Bipartite Threshold Multi-Secret Sharing Scheme Based on Hypersphere

Bin Li

Department of Mathematics, Chengdu Normal University, Chengdu, China
E-mail: 1145398209@qq.com

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 $\mathbb{Z}_p$ 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-
Applications 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 be 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 $n_i$ 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 $n_1, n_2 \in \mathbb{Z}^*$ satisfying $m_i \geq \max\{|n_i - n_2| + 1, n_i\}$, $i = 1, 2$. 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 $k_j (1 \leq j \leq m_2)$ 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 $A = \{P_1, P_2, \ldots, P_{m_1}\}$, $B = \{\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_{m_2}\}$, 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 $\mathbb{Z}_p$, where $p$ is a large prime satisfying $p = 3 \mod 4$. 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 arbitrary $n+1$ integer module-$p$.

Let $[Ox_1, x_2, \ldots, x_{n+1}]$ be $n+1$ dimension Cartesian orthogonal coordinate system in real Euclidean space $\mathbb{R}^{n+1}$.

**Definition 2.** Assume that $Q(a_1, a_2, \ldots, a_{n+1})$ is a point of $\mathbb{R}^{n+1}$, $N \in \mathbb{Z}_p$, where $p$ is a large prime satisfying $p = 3 \mod 4$. 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 arbitrary $n+1$ integer module-$p$.
and let \( N \) denote the radius of hypersphere \( \Sigma \). Then the spherical representation of hypersphere \( \Sigma \) is defined as follows:

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

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

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

\[
r = r(t) = (x_1(t), x_2(t), \ldots, x_{n+1}(t)),
\]

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

The derived vector of curve \( \Gamma \)

\[
r'(t) = \frac{dr(t)}{dt} = \left( \frac{dx_1(t)}{dt}, \frac{dx_2(t)}{dt}, \ldots, \frac{dx_{n+1}(t)}{dt} \right)
\]

is called the tangent vector at point \( t \) of curve \( \Gamma \).

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

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

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

Then curve \( \Gamma \) is called the spherical curve of hypersphere \( \Sigma \).

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

\[
\delta: (z_1, z_2, \ldots, z_n) \leftrightarrow (x_1, x_2, \ldots, x_{n+1})
\]

such that

\[
\begin{align*}
x_1 &= x_1(z_1, z_2, \ldots, z_n), \\
x_2 &= x_2(z_1, z_2, \ldots, z_n), \\
&\quad \vdots \\
x_{n+1} &= x_{n+1}(z_1, z_2, \ldots, z_n).
\end{align*}
\]

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

\[
F(u, v) = g^{uv},
\]

and a coordinate function over \( Z_p \)

\[
y_{ij} = y_{ij}^t (i = 0, 1, 2, \ldots; j = 1, 2, \ldots, n+1).
\]

### 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 \( S_1, S_2, \ldots, S_j \). 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 shares $k_i$ ($1 \leq i \leq m_1$) and number $u_1$ from $\mathbb{Z}_p$ 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 $\overline{k}_j$ ($1 \leq j \leq m_2$) and number $u_2$ from $\mathbb{Z}_p$ such that $u_1 \neq u_2$ 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 $n_1 \geq n_2$, then $n = n_1$. We assume that $t$ shared secrets $s_1, s_2, \cdots, s_t$ are all from $\mathbb{Z}_p$ where $1 \leq t \leq n$. 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

\[
\begin{align*}
&x_1(s_1, s_2, \cdots, s_t) = a_1, \\
&x_2(s_1, s_2, \cdots, s_t) = a_2, \\
&\vdots \\
&x_{n+1}(s_1, s_2, \cdots, s_t) = a_{n+1},
\end{align*}
\]

which yields a point $Q(a_1, a_2, \cdots, a_{n+1}) \in \mathbb{Z}_p^{n+1}$.

The secret dealer chooses a positive integer $N \in \mathbb{Z}_p^*$ to get a spherical representation of a hypersphere

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

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

The secret dealer chooses $k_0 \in \mathbb{Z}_p$ such that $k_0 \neq k_i$ ($1 \leq i \leq m_1$) and a bivariate function like (5), together with the coordinate function (6) to calculate over $\mathbb{Z}_p$ as follows:

\[
y_{0j} = y_{0j}, j = 1, 2, \cdots, n.
\]

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

\[
\sum_{i=1}^{n+1} (y_{0i} - a_i)^2 = N^2,
\]

which yields a point on $\Sigma$,

$\mathbf{U}_0\left(y_{01}, y_{02}, \cdots, y_{0,n+1}\right)$.

It is not difficult to get a hypertangent plane $\pi$ of $\Sigma$ at $U_0$:

\[
\sum_{i=1}^{n+1} (y_{0i} - a_i)(x_i - y_{0i}) = 0.
\]

Letting $\xi_j = y_{0j} - a_j, M = \sum_{i=1}^{n+1} y_{0i} (y_{0i} - a_i)$, one obtains a following equation of hypertangent plane $\pi$:

\[
\sum_{j=1}^{n+1} \xi_j x_j = M.
\]
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:

\[
y_{i1} = F(u_i, k_i) = g^{u_i + k_i}, \quad (1 \leq i \leq m_1);
\]

\[
y_{i0} = y_{i1}^{j}, \quad (1 \leq i \leq m_1, 1 \leq j \leq n);
\]

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

\[
H_i = M - \sum_{j=1}^{n} \xi_j y_{ij}, \quad (1 \leq i \leq m_1);
\]

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

Thus, point $U \left( y_{i1}, y_{i2}, \cdots, y_{i,n+1} \right)$ is on the hypertangent plane $\pi$. There are $m_1$ points in all. The secret dealer publishes $H_i \left( 0 \leq i \leq m_1 \right)$, 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 $\Gamma$ on the hypersphere $\sum$,

\[
r = r(t) = (x_1(t), x_2(t), \cdots, x_{n+1}(t)).
\]  

(9)

Differentiating (9) it follows

\[
r'(t) = (x'_1(t), x'_2(t), \cdots, x'_{n+1}(t)).
\]  

(10)

The secret dealer $D$ set $t = t_0 \in Z_p$ such that $x_i(t_0) \neq y_{0i}$, which yields that

\[
r(t_0) = (x_1(t_0), x_2(t_0), \cdots, x_{n+1}(t_0)),
\]

\[
r'(t_0) = (x'_1(t_0), x'_2(t_0), \cdots, x'_{n+1}(t_0)).
\]

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

\[
r'(t_0) \cdot (\rho - r(t_0)) = 0,
\]

That is,

\[
\sum_{i=1}^{n+1} x'_i(t_0)(x_i - x_i(t_0)) = 0,
\]

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

Letting $\xi_j = x'_j(t_0), \quad \bar{M} = \sum_{i=1}^{n+1} x_i(t_0)x_i'(t_0)$, one gets the following equation of the hypernormal plane $\pi$:

\[
\sum_{i=1}^{n+1} \xi_j x_i = \bar{M}.
\]  

(11)

The secret dealer $D$ chooses numbers $\gamma_i, u_2 \in Z_p$ such that

\[
u_2 \neq u_1, \gamma_i \neq \bar{k}_h \left( 0 \leq i \leq n - n_2, 1 \leq h \leq m_2 \right),
\]

together with the bivariate function and the coordinate function as well as the secret share $\bar{k}_h$ of $m_2$ participants $P_h$ in group $B$ to calculate over $Z_p$ as follows:
where $\delta = n - n_2, 0 \leq i \leq \delta, 1 \leq h \leq m_2, 1 \leq j \leq n$.

Hence the secret dealer $D$ obtains altogether $m_2 + \delta + 1$ hyperplanes, those are $V_1(\overline{y}_{i1}, \overline{y}_{i2}, \cdots, \overline{y}_{in})$ and $V_{\delta+h}(\overline{y}_{\delta+h,1}, \overline{y}_{\delta+h,2}, \cdots, \overline{y}_{\delta+h,n+1})$. At the same time the secret dealer $D$ publishs $\overline{H}_i, \overline{H}_{\delta+h}$ and the coordinate of $V_i(0 \leq i \leq \delta)$ 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 $P_i(1 \leq i \leq n)$. Each participant $P_i$ uses his private share $k_i$ and the public information on the NB to calculate $y_{ij}(1 \leq i \leq n, 1 \leq j \leq n)$ respectively. Then these $n$ cooperative participants substitute $y_{ij}$, $H_i$ and the coordinate of $U_0$ into the following undetermined expression

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

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 $\xi_i(1 \leq i \leq n)$ and $M$ in (12), they obtain the equation of hyper-tangent plane $\pi$ about the hypersphere $\Sigma$ at point $U_0$,

$$\sum_{j=1}^{n+1} \xi_j x_j = M. \tag{13}$$

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

These $n$ cooperative participants get a normal vector $\xi = (\xi_1, \xi_2, \cdots, \xi_{n+1})$ from (13), which derive the equation of normal line $L$ about $\pi$ at point $U_0$ as follows:
\[ \frac{x_1 - y_{01}}{\xi_1} = \frac{x_2 - y_{02}}{\xi_2} = \ldots = \frac{x_{n+1} - y_{0,n+1}}{\xi_{n+1}}, \]  

(14)

where \((x_1, x_2, \ldots, x_{n+1})\) 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 \(F_j (1 \leq j \leq n_2)\) who possess secret share \(k_j\) respectively. They use \(k_j\) and the public information on \(NB\) to obtain the following system of equations:

\[
\begin{align*}
\gamma_{01} \bar{\xi}_1 + \gamma_{02} \bar{\xi}_2 + \ldots + \gamma_{0n} \bar{\xi}_n + \psi_1 &= \bar{M}, \\
\gamma_{11} \bar{\xi}_1 + \gamma_{12} \bar{\xi}_2 + \ldots + \gamma_{1n} \bar{\xi}_n + \psi_2 &= \bar{M}, \\
\vdots &
\end{align*}
\]

(15)

From (15) it follows \(\bar{\xi}_i (1 \leq i \leq n)\) and \(\bar{M}\). By calculating \(\bar{\xi}_{n+1} = \psi_0^{-1} \gamma_{0,n+1}\), these \(n\) cooperative participants can obtain the equation of hypernormal plane \(\pi\) about hypersphere \(\Sigma\),

\[
\sum_{j=1}^{n+1} \bar{\xi}_j x_i = \bar{M}.
\]

(16)

At last, these \(n\) 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):

\[
\begin{align*}
\frac{x_1 - y_{01}}{\xi_1} = \frac{x_2 - y_{02}}{\xi_2} = \ldots = \frac{x_{n+1} - y_{0,n+1}}{\xi_{n+1}}, \\
\sum_{j=1}^{n+1} \bar{\xi}_j x_i = \bar{M}.
\end{align*}
\]

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

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 \(\pi\) of any spherical curve \(\Gamma\) on a hypersphere \(\Sigma\) always passes the centre of this hypersphere.

**Proof.** Let us put the spherical representation of \(\Sigma\) as follows:

\[
\sum_{j=1}^{n+1} (x_j - a_j)^2 = N^2,
\]
and let spherical curve $\Gamma$ be
\[ r(t) = (x_1(t), x_2(t), \ldots, x_{n+1}(t)). \]

Hence, we have
\[ \sum_{j=1}^{n+1} (x_j(t) - a_j)^2 = N^2, \]
and there exist a tangent vector of arbitrary point $(x_1(t_0), x_2(t_0), \ldots, x_{n+1}(t_0))$ on the spherical curve $\Gamma$,
\[ r'(t_0) = (x'_1(t_0), x'_2(t_0), \ldots, x'_{n+1}(t_0)). \]

Let the coordinate of moving point on the hypernormal plane at $t_0$ be $(X_1, X_2, \ldots, X_{n+1})$, then the equation of this hypernormal plane is
\[ \sum_{i=1}^{n+1} x'_i(t_0) (X_i - x_i(t_0)) = 0. \]

It implies
\[ \sum_{i=1}^{n+1} x'_i(t_0) X_i - \sum_{i=1}^{n+1} x'_i(t_0) x_i(t_0) = 0. \] (17)

Differentiating $\sum_{j=1}^{n+1} (x_j(t) - a_j)^2 = N^2$, we have
\[ \sum_{i=1}^{n+1} x'_i(t)(x_i(t) - a_i) = 0. \]

Which implies that when $t = t_0$, we get
\[ \sum_{i=1}^{n+1} x'_i(t_0) x_i(t_0) = \sum_{i=1}^{n+1} a_i x'_i(t_0). \] (18)

Substituting (18) into (17), we obtain the hypernormal plane $\pi$ as follows:
\[ \sum_{i=1}^{n+1} x'_i(t_0) (X_i - a_i) = 0. \]

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

This completes the proof.

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

**Theorem 3.** The unique hypertangent plane $\pi$ over $Z_p$ is determined by arbitrary $n$ different points of $m_1$ points derived from the secret shares $k_i$ $(1 \leq i \leq m_1)$ 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:
\[
\begin{align*}
-M + y_{01}\xi_1 + y_{02}\xi_2 + \cdots + y_{0n}\xi_n &= -H_0, \\
-M + y_{11}\xi_1 + y_{12}\xi_2 + \cdots + y_{1n}\xi_n &= -H_1, \\
&\quad \vdots \\
-M + y_{n1}\xi_1 + y_{n2}\xi_2 + \cdots + y_{nn}\xi_n &= -H_n.
\end{align*}
\] (19)
where $M$ and $\xi_i (1 \leq i \leq n)$ are unknown numbers of this system.

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

$$D = \begin{vmatrix}
-1 & y_{01} & y_{02} & \cdots & y_{0n} \\
-1 & y_{11} & y_{12} & \cdots & y_{1n} \\
-1 & \vdots & \vdots & \ddots & \vdots \\
-1 & y_{m1} & y_{m2} & \cdots & y_{mn}
\end{vmatrix} = \begin{vmatrix}
1 & 1 & \cdots & 1 \\
y_{01} & y_{11} & \cdots & y_{1n} \\
y_{02}^2 & y_{12}^2 & \cdots & y_{1n}^2 \\
\vdots & \vdots & \ddots & \vdots \\
y_{0n}^n & y_{1n}^n & \cdots & y_{1n}^n
\end{vmatrix} = \prod_{i \neq j \neq 0} (y_{ji} - y_{jj}).$$

Since $y_{ji} = F(u_i, k_j) = g^{n^i k_j}$, $y_{jj} = F(u_i, k_j) = g^{n^i k_j}$,

where $F(u, v)$ is the bivariate function over $\mathbb{Z}_p$ and $g$ is a primitive root of modulo-$p$.

For any $k_i \neq k_j$, we have $y_{ji} \neq y_{jj}$, hence $D \neq 0$. It follows from Gramer rule that (19) has a unique set of solutions $M$, $\xi_i (1 \leq i \leq n)$. Thus, the unique hypertangent plane $\pi$ over $\mathbb{Z}_p$ can be determined by this set of solutions.

As a result, we obtain theorem.

Similarly, we can prove that the unique hypernormal plane $\pi$ over $\mathbb{Z}_p$ is determined by arbitrary $n_2$ different points of $m_2$ points derived from the secret shares $\bar{k}_j (1 \leq j \leq m_2)$ together with $\delta + 1$ public points $V_i (0 \leq i \leq \delta)$.

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 $\mathbb{R}^{n+1}$ cannot determine unique hyperplane over $\mathbb{Z}_p$.

**Proof.** Suppose in existence $n$ points (there is no harm in taking $U_0, U_1, \cdots, U_{n-1}$) can determine a hyperplane $\pi$. Then, we pick a point $W$ which is out of $\pi_1$ in $\mathbb{R}^{n+1}$ 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 $\pi_2$ over $\mathbb{Z}_p$. Because $W$ is out of $\pi_1$, it follows that $\pi_1 \neq \pi_2$. However, $U_0, U_1, \cdots, U_{n-1}$ are on not only $\pi_1$ but also $\pi_2$. 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 $A$ submitting their secret shares can only produce $n_1$ points including $U_0$ at most. So that they have no way of determining hypertangent plane $\pi$. Similarly, $n_2 - 1$ or fewer participants in group $B$ have no way of determining hypernormal plane $\pi$ 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 $S_1, S_2, \cdots, S_r$.

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
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 \( H_i, \overrightarrow{H}_j \), that means the attacker could not obtain the shared secrets from the public informations on \( NB \). Moreover, together with the bivariate function, calculating \( k_i, \overrightarrow{k}_j \) from \( y_{01}, \overrightarrow{y}_{01} \) 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 \( \overrightarrow{k}_j \) 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

\[
\rho = \min \{ \rho_h | \rho_h = \log |S| / \log |K_h|, 1 \leq h \leq m_1 + m_2 \} = p / p = 1.
\]

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 \( k_i, \overrightarrow{k}_j \) 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 re-compute 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

\[ n = \max(n_1, n_2) \quad \text{and} \quad \overline{n} = \max(\overline{n_1}, \overline{n_2}), \]

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 \( g^{n+p} \) over \( \mathbb{Z}_p \) altogether \( m_1 + 1 \) times and calculate \( g^{m_2 + \xi_j} \) over \( \mathbb{Z}_p \) altogether \( m_2 + n_1 - n_2 + 1 \) times.

2) In the reconstruction stage: authorized participants in group A calculate \( g^{n+p} \) over \( \mathbb{Z}_p \) altogether \( n_1 \) times and ones in group B calculate \( g^{n_2 + \xi_j} \) over \( \mathbb{Z}_p \) altogether \( n_2 \) times.

Thus it can be 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 \( O((\log p)^3) \). 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


