Scientific Research Publishing

American Journal of Computational Mathematics, 2019, 9, 207-220
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

Bipartite Threshold Multi-Secret Sharing Scheme Based on Hypersphere

Bin Li

Department of Mathematics, Chengdu Normal University, Chengdu, China
Email: 1145398209@qq.com

How to cite this paper: Li, B. (2019) Bipartite Threshold Multi-Secret Sharing Scheme Based on Hypersphere. *American Journal of Computational Mathematics*, **9**, 207-220.
https://doi.org/10.4236/ajcm.2019.94016

Received: April 23, 2018
Accepted: October 25, 2019
Published: October 28, 2019

Abstract

To address the problem that existing bipartite secret sharing scheme is short of dynamic characteristic, and to solve the problem that each participant can only use secret share once, this paper proposed a bipartite (n_1+n_2, m_1+m_2) -threshold multi-secret sharing scheme which combined cryptography and hypersphere geometry. In this scheme, we introduced a bivariate function and a coordinate function over finite field Z_p to calculate the derived points of secret share, which can reconstruct the shared secrets by producing the intersection point of hypernormal plane and normal line on the hypertangent plane. At the initial stage the secret dealer distributes to each participant a secret share that can be kept secret based on the intractability of discrete logarithm problem and need not be changed with updating the shared secrets. Each cooperative participant only needs to submit a derived point calculated from the secret share without exposing this secret share during the process of reconstructing the shared secret. Analyses indicate that the proposed scheme is not only sound and secure because of hypersphere geometric properties and the difficulty of discrete logarithm problem, but also efficient because of its well dynamic behavior and the invariant secret share. Therefore, this bipartite threshold multi-secret sharing scheme is easy to implement and is applicable in practical settings.

Keywords

Bipartite Threshold, Multi-Secret Sharing, Hypersphere, Hypernormal Plane, Hypertangent Plane

1. Introduction

Secret sharing plays a significant role in information security. It has become one of the most important research areas in modern cryptography and has wide ap-

plications in many fields. Its theories models are rapidly developed. A secret sharing scheme allows a secret dealer to split a secret into secret shares and to distribute the secret shares among a group of participants in the way that only if a certain specified subset of the participants pooling together their shares can reconstruct the shared secret, while any unqualified subsets cannot obtain anything about the shared secret. Particularly, a (t,n)-threshold secret sharing scheme allows the secret to being shared by a secret dealer among n participants in such a way that any t or more participants gathering their secret shares together can recover the shared secrets, but $t-1$ or fewer participants cannot obtain any knowledge about the shared secret. Two basic (t,n)-threshold secret sharing schemes based on Lagrange interpolating and affine geometry were proposed by Shamir [1] and Blakley [2] for the first time respectively in 1979. Since then, many constructions have been proposed [3] [4] [5] [6] [7]. They usually consist of two basic protocols, one is a distribution protocol in which the secret S is distributed by the secret dealer to participants, another is a reconstruction protocol in which the secret S is recovered by pooling the secret shares of a qualified subset of the participants.

In the original (t,n)-threshold secret sharing schemes, if there are r secrets to be shared among the same n participants, the secret dealer should run the (t,n)-threshold secret sharing scheme for r times. It results in a low efficiency. To solve the problem, Blundo *et al.* [8] introduced the concept of multi-secret sharing schemes according to the situation where the same set of shared control members shares more than one secret in 1993. This is an alternative way to improve the efficiency of secret sharing scheme, named multi-secret sharing scheme (MSS), which use same shares to reconstruct multiple shared secrets. There are various proposals of MSS scheme. For instance, MSS schemes proposed by [9] [10] are based on polynomials, and MSS scheme proposed by [11] is based on elliptic curve of bilinear map, and MSS scheme proposed by [12] is based on cellular automata, and so on.

These secret sharing schemes are all based on an assumption that all participants are equal in status, right and dependability. However, the assumption is very hard to satisfy in fact. In many cases, participants have different access right. Padro *et al.* [13] researched secret sharing schemes with bipartite access structure. Bipartite access structure, informally, is that the set of participants can be divided into two parts in such a way which all participants in the same part play an equivalent role in the structure. Papers [14] [15] gave $\left(n_1+n_2, m_1+m_2\right)$-threshold secret sharing schemes with two kinds of different access rights which based on the solution structures of constant coefficients homogeneous linear difference equation and noncyclic polynomial sequence respectively. Further, people can consider in any access structure the partition that is derived from a suitable equivalence relation on the set of participants. Because of its practical interest, secret sharing for multipartite access structures has been studied by several authors [16] [17] [18].

In all of the above-mentioned schemes, there is a drawback that some partici-

pants might have left the group and adversary might have corrupted more than n_1-1 (or n_2-1) participants. The security policy and adversary structure of a secret sharing scheme may change after the setup of the scheme and before the recovery of the shared secret. So it is desirable to design a bipartite threshold secret sharing scheme which allows the value n_1 or n_2 of threshold and number m_1 or m_2 of participants to change before the recovery of the secret, and which remains secure under these changes.

In this paper, we use the hypertangent plane and the hypernormal plane on the hypersphere to construct a (n_1+n_2, m_1+m_2)-threshold multi-secret sharing scheme. This threshold scheme is ideal which not only the participants can join or leave the system dynamically but also the value of threshold is easy to change as well as multi-secret could be shared and renewed. In addition, the participants need not provide their real secret shares and the secret shares need not to be renewed when the shared secret is changed.

Organization of this paper is as follows. We introduce related notions and results in Section 2. In Section 3, we propose our construction by using geometric method. Section 4 details our validity analysis, security analysis and performance analysis respectively. We draw the conclusion in Section 5.

2. Definitions and Preliminaries

In this section we review some basic definitions and notations that will be used through the paper.

Definition 1. Let A, B be two groups of participants with difference access right such that $A\cap B=\phi$, $|A|=m_1$, $|B|=m_2$. Set $n_1, n_2 \in Z^*$ satisfying $m_i \geq \max\{|n_1-n_2|+1, n_i\}$, $i=1,2$. Each participant in A obtains a secret share $k_i\,(1\leq i\leq m_1)$ respectively and each participant in B obtains a secret share $\overline{k}_j\,(1\leq j\leq m_2)$ respectively. The shared secret S can be restored only if at least n_1 participants in group A and n_2 participants in group B combine their secret shares. Then this method is called bipartite (n_1+n_2, m_1+m_2)-threshold secret sharing scheme, where the number n_1, n_2 are called the value of threshold.

In this paper, Let $A=\{P_1, P_2, \cdots, P_{m_1}\}$, $B=\{\overline{P}_1, \overline{P}_2, \cdots, \overline{P}_{m_2}\}$, where $P_i\,(1\leq i\leq m_1)$, $\overline{P}_j\,(1\leq j\leq m_2)$ are some participants. Let D be the secret dealer who distributes the secret shares among the participants, NB be an electronic proclamation board on which the secret dealer can write information but others cannot. All operations in this paper are carried out over finite field Z_p, where p is a large prime satisfying $p\equiv 3 \bmod 4$. The following theorem is proposed in [19].

Theorem 1. Let p be an odd prime. If 2 is not quadratic residue module-p, then arbitrary $N^2\in[0, p)$ can be expressed to sum of squares for arbitrany n+1 integer module-p.

Let $[O; x_1, x_2, \cdots, x_{n+1}]$ be n+1 dimension Cartesian orthogonal coordinate system in real Euclidean space R^{n+1}.

Definition 2. Assume that $Q(a_1, a_2, \cdots, a_{n+1})$ is a point of R^{n+1}, $N\in Z_p$,

and let N denote the radius of hypersphere Σ. Then the spherical representation of hypersphere Σ is defined as follows:

$$\sum_{i=1}^{n+1}\left(x_i-a_i\right)^2=N^2, \tag{1}$$

where $\left(x_1,x_2,\cdots,x_{n+1}\right)$ is the coordinate of arbitrary point on hypersphere Σ. $Q\left(a_1,a_2,\cdots,a_{n+1}\right)$ is called the centre of hypersphere.

Definition 3. For $(a,b)\subset R$, *a R*-continuously differentiable curve Γ from (*a*,*b*) to R^{n+1} is defined as vector function in [20] by

$$\boldsymbol{r}=\boldsymbol{r}(t)=\left(x_1(t),x_2(t),\cdots,x_{n+1}(t)\right), \tag{2}$$

where $t\in(a,b)$.

The derived vector of curve Γ

$$\boldsymbol{r}'(t)=\frac{\mathrm{d}\boldsymbol{r}(t)}{\mathrm{d}t}=\left(\frac{\mathrm{d}x_1(t)}{\mathrm{d}t},\frac{\mathrm{d}x_2(t)}{\mathrm{d}t},\cdots,\frac{\mathrm{d}x_{n+1}(t)}{\mathrm{d}t}\right) \tag{3}$$

is called the tangent vector at point t of curve Γ.

If for all $t\in(a,b)$, we have $\boldsymbol{r}'(t)\neq\boldsymbol{0}$, then Γ is called the regular curve.

If for all $t\in(a,b)$, the coordinates of regular curve Γ satisfy

$$\sum_{i=1}^{n+1}\left(x_i(t)-a_i\right)^2=N^2,$$

Then curve Γ is called the spherical curve of hypersphere $\sum$.

To deal with multi-secret sharing problem, for $Z_p\subset(a,b)$, we pick a transform between Z_p^t and Z_p^{n+1} as follows:

$$\delta:\left(z_1,z_2,\cdots,z_t\right)\leftrightarrow\left(x_1,x_2,\cdots,x_{n+1}\right)$$

such that

$$\begin{cases}x_1=x_1\left(z_1,z_2,\cdots,z_t\right),\\ x_2=x_2\left(z_1,z_2,\cdots,z_t\right),\\ \quad\vdots\\ x_{n+1}=x_{n+1}\left(z_1,z_2,\cdots,z_t\right).\end{cases} \tag{4}$$

In addition, let g be a primitive root of module-p, we define a bivariate function over Z_p,

$$F(u,v)=g^{u+v}, \tag{5}$$

and a coordinate function over Z_p,

$$y_{ij}=y_{i1}^j\left(i=0,1,2,\cdots;j=1,2,\cdots,n+1\right). \tag{6}$$

3. Proposed Scheme

In this section, we propose a bipartite multi-secret sharing scheme based on hypersphere. In our scheme, a secret dealer is responsible for generating m_1+m_2 different secret share from the shared secrets $S_1,S_2,\cdots,S_t$. And then, only given n_1+n_2 secret share, the shared secrets can be reconstructed.

3.1. The Distribution of the Secret Shares

The secret dealer randomly selects m_1 different secret share $k_i\left(1\le i\le m_1\right)$ and number u_1 from Z_p, then distributes k_i and u_1 to each participant P_i in group A through a secret channel as the secret share of these participants respectively. Similarly, m_2 different secret shares $\bar{k}_j\left(1\le j\le m_2\right)$ and number u_2 from Z_p such that $u_1\ne u_2$ are selected by D to distribute to participants in group B through same secret channel.

Taking $n=\max\left\{n_1,n_2\right\}$, without loss of generality, suppose that $n_1\ge n_2$, then $n=n_1$. We assume that t shared secrets $s_1,s_2,\cdots,s_t$ are all from Z_p where $1\le t\le n$. By setting $\left(z_1,z_2,\cdots,z_t\right)=\left(s_1,s_2,\cdots,s_t\right)$ in (4), the secret dealer calculates

$$\begin{cases} x_1\left(s_1,s_2,\cdots,s_t\right)=a_1, \\ x_2\left(s_1,s_2,\cdots,s_t\right)=a_2, \\ \quad\vdots \\ x_{n+1}\left(s_1,s_2,\cdots,s_t\right)=a_{n+1}, \end{cases} \tag{7}$$

which yields a point $Q\left(a_1,a_2,\cdots,a_{n+1}\right)\in Z_p^{n+1}$.

The secret dealer chooses a positive integer $N\in Z_p^*$ to get a spherical representation of a hypersphere

$$\sum_{i=1}^{n+1}\left(x_i-a_i\right)^2=N^2,$$

where $Q\left(a_1,a_2,\cdots,a_{n+1}\right)$ is the centre of this hypersphere.

The secret dealer chooses $k_0\in Z_p$ such that $k_0\ne k_i\left(1\le i\le m_1\right)$ and a bivariate function like (5), together with the coordinate function (6) to calculate over Z_p as follows:

$$y_{01}=F\left(u_1,k_0\right)=g^{u_1+k_0},$$
$$y_{0j}=y_{01}^j,\ j=1,2,\cdots,n.$$

$y_{0,n+1}\in Z_p$ follows from the spherical representation, that is, $y_{0,n+1}\in Z_p$ satisfies

$$\sum_{i=1}^{n+1}\left(y_{0i}-a_i\right)^2=N^2,$$

which yields a point on Σ,

$$U_0\left(y_{01},y_{02},\cdots,y_{0,n+1}\right).$$

It is not difficult to get a hypertangent plane π of Σ at U_0:

$$\sum_{i=1}^{n+1}\left(y_{0i}-a_i\right)\left(x_i-y_{0i}\right)=0.$$

Letting $\xi_i=y_{0i}-a_i, M=\sum_{i=1}^{n+1}y_{0i}\left(y_{0i}-a_i\right)$, one obtains a following equation of hypertangent plane π:

$$\sum_{i=1}^{n+1}\xi_i x_i=M. \tag{8}$$

The secret dealer D make computation according to the secret share k_i of the participant P_i in group A and value u_1 as follows:

$$y_{i1} = F(u_1, k_i) = g^{u_1+k_i},\ (1 \le i \le m_1);$$
$$y_{ij} = y_{i1}^{j} = g^{(u_i+k_i)j},\qquad (1 \le i \le m_1, 1 \le j \le n);$$

$$y_{i,n+1} = \left(M - \sum_{j=1}^{n} \xi_j y_{ij}\right)\xi_{n+1}^{-1},\quad (1 \le i \le m_1);$$

$$H_i = M - \sum_{j=1}^{n} \xi_j y_{ij},\qquad (1 \le i \le m_1);$$

$$H_0 = \xi_{n+1} y_{0,n+1}.$$

Thus, point $U_i(y_{i1}, y_{i2}, \cdots, y_{i,n+1})$ is on the hypertangent plane π. There are m_1 points in all. The secret dealer publishs $H_i\ (0 \le i \le m_1)$, the coordinates of point U_0, the expressions of the bivariate function and the coordinate function on NB.

The secret dealer D chooses a spherical curve Γ on the hypersphere $\sum$,

$$\boldsymbol{r} = \boldsymbol{r}(t) = (x_1(t), x_2(t), \cdots, x_{n+1}(t)). \tag{9}$$

Differentiating (9) it follows

$$\boldsymbol{r}'(t) = (x_1'(t), x_2'(t), \cdots, x_{n+1}'(t)). \tag{10}$$

The secret dealer D set $t = t_0$ with $t_0 \in Z_p$ such that $x_1(t_0) \ne y_{01}$, which yields that

$$\boldsymbol{r}(t_0) = (x_1(t_0), x_2(t_0), \cdots, x_{n+1}(t_0)),$$
$$\boldsymbol{r}'(t_0) = (x_1'(t_0), x_2'(t_0), \cdots, x_{n+1}'(t_0)),$$

Then the secret dealer D can derive a hypernormal plane $\overline{\pi}$ of curve Γ at $t = t_0$,

$$\boldsymbol{r}'(t_0) \cdot (\boldsymbol{\rho} - \boldsymbol{r}(t_0)) = 0,$$

That is,

$$\sum_{i=1}^{n+1} x_i'(t_0)(x_i - x_i(t_0)) = 0,$$

where $\boldsymbol{\rho} = (x_1, x_2, \cdots, x_{n+1})$ is a vector of the moving point coordinates.

Letting $\overline{\xi}_i = x_i'(t_0)$, $\overline{M} = \sum_{i=1}^{n+1} x_i(t_0) x_i'(t_0)$, one gets the following equation of the hypernormal plane $\overline{\pi}$:

$$\sum_{i=1}^{n+1} \overline{\xi}_i x_i = \overline{M}. \tag{11}$$

The secret dealer D chooses numbers $\gamma_i, u_2 \in Z_p$ such that $u_2 \ne u_1, \gamma_i \ne \overline{k}_h\ (0 \le i \le n - n_2, 1 \le h \le m_2)$, together with the bivariate function and the coordinate function as well as the secret share $\overline{k}_h$ of m_2 participants P_h in group B to calculate over Z_p as follows:

$$\begin{aligned}
&\overline{y}_{i1} = F\left(u_2, \gamma_i\right) = g^{u_2+\gamma_i},\\
&\overline{y}_{ij} = \overline{y}_{i1}^{j} = g^{(u_2+\gamma_i)j},\\
&\overline{y}_{\delta+h,1} = F\left(u_2, \overline{k}_h\right) = g^{u_2+\overline{k}_h},\\
&\overline{y}_{\delta+h,j} = \overline{y}_{\delta+h,1}^{j} = g^{\left(u_2+\overline{k}_h\right)j},\\
&\overline{H}_i = \overline{M} - \sum_{j=1}^{n} \overline{\xi}_j \overline{y}_{ij},\\
&\overline{y}_{i,n+1} = \left(\overline{M} - \sum_{j=1}^{n} \overline{\xi}_j \overline{y}_{ij}\right) \overline{\xi}_{n+1}^{-1},\\
&\overline{H}_{\delta+h} = \overline{M} - \sum_{j=1}^{n} \overline{\xi}_j \overline{y}_{\delta+h,j},\\
&\overline{y}_{\delta+h,n+1} = \left(\overline{M} - \sum_{j=1}^{n} \overline{\xi}_j \overline{y}_{\delta+h,j}\right) \overline{\xi}_{n+1}^{-1}.
\end{aligned}$$

where $\delta = n - n_2, 0 \le i \le \delta, 1 \le h \le m_2, 1 \le j \le n$.

Hence the secret dealer D obtains altogether $m_2 + \delta + 1$ hyperplanes, those are $V_i\left(\overline{y}_{i1}, \overline{y}_{i2}, \cdots, \overline{y}_{i,n+1}\right)$ and $V_{\delta+h}\left(\overline{y}_{\delta+h,1}, \overline{y}_{\delta+h,2}, \cdots, \overline{y}_{\delta+h,n+1}\right)$. At the same time the secret dealer D publishes $\overline{H}_i, \overline{H}_{\delta+h}$ and the coordinate of $V_i\left(0 \le i \le \delta\right)$ on *NB*.

3.2. Reconstruction of the Secrets

For arbitrary $n_1 (= n)$ participants in group A gather their secret shares together, without loss of generality, suppose that they are $P_i\left(1 \le i \le n\right)$. Each participant P_i uses his private share k_i and the public information on the *NB* to calculate $y_{ij}\left(1 \le i \le n, 1 \le j \le n\right)$ respectively. Then these n cooperative participants substitute y_{ij}, H_i and the coordinate of U_0 into the following undetermined expression

$$\sum_{j=1}^{n} \xi_j y_{ij} + H_i = M, \ \left(0 \le i \le n\right).$$

Which yields that the following system of equations:

$$\begin{cases}
y_{01}\xi_1 + y_{02}\xi_2 + \cdots + y_{0n}\xi_n + H_0 = M,\\
y_{11}\xi_1 + y_{12}\xi_2 + \cdots + y_{1n}\xi_n + H_1 = M,\\
\vdots\\
y_{n1}\xi_1 + y_{n2}\xi_2 + \cdots + y_{nn}\xi_n + H_n = M.
\end{cases} \tag{12}$$

Calculating $\xi_i\left(1 \le i \le n\right)$ and M in (12), they obtain the equation of hypertangent plane π about the hypersphere $\sum$ at point U_0,

$$\sum_{i=1}^{n+1} \xi_i x_i = M. \tag{13}$$

where ξ_{n+1} is given by $\xi_{n+1} = H_0 y_{0,n+1}^{-1}$.

These n cooperative participants get a normal vector $\boldsymbol{\xi} = \left(\xi_1, \xi_2, \cdots, \xi_{n+1}\right)$ from (13), which derive the equation of normal line L about π at point U_0 as follows:

$$\frac{x_1 - y_{01}}{\xi_1} = \frac{x_2 - y_{02}}{\xi_2} = \cdots = \frac{x_{n+1} - y_{0,n+1}}{\xi_{n+1}}, \tag{14}$$

where $(x_1, x_2, \cdots, x_{n+1})$ is a moving point coordinate vector.

Similarly, arbitrary n_2 participants in group B gather their secret shares together, without loss of generality, suppose that they are $\overline{P}_j (1 \le j \le n_2)$ who possess secret share $\overline{k}_j$ respectively. They use $\overline{k}_j$ and the public information on NB to obtain the following system of equations:

$$\begin{cases} \overline{y}_{01}\overline{\xi}_1 + \overline{y}_{02}\overline{\xi}_2 + \cdots + \overline{y}_{0n}\overline{\xi}_n + \overline{H}_0 = \overline{M} \\ \overline{y}_{11}\overline{\xi}_1 + \overline{y}_{12}\overline{\xi}_2 + \cdots + {}_{1n}\,\overline{y}\overline{\xi}_n + \overline{H}_1 = \overline{M}, \\ \vdots \\ \overline{y}_{\delta 1}\overline{\xi}_1 + \overline{y}_{\delta 2}\overline{\xi}_2 + \cdots + \overline{y}_{\delta n}\overline{\xi}_n + \overline{H}_\delta = \overline{M}, \\ \overline{y}_{\delta+1,1}\overline{\xi}_1 + \overline{y}_{\delta+1,2}\overline{\xi}_2 + \cdots + \overline{y}_{\delta+1,n}\overline{\xi}_n + \overline{H}_{\delta+1} = \overline{M}, \\ \vdots \\ \overline{y}_{\delta+n_2,1}\overline{\xi}_1 + \overline{y}_{\delta+n_2,2}\overline{\xi}_2 + \cdots + \overline{y}_{\delta+n_2,n}\overline{\xi}_n + \overline{H}_{\delta+n_2} = \overline{M}. \end{cases} \tag{15}$$

From (15) it follows $\overline{\xi}_i (1 \le i \le n)$ and $\overline{M}$. By calculating $\overline{\xi}_{n+1} = \overline{H}_0 y_{0,n+1}^{-1}$, these n_2 cooperative participants can obtain the equation of hypernormal plane $\overline{\pi}$ about hypersphere $\sum$,

$$\sum_{i=1}^{n+1} \overline{\xi}_i x_i = \overline{M}. \tag{16}$$

At last, these n_1 cooperative participants in group A and that n_2 cooperative participants in group B solve in common the following set of equations which consist of (14) and (16):

$$\begin{cases} \dfrac{x_1 - y_{01}}{\xi_1} = \dfrac{x_2 - y_{02}}{\xi_2} = \cdots = \dfrac{x_{n+1} - y_{0,n+1}}{\xi_{n+1}}, \\ \displaystyle\sum_{i=1}^{n+1} \overline{\xi}_i x_i = \overline{M}. \end{cases}$$

Which yields the centre coordinate of hypersphere $\sum$, that is, $(x_1, x_2, \cdots, x_{n+1}) = (a_1, a_2, \cdots, a_{n+1})$. Then by solving the transformation formula (7), these participants can recover the shared secrets $s_1, s_2, \cdots, s_t$.

4. Analysis of the Scheme

4.1. Correctness Proof

If the secret dealer and the participants are all honest in this scheme, at least n_1 participants in group A and at least n_2 participants in group B get together to reconstruct the shared secrets during the execution of reconstruction algorithm. To obtain this conclusion, we need only to prove the following theorem.

Theorem 2. The hypernormal plane π of any spherical curve Γ on a hypersphere $\sum$ always passes the centre of this hypersphere.

Proof. Let us put the spherical representation of $\sum$ as follows:

$$\sum_{i=1}^{n+1} (x_i - a_i)^2 = N^2,$$

and let spherical curve Γ be

$$\boldsymbol{r}(t)=\left(x_1(t),x_2(t),\cdots,x_{n+1}(t)\right).$$

Hence, we have

$$\sum_{i=1}^{n+1}\left(x_i(t)-a_i\right)^2=N^2,$$

and there exist a tangent vector of arbitrary point $\left(x_1(t_0),x_2(t_0),\cdots,x_{n+1}(t_0)\right)$ on the spherical curve Γ,

$$\boldsymbol{r}'(t_0)=\left(x_1'(t_0),x_2'(t_0),\cdots,x_{n+1}'(t_0)\right).$$

Let the coordinate of moving point on the hypernormal plane at t_0 be $\left(X_1,X_2,\cdots,X_{n+1}\right)$, then the equation of this hypernormal plane is

$$\sum_{i=1}^{n+1}x_i'(t_0)\left(X_i-x_i(t_0)\right)=0.$$

It implies

$$\sum_{i=1}^{n+1}x_i'(t_0)X_i-\sum_{i=1}^{n+1}x_i'(t_0)x_i(t_0)=0. \tag{17}$$

Differentiating $\sum_{i=1}^{n+1}\left(x_i(t)-a_i\right)^2=N^2$, we have

$$\sum_{i=1}^{n+1}x_i'(t)\left(x_i(t)-a_i\right)=0.$$

Which implies that when $t=t_0$, we get

$$\sum_{i=1}^{n+1}x_i'(t_0)x_i(t_0)=\sum_{i=1}^{n+1}a_ix_i'(t_0). \tag{18}$$

Substituting (18) into (17), we obtain the hypernormal plane $\overline{\pi}$ as follows:

$$\sum_{i=1}^{n+1}x_i'(t_0)\left(X_i-a_i\right)=0.$$

Obviously, it passes the centre $\left(a_1,a_2,\cdots,a_{n+1}\right)$ of hypersphere.

This completes the proof.

In our scheme, since the normal line L of hypertangent plane π at U_0 passes the centre of hypersphere too, it follows that the cross point of normal line L and hypernormal plane $\overline{\pi}$ is the centre of hypersphere.

Theorem 3. The unique hypertangent plane π over Z_p is determined by arbitary n different points of m_1 points derived from the secret shares $k_i\left(1\le i\le m_1\right)$ together with point U_0.

Proof. The system of Equations (12) determined by n different points and the public point U_0 can be modified as follows:

$$\begin{cases}-M+y_{01}\xi_1+y_{02}\xi_2+\cdots+y_{0n}\xi_n=-H_0,\\ -M+y_{11}\xi_1+y_{12}\xi_2+\cdots+y_{1n}\xi_n=-H_1,\\ \vdots\\ -M+y_{n1}\xi_1+y_{n2}\xi_2+\cdots+y_{nn}\xi_n=-H_n,\end{cases} \tag{19}$$

where M and $\xi_i\left(1\le i\le n\right)$ are unknown numbers of this system.

The determinant of coefficient for (19) can be obtained that

$$D=\begin{vmatrix}-1 & y_{01} & y_{02} & \cdots & y_{0n}\\ -1 & y_{11} & y_{12} & \cdots & y_{1n}\\ -1 & \vdots & \vdots & & \vdots\\ -1 & y_{n1} & y_{n2} & \cdots & y_{nn}\end{vmatrix}=-\begin{vmatrix}1 & 1 & \cdots & 1\\ y_{01} & y_{11} & \cdots & y_{n1}\\ y_{01}^2 & y_{11}^2 & \cdots & y_{n1}^2\\ \vdots & \vdots & & \vdots\\ y_{01}^n & y_{11}^n & \cdots & y_{n1}^n\end{vmatrix}=-\prod_{n\ge i>j\ge 0}\left(y_{i1}-y_{j1}\right).$$

Since $y_{i1}=F\left(u_1,k_i\right)=g^{u_1+k_i}$,

$$y_{j1}=F\left(u_1,k_j\right)=g^{u_1+k_j},$$

where $F\left(u,v\right)$ is the bivariate function over Z_p and g is a primitive root of modulo-p.

For any $k_i\ne k_j$, we have $y_{i1}\ne y_{j1}$, hence $D\ne 0$. It follows from Gramer rule that (19) has a unique set of solutions M, $\xi_i\left(1\le i\le n\right)$. Thus, the unique hypertangent plane π over Z_p. Can be determined by this set of solutions.

As a result, we obtain theorem.

Similarly, we can prove that the unique hypernormal plane $\overline{\pi}$ over Z_p is determined by arbitary n_2 different points of m_2 points derived from the secret shares $\overline{k}_j\left(1\le j\le m_2\right)$ together with $\delta+1$ public points $V_i\left(0\le i\le\delta\right)$.

The above theorem show a deterministic condition for the hypertangent plane or the hypernormal plane.

4.2. Security Analysis

The security of proposed scheme is based on the deterministic condition of hyperplane.

Theorem 4. Arbitrary n points in R^{n+1} cannot determine unique hyperplane over Z_p.

Proof. Suppose in existence n points (there is no harm in taking $U_0,U_1,\cdots,U_{n-1}$) can determine a hyperplane π_1. Then, we pick a point W which is out of π_1 in R^{n+1} such that the coordinate vectors of $U_0,U_1,\cdots,U_{n-1}$, W is linearly independent. By theorem 3, it is obvious that $U_0,U_1,\cdots,U_{n-1}$, W can determine unique hyperplane π_2 over Z_p. Because W is out of π_1, it follows that $\pi_1\ne\pi_2$. However, $U_0,U_1,\cdots,U_{n-1}$ are on not only π_1 but also π_2. This is a contradiction. Thus, we completes the proof of theorem 4.

It can be shown from the theorem 4 that n_1-1 or fewer participants in group A submiting their secret shares can only produce n_1 points including U_0 at most. So that they have no way of determining hypertangent plane π. Similarly, n_2-1 or fewer participants in group B have no way of determining hypernormal plane $\overline{\pi}$ too. This shows that the less than n_1 participants in group A or the less than n_2 participants in group B gathering their secret shares together cannot recover the shared secrets $S_1,S_2,\cdots,S_t$.

In addition, it is not difficult for an attacker to get the public informations $H_i,\overline{H}_j$ in the proposed scheme. Hwever, $H_i,\overline{H}_j$ are product of the coefficient

$\xi_{n+1}, \overline{\xi}_{n+1}$ and the last coordinate value of points which are derived from the secret shares of m_1 participants in group A and m_2 participants in group B respectively. They are calculated by the equation of hyperplanes and the front n coordinate value of derived points. On the contrary, the front n coordinate value of derived points cannot be predicted by $H_i, \overline{H}_j$, that means the attacker could not obtain the shared secrets from the public informations on *NB*. Moreover, together with the bivariate function, calculating $k_i, \overline{k}_j$ from $y_{01}, \overline{y}_{01}$ respectively need to solve the discrete logarithm problem, As we know that the discrete logarithm problem is intractable, it is impossible for an attacker to obtain the participant's secret share.

4.3. Performance Analysis

4.3.1. Information Rate of the Proposed Scheme

By the construction of proposed scheme, each share k_i or $\overline{k}_j$ is choosed from Z_p, and the shared secrets $S_1, S_2, \cdots, S_t$ from Z_p too. It follows that $|K_h| = |S| = p$,where K_h is a set of possible secret shares of participants in group A or in group B, and S is a set of possible shared secrets. Hence, the information rate of this scheme is

$$\rho = \min\left\{\rho_h \mid \rho_h = \lg|S|/\lg|K_h|, 1 \le h \le m_1 + m_2\right\} = p/p = 1.$$

This shows that the proposed scheme is ideal one.

4.3.2. Advantages of the Proposed Scheme

1) Multiple secrets can be reconstructed simultaneously within a secret sharing session.

2) Since the participants provide the derived points of secret shares but not the secret share $k_i, \overline{k}_j$ during the reconstruction of secrets, it follows that the secret shares of participants are still kept confidential after recovering all of the secrets and the secret shares could be used to share a new set of secrets.

3) When a new participant joins the system, the secret dealer needs only to select a new secret share that its derived points is on the hyperplane to distribute to this new participant secretly. When we need to delete a participant, the dealer needs only to change the value of parameter u in the bivariate function to recompute hyperplane, whereas the remainder participants can share next secrets by same secret shares. So it is very easy that the participants can join or leave the system.

4) When the value of threshold n_1 or n_2 is changed, namely, $(n_1 + n_2, m_1 + m_2)$ change into $(\overline{n}_1 + \overline{n}_2, m_1 + m_2)$, let us put $n = \max(n_1, n_2)$ and $\overline{n} = \max(\overline{n}_1, \overline{n}_2)$, the secret dealer needs only to turn the n+1 dimension space into a $\overline{n}+1$ dimension space and go on according to the same scheme. Whereas there is no need to change the one's own secret share for each participant.

The above advantages of this scheme are not provided by the secret sharing scheme with bipartite access structure [13] [14] [15]. In addition, the scheme

uses hypersphere geometry to study, which is more intuitive and clear than the scheme [13] [14] [15], and the method is more unique.

4.3.3. Computational Complexity

The only operations used in this scheme are linear combination operation, determinant operation and exponentiation operation, of which the former is negligible complexity. Obviously, the performance of the scheme mainly depends on the calculation of determinant, which is relatively easy to implement. If the determinant is computed by Wiedemann algorithm in [19], the performance of this scheme will be further improved. In the following, we count the number of times of exponentiation operations taken by the secret dealer and each participant.

1) In the distribution stage: the secret dealer D calculate $g^{u_1+k_i}$ over Z_p altogether m_1+1 times and calculate $g^{u_2+\bar{k}_j}$ over Z_p altogether $m_2+n_1-n_2+1$ times.

2) In the reconstruction stage: authorized participants in group A calculate $g^{u_1+k_i}$ over Z_p altogether n_1 times and ones in group B calculate $g^{u_2+\bar{k}_j}$ over Z_p altogether n_2 times.

Thus it can seen that the proposed scheme needs $m_1+m_2+2(n+1)$ exponentiation operations. We remark that one exponentiation operation can be done in time $O\left((\log p)^3\right)$. In that way, sharing and reconstructing the secrets can be done in all time $O\left((m_1+m_2+2(n+1))(\log p)^3\right)$. It is obvious that the proposed scheme satisfies the definition of a computationally efficient secret sharing scheme.

This scheme is more effective than other secret sharing schemes [6]-[12] on general access structure when sharing larger secrets. Assuming that the length of the secret shared is $t\times 512$ bits, a comparison is made between the scheme in [6] and the one in this paper. In the scheme in [6], the length of module-p should be at least $t\times 512$ bits. With the scheme in my paper, the shared secret can be divided into t sub-secrets, and then the t sub-secrets can be shared. Therefore, the length of module-p is 512 bits, which greatly reduces the computational complexity compared with the scheme in [6].

5. Conclusion

In this paper, an efficient bipartite (n_1+n_2, m_1+m_2)-threshold multi-secret sharing scheme is proposed, which is based on a hypersphere by using a geometric method, In this scheme, multi-secret could be shared and each participant needs only to hold one secret share in renewing the shared secrets without updating each participant's secret share. Compared with the existing bipartite secret sharing scheme, it is easy to show that not only the participants can leave the system and new participants can be added into the system dynamically, but also the values of threshold n_1, n_2 can be changed. Therefore, the proposed scheme is very effective and practical.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

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

[2] Blakley, G. (1979) Safeguarding Cryptographic Keys. *Proceedings of* 1979 *International Workshop on Managing Requirements Knowledge*, **48**, 313-317. https://doi.org/10.1109/MARK.1979.8817296

[3] McEliece, R.J. and Sarwate, D.V. (1981) On Sharing Secrets and Reed-Solomon codes. *Communications of the ACM*, **24**, 583-584. https://doi.org/10.1145/358746.358762

[4] Asmuth, C. and Bloom, J.A. (1983) A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, **29**, 208-210. https://doi.org/10.1109/TIT.1983.1056651

[5] Karnin, E.D., Green, J.W. and Hellman, M.E. (1983) On Secret Sharing System. *IEEE Transactions on Information Theory*, **29**, 35-41. https://doi.org/10.1109/TIT.1983.1056621

[6] Nojoumian, M. and Stinson, D.R. (2013) On Dealer-Free Dynamic Threshold Schemes. *Advances in Mathematics of Communications*, **7**, 39-56. https://doi.org/10.3934/amc.2013.7.39

[7] Fine, B., Moldenhauer, I.S. and Rosenberger, G. (2013) A Secret Sharing Scheme Based on the Closet Vector Theorem and a Modification to a Private Key Cryptosystem. *Groups Complexity Cryptology*, **5**, 223-238. https://doi.org/10.1515/gcc-2013-0012

[8] Blundo, C., Santis, A.D. and Crescenzo, G.D. (1995) Multi-Secret Sharing Schemes. *Advances in Cryptology*, **839**, 150-163.

[9] Shao, J., Zhang, J. and Zhao, R. (2007) A Practical Verifiable Multi-Secret Sharing Scheme. *Computer Standards and Interfaces*, **29**, 138-141. https://doi.org/10.1016/j.csi.2006.02.004

[10] Dehkordi, M.H. and Mashhadi, S. (2008) New Efficient and Practical Verifiable Multi-Secret Sharing Schemes. *Information Sciences*, **178**, 2262-2274. https://doi.org/10.1016/j.ins.2007.11.031

[11] Wang, S.T., Tsai, Y.R. and Shen, C.C. (2011) Verifiable Threshold, Scheme in Multi-Secret Sharing Distributions upon Extensions of ECC. *Wireless Personal Communications*, **56**, 173-182. https://doi.org/10.1007/s11277-009-9875-0

[12] Eslami, Z. and Ahmadabadi, J.Z. (2010) A Verifiable Multi-Secret Sharing Scheme Based on Cellular Automata. *Information Sciences*, **180**, 2889-2894. https://doi.org/10.1016/j.ins.2010.04.015

[13] Padro, C. and Saez, G. (2000) Secret Sharing Schemes with Bipartite Access Structure. *IEEE Transactions on Information Theory*, **46**, 2596-2604. https://doi.org/10.1109/18.887867

[14] Li, B. (2006) Difference Secret Sharing Scheme Based on Special Access Right. *Journal of Sichuan University*, **43**, 78-83.

[15] Li, B. (2014) The Secret Sharing Scheme Based on Acyclic Polynomial Sequence. *Journal of Sichuan University*, **51**, 423-427.

[16] Marti, J.F. and Padro, C. (2007) On Secret Sharing Schemes, Matroids and Polymatroids. *Proceedings of the Fourth Theory of Cryptography Conference Amsterdam*, **4392**, 253-272.

[17] Ng, S.L. and Walker, M. (2001) On the Composition of Matroids and Ideal Secret Sharing Schemes. *Designs*, *Codes and Cryptography*, **24**, 49-67.

[18] Cheng, Q., Yin, Y., Xiao, K. and Hsu, C.-F. (2009) On Non-Representable Secret Sharing Matroids. *Proceedings of the* 5*th International Conference on Information Security Practice and Experience*, **5451**, 124-135.

[19] Wu, T.C. and He, W.H. (1995) A Geometric Approach for Sharing Secrets. *Computers & Security*, **14**, 135-145. https://doi.org/10.1016/0167-4048(95)97047-E

[20] Li, B. (2014) The Threshold Secret Sharing Scheme Based on Hyperspace Parameter Curve. *Journal of Zhejiang University*, **41**, 518-522.