermite interpolation is used to reconstruct the secret again to obtain the pivot element (secret).

$$H_{2n+1}(x) = \sum_{j=0}^{n} f\left(x_j\right) H_{n,j}(x) + \sum_{j=0}^{n} f'\left(x_j\right) \hat{H}_{n,j}(x) \tag{6}$$

Where

$$H_{n,j}(x) = \left[1 - 2\left(x - x_j\right) \hat{L}_{n,j}\left(x_j\right)\right] L_{n,j}^2(x) \tag{7}$$

And

$$\hat{H}_{n,j}(x) = \left(x - x_j\right) L_{n,j}^2(x). \tag{8}$$

- **Seventh Step:** After obtaining the pivot element, it will calculate the (Pivot Mod G) to get the Dimensions (N) of the Magic cube, and (G Divide N) to obtain the difference (D) between the Magic cube numbers.

– **Eighth Step:** After obtaining (Pivot, Dimensions and Difference) of the magic cube, it is easy to obtain the starting number (A) of the Magic cube by the equation regarding the Eq. (10) below:

$$\text{Pivot} = \frac{(2 * A) + D * \left(N^2 - 1\right)}{2} \tag{9}$$

$$\text{Start Number} = \frac{(\text{Pivot} * 2) - D * \left(N^2 - 1\right)}{2} \tag{10}$$

Example:
Assume that a folded magic cube of odd order (5 * 5) consisting of six magic squares, starting by the number 5 and with a constant difference between the sequential numbers is 3 as shown in Fig. 4.

53	74	5	26	47
71	17	23	44	50
14	20	41	62	68
32	38	59	65	11
35	56	77	8	29

1st Square

128	149	80	101	122
146	92	98	119	125
89	95	116	137	143
107	113	134	140	86
110	131	152	83	104

2nd Square

203	224	155	176	197
221	167	173	194	200
164	170	191	212	218
182	188	209	215	161
185	206	227	158	179

3rd Square

278	299	230	251	272
296	242	248	269	275
239	245	266	287	293
257	263	284	290	236
260	281	302	233	254

4th Square

353	374	305	326	347
371	317	323	344	350
314	320	341	362	368
332	338	359	365	311
335	356	377	308	329

5th Square

428	449	380	401	422
446	392	398	419	425
389	395	416	437	443
407	413	434	440	386
410	431	452	383	404

6th Square

Dimension = 5, Difference = 3, Start = 5

Fig. 4. The magic cube

The Pivot element (41) of the first magic square is selected in the magic cube to be the secret within a polynomial. After that select the other coefficients randomly within the polynomial to produce (y_i) as stated in Eq. (11), additionally, compute the derivative of polynomial to deduce the ($y\prime_i$) as stated in Eq. (12). The magic cube properties are represented in the Hermite interpolation with the following important parameters:

Where $n =$ participants, $k =$ threshold, $D =$ difference.

$$n = 6, k = 3, p = 53, p > s \text{ and } p > n$$

$$F(x) = (pivot) + a_1 x + a_2 x^2 + \ldots + a_k x^k \quad mod\ prime$$
$$F(x) = 41 + 9x + 11x^2 \quad mod\ 53 \tag{11}$$

And

$$f'(x) = a_1 + 2 \cdot a_2 x + \ldots.. + K \cdot a_k x^{k-1} \quad mod\ prime$$

$$f'(x) = 9 + 22x \quad mod \quad 53 \tag{12}$$

As a result; six points (x_i, y_i) and $(y\prime_i)$ of the polynomial are calculated and sent to six trusted subscribers (n) by the dealer as explained in Table 1.

Table 1. $(X, f(x))$ and the derivative $(f^{'}(x))$

(x)	$f(x)$	$f^{'}(x)$	Points $(x, f(x))$, $(f^{'}(x))$
1	8	31	(1, 8), (31)
2	50	0	(2, 50), (0)
3	8	22	(3, 8), (22)
4	41	44	(4, 41), (44)
5	43	13	(5, 43), (13)
6	14	35	(6, 14), (35)

Compute a suitable (G) number that fits to the pivot element and the dimensions (D) of the cube to be $(G = 18)$. Pivot $> G$, $G >$ Dimension (N).

$$41 \ > \ 18 \ > \ 5$$

Distribute the generated six points to six subscribers accompanied by the element (G). The selection of any three points $(k = 3)$ to reconstruct the secret (Pivot) will be verified:

For Example: $D_0 = (1, 8, 31), \quad D_1 = (2, 50, 0), \quad D_2 = (3, 8, 22)$.

Compute the Hermite interpolation:

First compute the Lagrange polynomials and their derivatives:

$$L_{2,0}(x) = \frac{x - x_1}{x_0 - x_1} * \frac{x - x_2}{x_0 - x_2} = \frac{1}{2}x^2 - \frac{5}{2}x + 3, \quad L'_{2,0}(x) = x - \frac{5}{2} = -1.5$$

And

$$L_{2,1}(x) = \frac{x - x_0}{x_1 - x_0} * \frac{x - x_2}{x_1 - x_2} = -x^2 + 4x - 3, \quad L'_{2,1}(x) = -2x + 4 = 0$$

$$L_{2,2}(x) = \frac{x - x_0}{x_2 - x_0} * \frac{x - x_1}{x_2 - x_1} = \frac{1}{2}x^2 - \frac{3}{2}x + 1, \quad L'_{2,2}(x) = x - \frac{3}{2} = 1.5$$

The polynomials $\mathrm{H}_{2,\,\mathrm{j}}$ and $\widehat{\mathrm{H}}_{2,\,\mathrm{j}}$ are then:

$$H_{n,j}(x) = [1 - 2(x - x_j)\hat{L}_{n,j}(x_j)]L^2_{n,j}(x)$$

$$H_{2,0}(x) = [1 - 2(x - 1)(-1.5)]\left(\frac{1}{2}x^2 - \frac{5}{2}x + 3\right)^2 = -18$$

$$H_{2,1}(x) = [1 - 2(x-2)(0)]\left(-x^2 + 4x - 3\right)^2 = 9$$

And

$$H_{2,2}(x) = [1 - 2(x-3)(1.5)]\left(\frac{1}{2}x^2 - \frac{3}{2}x + 1\right)^2 = 10$$

$$\hat{H}_{n,j}(x) = \left(x - x_j\right)L_{n,j}^2(x)$$

$$\widehat{H}_{2,0}(x) = (x-1)\left(\frac{1}{2}x^2 - \frac{5}{2}x + 3\right)^2 = -9$$

$$\widehat{H}_{2,1}(x) = (x-2)\left(-x^2 + 4x - 3\right)^2 = -18$$

And

$$\widehat{H}_{2,2}(x) = (x-3)\left(\frac{1}{2}x^2 - \frac{3}{2}x + 1\right)^2 = -3$$

Finally,

$$H_5(x) = (-18 * 8) + (9 * 50) + (10 * 8) + (-9 * 31) + (-18 * 0) + (-3 * 22) = 41$$

Therefore,

$$H_{2n+1}(x) = \sum_{j=0}^{n} f\left(x_j\right)H_{n,j}(x) + \sum_{j=0}^{n} f'\left(x_j\right)\hat{H}_{n,j}(x)$$

$$\mathrm{F(x)} = 41 + 9x + 11x^2$$

After obtaining the Pivot element and (G) elements, it is possible to deduce the dimensions (D) of the original Magic Cube:

$$\begin{aligned} \text{Pivot Mod G} &= \text{N} \\ 41 \,\%\, 18 &= 5. \end{aligned} \tag{13}$$

By the same steps deduce the difference (D) between the numbers of the original Magic Cube according to the Eq. (14):

$$\begin{aligned} G/N &= D \\ 18/5 &= 3 \end{aligned} \tag{14}$$

After gotten the following parameters (Pivot, Difference and Dimension), the starting number (A) can be obtained by:

$$\text{Start Number} = \frac{(\text{Pivot} * 2) - D * \left(N^2 - 1\right)}{2}$$

$$\text{Start Number} = \frac{(41 * 2) - 3 * \left(5^2 - 1\right)}{2} = 5$$

Finally, the six participants will have the ability to rebuild the original magic cube again as shown in Fig. 5 below (Table 2):

53	74	5	26	47
71	17	23	44	50
14	20	41	62	68
32	38	59	65	11
35	56	77	8	29

1st Square

128	149	80	101	122
146	92	98	119	125
89	95	116	137	143
107	113	134	140	86
110	131	152	83	104

2nd Square

203	224	155	176	197
221	167	173	194	200
164	170	191	212	218
182	188	209	215	161
185	206	227	158	179

3rd Square

278	299	230	251	272
296	242	248	269	275
239	245	266	287	293
257	263	284	290	236
260	281	302	233	254

4th Square

353	374	305	326	347
371	317	323	344	350
314	320	341	362	368
332	338	359	365	311
335	356	377	308	329

5th Square

428	449	380	401	422
446	392	398	419	425
389	395	416	437	443
407	413	434	440	386
410	431	452	383	404

6th Square

Fig. 5. The reconstructed original magic cube

Table 2. The proposed algorithm

1) Initialization of Algorithm
a- Choose a magic cube with six magic squares of odd order
2) Constructing Magic Cube (odd order)
a- The magic cube starts with a Start Number (A)
b- Choose the dimensions of the cube (N) and the amount of the difference between the cube numbers (D)
3) Encryption Process
a- Choose the Pivot element of the first magic square in the magic cube to be (secret) within the polynomial $f(x) =$ pivot $+ a_1x + a_2x^2$ *mod prime*, compute the polynomial derivative $f'(x) = a_1 + 2.a_2x$ *mod prime*
b- Conclusion Six points of (x_i, y_i) and (y'_i)
c- Send points and its derivatives to six trusted subscribers
d- Determine the Threshold value
4) Generating (G) element
a- Chose the element (G) with conditions (Pivot $>$ G $>$ N)
b- The selected G number should satisfy the condition of (Pivot Mod $G = N$) and (G Divide $N = D$)
c- Send the (G) number to subscribers publicly
5) Decryption Process
a- Reconstruct the secret again by a specified number of subscribers (Threshold) to get the Pivot element via Hermite Interpolation
b- Pivot Mod $G = N$

(*continued*)

Table 2. (*continued*)

c- $D = G$ Divide N where the resultant integer is taken and the remainder value is ignored
d- After acquiring the properties of the magic cube (Pivot, D and N), the starting number (A) of the magic cube can be obtained through:
Start Number $(A) = \frac{(\text{Pivot} * 2) - D * (N^2 - 1)}{2}$
6) Reconstructing Magic Cube
a- Reconstructed the original magic cube through the characteristics obtained by the participants

6 Conclusion

A secret sharing scheme has been addressed where no single share can reveal any information without cooperation with other shareholders. In case one or more participant was fake then the secret cannot be reconstructed. The present method depended basically on folded magic cube with Hermite mathematical formula. The main reason for the folded magic cube is to exploit the magic cube characteristics in embedding the secret value. The dimension cube acts the main value that distributed among the shareholders across the Hermite interpolation. Hermite polynomial represents a new direction method toward the new variant of Lagrange equations that distribute the secret efficiently. The proposed method produced a good implementation and an efficient secret reconstruction for the secret value.

References

1. Tieng, D.G., Nocon, E.: Some attacks on Shami's secret sharing scheme by inside adversaries (2016)
2. Narani, S.: Social secret sharing for resource management in cloud. arXiv preprint arXiv: 1302.1185 (2013)
3. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
4. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, vol. 48, no. 313 (1979)
5. Dawson, E., Donovan, D.: The breadth of Shamir's secret-sharing scheme. Comput. Secur. **13**(1), 69–78 (1994)
6. Pang, L.J., Wang, Y.M.: A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing. Appl. Math. Comput. **167**(2), 840–848 (2005)
7. Peng, K.: Investigation and survey of secret sharing in verifiable distributed systems. In: 2011 12th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 342–347. IEEE (2011)
8. Tadayon, M.H., Khanmohammadi, H., Haghighi, M.S.: Dynamic and verifiable multi-secret sharing scheme based on Hermite interpolation and bilinear maps. IET Inf. Secur. **9**(4), 234–239 (2014)
9. Muthukumar, K.A., Nandhini, M.: Modified secret sharing algorithm for secured medical data sharing in cloud environment. In: 2016 2nd International Conference on Science Technology Engineering and Management, ICONSTEM 2016, pp. 67–71 (2016)

10. Lan, Y., Wu, C., Zhang, Y.: A secret-sharing-based key management in wireless sensor network. In: Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, pp. 676–679 (2013)
11. Diaconu, A.V., Loukhaoukha, K.: An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. Math. Prob. Eng. (2013)
12. Feng, X., Tian, X., Xia, S.: A novel image encryption algorithm based on fractional Fourier transform and magic cube rotation (5), 1008–1011 (2011)
13. Tomoko Adachi. (2015). Multi secret sharing scheme based on Hermitian interpolation (New contact points of algebraic systems, logics, languages, and computer sciences).
14. Adachi, T., Okazaki, C.: A multi-secret sharing scheme with many keys based on Hermite interpolation. J. Appl. Math. Phys. **2**(13), 1196 (2014)
15. Al-Najjar, S.A., Nuha, A.R., AAl-Heety, F.: Computation of odd magic square using a new approach with some properties. Eng. Technol. J. **30**(7), 1203–1210 (2012)
16. Duan, Z., Liu, J., Li, J., Tian, C.: Improved even order magic square construction algorithms and their applications in multi-user shared electronic accounts. Theoret. Comput. Sci. **607**, 391–410 (2015)
17. Heinz, H.D., Hendricks, J.R.: Magic squares lexicon: illustrated, published by HDH as demand indicates. 15450 92A Avenue, Surrey, BC, V3R 9B1, Canada, hdheinz@ istar. ca [ISBN 0-9687985-0-0]. John R. Hendricks, 308, p. 151 (2000)
18. Dawood, O.A., Rahma, A.M.S., Hossen, A.M.J.A.: Generalized method for constructing magic cube by folded magic squares. Int. J. Intell. Syst. Appl. **8**(1), 1 (2016)
19. Trenkler, M.: Magic cubes. Math. Gaz. **82**(493), 56–61 (1998)
20. Rajavel, D., Shantharajah, S.P.: Cubical key generation and encryption algorithm based on hybrid cube's rotation. In: International Conference on Pattern Recognition, Informatics and Medical Engineering (2012)

Author Queries

Chapter 26

Query Refs.	Details Required	Author's response
AQ1	Please check and confirm if the inserted citations of Fig. 3 and Table 2 are correct. If not, please suggest an alternate citations.	
AQ2	To maintain sequential order, figures, equations and their citations have been renumbered. Please check and correct if necessary.	