Scientific Research Publishing

American Journal of Computational Mathematics, 2021, 11, 175-188
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

Verifiable Secret Sharing Scheme Based on Certain Projective Transformation

Bin Li

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

How to cite this paper: Li, B. (2021) Verifiable Secret Sharing Scheme Based on Certain Projective Transformation. *American Journal of Computational Mathematics*, **11**, 175-188.
https://doi.org/10.4236/ajcm.2021.112012

Received: May 14, 2021
Accepted: June 21, 2021
Published: June 24, 2021

Abstract

The main purpose of verifiable secret sharing scheme is to solve the honesty problem of participants. In this paper, the concept of nonzero k-submatrix and theresidual vector of system of hyperplane intersecting line equations is proposed. Based on certain projective transformations in projective space, a verifiable (t, n)-threshold secret sharing scheme is designed by using the structure of solutions of linear equations and the difficulty of solving discrete logarithm problems. The results show that this scheme can verify the correctness of the subkey provided by each participant before the reconstruction of the master key, and can effectively identify the fraudster. The fraudster can only cheat by guessing and the probability of success is only $1/p$. The design of the scheme is exquisite and the calculation complexity is small. Each participant only needs to hold a subkey, which is convenient for management and use. The analysis shows that the scheme in this paper meets the security requirements and rules of secret sharing, and it is a computationally secure and effective scheme with good practical value.

Keywords

Threshold Secret Sharing, Projective Transformation, Nonzero k–Submatrix, Residual Vector of Equations

1. Introduction

Secret sharing is a method proposed to solve the problem of key management. It is mainly used to prevent important information from being lost, destroyed, changed or falling into the wrong hands. It is an important subject in information security and cryptography. It is widely used in data management, financial network, e-commerce, e-government and many other fields [1] [2]. The basic idea of secret sharing is to share the master key in a group of participants, which

enables members of the authorized subset of participants to recover the master key through the subkey they get, while members of any participant's unauthorized subset cannot recover the master key through the subkey they get.

As early as 1979, Shamir [3] and Blakley [4] proposed (t,n)-threshold secret sharing scheme respectively. The algorithm given by Shamir system is based on polynomial interpolation, while Blakley system is based on finite geometry. The (t,n)-threshold secret sharing scheme requires that any t or more than t members of n participants cooperate to derive the master key, while no $t-1$ members cooperate to derive the master key. After these two masters, more secret sharing schemes have been proposed one after another, which are constructed by using mathematical knowledge and methods in different fields. For example, Article [5] uses Reed-Solomon code to construct secret sharing scheme, Article [6] uses Chinese Remainder Theorem to construct secret sharing scheme, Article [7] uses matrix operation on finite field to construct secret sharing scheme, Article [8] uses one-way function to construct secret sharing scheme, Article [9] uses vector space to construct secret sharing scheme, etc. Especially in recent years, people have made some gratifying achievements in the design and research of more complex secret sharing schemes [10] [11] [12] [13]. It should be pointed out that there may be dishonest participants in the actual use of these schemes. In view of how to effectively prevent fraud, many authors have conducted in-depth research on them. In Article [14]-[22], different schemes of secret sharing that can prevent fraud are proposed respectively.

However, none of the schemes mentioned above gives the probability of successful fraud accurately. Moreover, some schemes are complex in design, lack of intuition and conciseness, and fail to grasp the design principles of secret sharing schemes. The design principle of secret sharing scheme is not only to ensure its correctness, but also to pay attention to its security and effectiveness. According to this principle, this paper designs a kind of secret sharing scheme based on certain projective transformation. This scheme uses the special projective transformation in projective space to build the relationship between the master key and the subkey, so that the dealer (that is, the subkey distributor) can find the subkey through the master key to distribute the participants. Members of the authorized subset can gather their subkeys to find the relationship between the components of the shadow subkey vector, and recover the shadow subkey together with the residual vector of the intersecting line equations formed by the projection plane of the shadow subkey point in the space, so as to synthesize the master key. The secret sharing scheme designed in this way accords with the idea of (t,n)-threshold secret sharing, which is simple, intuitive, practical and easy to implement.

Organization of this paper is as follows. We introduce related definitions and preliminaries in Section 2. In Section 3, we propose our construction by using certain projective transformation method. Section 4 describes our security analysis and effectiveness analysis respectively. We draw the conclusion in Section 5.

2. Definitions and Preliminaries

If the projective plane is extended to the n-dimensional projective space and the infinite point is regarded as a common point, then according to the projective coordinate system established in Article [23], we can get the n-dimensional projective coordinate system σ.

Definition 1. Under the projective coordinate system σ, let the coordinate of point k be $(k_1, k_2, \cdots, k_n)$ and the coordinate of point x be $(x_1, x_2, \cdots, x_n)$ in the n-dimensional projective space. If the transformation from point k to point x is

$$T: \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix} \quad \left(A = (a_{ij})_{n\times n}, |A| \neq 0\right), \tag{1}$$

Then T is called a projective transformation in the n-dimensional projective space, where A is called the transformation matrix of T.

Because of $|A| \neq 0$, the projective transformation T has inverse transformation, that is

$$T^{-1}: \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix} = A^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \tag{2}$$

Under projective transformation T, if the coordinates of the original image point k are known, then the coordinates of the unique image point x can be obtained; conversely, if the coordinates of the image point x are known, then the coordinates of the unique original image point k can also be obtained.

Let

$$\begin{aligned} &b_{11}x_1 + b_{12}x_2 + \cdots + b_{1n}x_n = 0, \\ &b_{21}x_1 + b_{22}x_2 + \cdots + b_{2n}x_n = 0, \\ &\qquad\qquad \vdots \\ &b_{n-1,1}x_1 + b_{n-1,2}x_2 + \cdots + b_{n-1,n}x_n = 0 \end{aligned} \tag{3}$$

be the equations of $n-1$ hyperplanes which are not parallel to each other in the n-dimensional projective space. It means that the vector group composed of the normal vectors $\beta_1 = (b_{11}, b_{12}, \cdots, b_{1,n-1})$, $\beta_2 = (b_{21}, b_{22}, \cdots, b_{2,n-1})$, $\cdots$, $\beta_{n-1} = (b_{n-1,1}, b_{n-1,2}, \cdots, b_{n-1,n-1})$ of these hyperplanes is linearly independent, so the intersecting line of these hyperplanes is unique, and the system of equations about the unknown number $x_1, x_2, \cdots, x_{n-1}$ is

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \cdots + b_{1,n-1}x_{n-1} = -b_{1n}x_n, \\ b_{21}x_1 + b_{22}x_2 + \cdots + b_{2,n-1}x_{n-1} = -b_{2n}x_n, \\ \qquad\qquad \vdots \\ b_{n-1,1}x_1 + b_{n-1,2}x_2 + \cdots + b_{n-1,n-1}x_{n-1} = -b_{n-1,n}x_n. \end{cases} \tag{4}$$

Since the determinant $|A|$ of coefficient matrix A of this system of equations is not equal to zero, it can be seen from Gramer's law that the system of Equations (4) can be reduced to

$$\begin{cases} x_1 = c_1 x_n, \\ x_2 = c_2 x_n, \\ \quad \vdots \\ x_{n-1} = c_{n-1} x_n. \end{cases} \tag{5}$$

Equation (5) is the system of hyperplane intersecting line Equations (3), which consists of $n-1$ equations.

Definition 2. The system of equations composed of any $n-t\,(1<t<n)$ equations in the system of hyperplane intersecting line Equations (5) is called a $(n-t)$-residue of the system of this intersecting line equations, which can be expressed as

$$\begin{cases} x_{i_1} = c_{i_1} x_n, \\ x_{i_2} = c_{i_2} x_n, \\ \quad \vdots \\ x_{i_{n-t}} = c_{i_{n-t}} x_n, \end{cases} \tag{6}$$

where $1 \le i_1 < i_2 < \cdots < i_{n-t} \le n-1$.

Obviously, $(n-t)$-residue is determined by the constant $c_{i_1}, c_{i_2}, \cdots, c_{i_{n-t}}$, we call the vector $\boldsymbol{c} = (c_{i_1}, c_{i_2}, \cdots, c_{i_{n-t}})$ composed of these constants the corresponding $(n-t)$-residual vector. There are $C_{n-1}^{n-t} = \dfrac{(n-1)!}{(n-t)!(t-1)!}$ $(n-t)$-residues in a system of hyperplane intersecting line equations.

For the convenience of this study, we might as well take the permutation $i_1 i_2 \cdots i_{n-t} = 12\cdots(n-t)$, that is, the $(n-t)$ –residue is

$$\begin{cases} x_1 = c_1 x_n, \\ x_2 = c_2 x_n, \\ \quad \vdots \\ x_{n-t} = c_{n-t} x_n, \end{cases} \tag{7}$$

the corresponding residual vector is $\boldsymbol{c} = (c_1, c_2, \cdots, c_{n-t})$.

For the n-dimensional projective space, under the given projective coordinate system σ, let the plane coordinate of hyperplane ξ be $(\xi) = (\xi_1, \xi_2, \cdots, \xi_n)$, and the point coordinate of space point x be $(x) = (x_1, x_2, \cdots, x_n)$, using the combination sign $[\xi x] = \xi_1 x_1 + \xi_2 x_2 + \cdots + \xi_n x_n$, we analyze the geometric meaning of the following formula

$$[\xi x] = \xi_1 x_1 + \xi_2 x_2 + \cdots + \xi_n x_n = 0 \tag{8}$$

If (ξ) is regarded as a definite array and (x) as a variable array, then formula (8) represents the algebraic condition of the motion of moving point x on the definite hyperplane ξ, and formula (8) is the equation of hyperplane ξ.

On the contrary, If (x) is regarded as a definite array and (ξ) as a variable array, then formula (8) represents the algebraic condition of the rotation of the moving hyperplane ξ through the fixed point x, at this time, formula (8) is the equation of point x, that is, the equation of the hyperplane bundle with x as its center. It can be seen that formula (7) as $(n-t)$-residue is a part of hyperplane bundle equation of passing point x.

Let p be prime number and g be the original root of p, that is, $g^1, g^2, \cdots, g^{p-1}$ generates all values from 1 to $p-1$ under module p. Since $(g, p)=1$, and the necessary and sufficient condition of $g^k \equiv g^h \bmod p$ (where $\bmod p$ denotes congruence with respect to prime number p) is $k \equiv h \bmod (p-1)$, there is a unique $c \in \{1, 2, \cdots, p-1\}$ for any $b \in \{1, 2, \cdots, p-1\}$ that makes $b \equiv g^c \bmod p$ hold, c is called the discrete logarithm of b with g as the base under module p. The so-called discrete logarithm problem is such a mathematical problem: when p is a large prime number, given the integer c, it is easy to calculate $g^c \equiv b \bmod p$; on the contrary, given the integer b, it is very difficult to calculate the integer c, which makes $g^c \equiv b \bmod p$ hold.

We know that if A is an n-order matrix, let $k \in N^*, k < n$ any k-row and k-column of A are taken, and k^2 elements at the intersection of k-row and k-column form a k-order determinant in the original order, then this k-order determinant is a k-order minor of matrix.

Definition 3. Let p be a prime number, Z_p be a p-element finite field, and A be a n-order matrix over Z_p. If $|A| \neq 0$ and any k-order minor of A is not equal to zero, then matrix A is a nonzero k-submatrix.

When the transformation matrix $A=(a_{ij})_{n\times n}$ is a nonzero k-submatrix, the corresponding projective transformation (1) is a special projective transformation. The scheme in this paper is based on this kind of projective transformation.

Theorem 1. Let $p\,(>n)$ be prime, Z_p be a p-element finite field, and the n-order matrix A over Z_p be a nonzero $(n-t)$-submatrix, where $t \in Z_p$, $t<n$. If $k_1, k_2, \cdots, k_t$ is known in projective transformation (1), the coordinate $(x_1, x_2, \cdots, x_n)$ of point x can be determined by the $(n-t)$-residual vector $\boldsymbol{c}=(c_1, c_2, \cdots, c_{n-t})$ of the system of hyperplane intersecting line equations of any passing point x and projective transformation (1).

Proof. From projective transformation (1), the following system of equations can be obtained.

$$\begin{cases} \sum_{j=t+1}^{n} a_{1j}k_j = x_1 - b_1, \\ \sum_{j=t+1}^{n} a_{2j}k_j = x_2 - b_2, \\ \quad\vdots \\ \sum_{j=t+1}^{n} a_{nj}k_j = x_n - b_n, \end{cases} \tag{9}$$

where $b_i = \sum_{j=1}^{t} a_{ij} k_j \ (i = 1, 2, \cdots, n)$.

The coefficient matrix of the system of equations composed of $n-t$ equations in front of the system of Equations (9) is

$$D = \begin{vmatrix} a_{1,t+1} & a_{1,t+2} & \cdots & a_{1n} \\ a_{2,t+1} & a_{2,t+2} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n-t,t+1} & a_{n-t,t+2} & \cdots & a_{n-t,n} \end{vmatrix} \tag{10}$$

Because matrix A is a nonzero $(n-t)$-submatrix, so $D \neq 0$. In the coefficient determinant D, let the algebraic cofactor of element $a_{ij} \ (1 \le i \le n-t, t+1 \le j \le n)$ be A_{ij}, let

$$D_j = \begin{vmatrix} a_{1,t+1} & \cdots & b_1 & \cdots & a_{1n} \\ a_{2,t+1} & \cdots & b_2 & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n-t,t+1} & \cdots & \underset{\downarrow}{b_n} & \cdots & a_{n-t,n} \\ & & j & & \end{vmatrix}, \quad \bar{D}_j = \begin{vmatrix} a_{1,t+1} & \cdots & x_1 - b_1 & \cdots & a_{1n} \\ a_{2,t+1} & \cdots & x_2 - b_2 & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n-t,t+1} & \cdots & \underset{\downarrow}{x_n - b_n} & \cdots & a_{n-t,n} \\ & & j & & \end{vmatrix}, \tag{11}$$

represent the determinant after the *j*-th column element in D is replaced, where $j = 1, 2, \cdots, (n-t)$.

Calculate

$$\begin{aligned} \bar{D}_1 &= \begin{vmatrix} x_1 - b_1 & a_{1,t+2} & \cdots & a_{1n} \\ x_2 - b_2 & a_{2,t+2} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n-t} - b_{n-t} & a_{n-t,t+2} & \cdots & a_{n-t,n} \end{vmatrix} \\ &= \begin{vmatrix} x_1 & a_{1,t+2} & \cdots & a_{1n} \\ x_2 & a_{2,t+2} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n-t} & a_{n-t,t+2} & \cdots & a_{n-t,n} \end{vmatrix} - \begin{vmatrix} b_1 & a_{1,t+2} & \cdots & a_{1n} \\ b_2 & a_{2,t+2} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n-t} & a_{n-t,t+2} & \cdots & a_{n-t,n} \end{vmatrix} \\ &= A_{1,t+1} x_1 + A_{2,t+1} x_2 + \cdots + A_{n-t,t+1} x_{n-t} - D_1 \end{aligned} \tag{12}$$

$$\begin{aligned} k_{t+1} &= \frac{\bar{D}_1}{D} = \frac{A_{1,t+1}}{D} x_1 + \frac{A_{2,t+1}}{D} x_2 + \cdots + \frac{A_{n-t,t+1}}{D} - \frac{D_1}{D} \\ &= \sum_{i=1}^{n-t} \frac{A_{i,t+1}}{D} x_i - \frac{D_1}{D} \end{aligned} \tag{13}$$

from Gramer's law.

Similarly, we can get

$$\begin{aligned} k_{t+2} &= \sum_{i=1}^{n-t} \frac{A_{i,t+2}}{D} x_i - \frac{D_2}{D} \\ &\vdots \\ k_n &= \sum_{i=1}^{n-t} \frac{A_{in}}{D} x_i - \frac{D_{n-t}}{D} \end{aligned} \tag{14}$$

Put $k_{t+1}, k_{t+2}, \cdots, k_n$ into the next t equations in the system of Equations (9), and get the following system of equations about $x_1, x_2, \cdots, x_n$ after finishing.

$$\begin{cases} \sum_{i=1}^{n-t}\sum_{j=t+1}^{n} a_{n-t+1,j}A_{ij}x_i - Dx_{n-t+1} = \sum_{j=1}^{n-t} a_{n-t+1,t+j}D_j - Db_{n-t+1}, \\ \sum_{i=1}^{n-t}\sum_{j=t+1}^{n} a_{n-t+2,j}A_{ij}x_i - Dx_{n-t+2} = \sum_{j=1}^{n-t} a_{n-t+2,t+j}D_j - Db_{n-t+2}, \\ \vdots \\ \sum_{i=1}^{n-t}\sum_{j=t+1}^{n} a_{n,j}A_{ij}x_i - Dx_n = \sum_{j=1}^{n-t} a_{n,t+j}D_j - Db_n. \end{cases} \tag{15}$$

It is known that the $(n-t)$-residue corresponding to the $(n-t)$-residual vector $\boldsymbol{c}=(c_1,c_2,\cdots,c_{n-t})$ is

$$\begin{cases} x_1 - c_1x_n = 0, \\ x_2 - c_2x_n = 0, \\ \vdots \\ x_{n-t} - c_{n-t}x_n = 0. \end{cases} \tag{16}$$

The system of Equation (15) contains t equations and the system of Equations (16) contains $n-t$ equations. Combining the system of Equations (15) with the system of Equations (16), a linear system of equations with n equations and n unknows $x_1,x_2,\cdots,x_n$ is obtained. Since the coefficient determinant E of this system of linear equations satisfies $E=(-D)^t=(-1)^t D^t\neq 0$, there is only one set of solutions for this system of linear equations. According to Gramer's law, $x_1,x_2,\cdots,x_n$ can be obtained. Certificate completion.

If we change the condition "known $k_1,k_2,\cdots,k_t$" of Theorem 1 to the more general condition "known $k_{i_1},k_{i_2},\cdots,k_{i_t}\ (1\le i_1<i_2<\cdots<i_t\le n)$", we can get the following more general theorem according to the similar proof method of Theorem 1.

Theorem 2. Let $p\ (>n)$ be prime, Z_p be a matrix A over Z_p be a nonzero $(n-t)$-submatrix, where $t\in Z_p$, $t<n$. If $k_{i_1},k_{i_2},\cdots,k_{i_t}\ (1\le i_1<i_2<\cdots<i_t\le n)$ is known in projective transformation (1), the coordinat $(x_1,x_2,\cdots,x_n)$ of point x can be determined by the $(n-t)$-residual vector $\boldsymbol{c}=(c_1,c_2,\cdots,c_{n-t})$ of the system of hyperplane intersecting line equations of any passing point x and projective transformation (1).

3. Composition of the Scheme

Based on the one to one mapping of projective transformation and the difficulty of solving the discrete logarithm problem, this paper proposes a verifiable threshold secret sharing scheme. In this scheme, the dealer who distributes the subkey needs a bulletin board (BB). Only the dealer can modify and update the content on the BB, and others can only read or download it. This scheme is composed of two parts: the distribution phase of the subkey and the reconstruction phase of the master key.

3.1. Distribution of Subkeys

At the beginning of this stage, the dealer needs to publish some system parame-

ters. He first takes a large prime number p, finds an original root g of the module p, let Z_p be the finite field of the module p, the dealer takes a non-zero $(n-t)$-submatrix A over Z_p, and then publishes p, g and A on the BB.

Let $Z_p^* = Z_p - \{0\}$ and $P = \{P_1, P_2, \cdots, P_N\}$ be the set of n participants. The master key S is decomposed into n different shadow subkeys by the dealer over Z_p^*, *i.e.* $S = \sum_{i=1}^{n} x_i \left(x_i \in Z_p^*\right)$. Then, in the n-dimensional projective space, the dealer calculates a $(n-t)$–residual vector $\boldsymbol{c} = (c_1, c_2, \cdots, c_{n-t})$ of the system of hyperplane intersecting line equations of space point x with coordinate $(x_1, x_2, \cdots, x_n)$, publishes the $(n-t)$-residual vector $\boldsymbol{c} = (c_1, c_2, \cdots, c_{n-t})$ on the BB, and uses the projective inverse transformation (2) to find $k_i \ (1 \le i \le n)$.

The dealer distributes $k_i \ (1 \le i \le n)$ as subkeys to participants $P_i \ (1 \le i \le n)$, calculates $y_i = g^{k_i} \bmod p \ (1 \le i \le n)$, and publishes vector $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$ as verification information on the BB.

3.2. Reconstruction of Master Key

When any t members $P_{j_1}, P_{j_2}, \cdots, P_{j_t}$ of n participants gather together to recover the master key S, they need to verify each other's subkeys. First calculate $g^{k_{j_i}} \bmod p \equiv h_{j_i} \ (1 \le i \le t)$, then check whether the corresponding y_{j_i} on the BB and h_{j_i} are consistent. If they are consistent, the subkey submitted by members is true. Otherwise, if some submits a false subkey, the corresponding y_{j_i} and h_{j_i} are inconsistent.

The recovery process of the master key is shown below. Let's set the transformation matrix to

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}. \tag{17}$$

After the verification is passed, the t members calculate the following formula together

$$\begin{pmatrix} a_{1j_1} & a_{1j_2} & \cdots & a_{1j_t} \\ a_{2j_1} & a_{2j_2} & \cdots & a_{2j_t} \\ \vdots & \vdots & & \vdots \\ a_{nj_1} & a_{nj_2} & \cdots & a_{nj_t} \end{pmatrix} \begin{pmatrix} k_{j_1} \\ k_{j_2} \\ \vdots \\ k_{j_t} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{t} k_{j_i} a_{1j_i} \\ \sum_{i=1}^{t} k_{j_i} a_{2j_i} \\ \vdots \\ \sum_{i=1}^{t} k_{j_i} a_{nj_i} \end{pmatrix}. \tag{18}$$

By projective transformation (1), a system of equations about unknown subkeys owned by the rest members of the participant set is generated, that is.

$$\begin{cases} \sum\limits_{1\le h\le n, h\ne j_i, 1\le i\le t} k_h a_{1h} = x_1 - \sum\limits_{i=1}^{t} k_{j_i} a_{1j_i} \\ \sum\limits_{1\le h\le n, h\ne j_i, 1\le i\le t} k_h a_{2h} = x_2 - \sum\limits_{i=1}^{t} k_{j_i} a_{2j_i} \\ \vdots \\ \sum\limits_{1\le h\le n, h\ne j_i, 1\le i\le t} k_h a_{nh} = x_n - \sum\limits_{i=1}^{t} k_{j_i} a_{nj_i} \end{cases} \tag{19}$$

This system of equations is considered to be composed of n equations with $n-t$ unknowns k_h $(1\le h\le n,\ h\ne j_i,\ i=1,2,\cdots,t)$, by eliminating these k_h, t equations $\sum\limits_{i=1}^{n}\xi_{ij}x_i = d_j$ about unknowns $x_1, x_2, \cdots, x_n$ can be obtained, where $j=1,2,\cdots,t$. Combined with the $(n-t)$-residue (16) corresponding to the $(n-t)$-residual vector published on the BB, the following system of equations are formed,

$$\begin{cases} \sum\limits_{i=1}^{n}\xi_{i1}x_i = d_1, \\ \quad\vdots \\ \sum\limits_{i=1}^{n}\xi_{it}x_i = d_t, \\ x_1 - c_1 x_n = 0, \\ \quad\vdots \\ x_{n-t} - c_{n-t}x_n = 0. \end{cases} \tag{20}$$

It can be seen from Theorem 2 that the unique solution $x_1, x_2, \cdots, x_n$ can be obtained by solving this system of equations, and then the master key $S = \sum\limits_{i=1}^{n} x_i$ can be recovered.

3.3. Give an Example

The implementation process of this scheme can be clearly shown by the following example.

In the initial stage, the dealer takes the prime number $p=11$, sets Z_{11} as the finite field of module 11, the number of participants $n=5$, the threshold value $t=3$, and selects matrix

$$A = \begin{pmatrix} 1 & 4 & 7 & 3 & 2 \\ 3 & 0 & 4 & 1 & 10 \\ 5 & 2 & 8 & 5 & 3 \\ 2 & 7 & 5 & 4 & 6 \\ 1 & 6 & 2 & 0 & 8 \end{pmatrix}. \tag{21}$$

It is proved that $|A|\ne 0$ and any 2-order minor of A is not equal to zero, so A is a nonzero 2-submatrix.

Set the master key $S=7$. In the subkey distribution stage, the dealer decomposes S into $S=2+7+5+1+3$ over Z_{11} and obtain shadow subkeygroup

$(x_1, x_2, x_3, x_4, x_5) = (2,7,5,1,3)$. Then, the inverse projective transformation (2) is used for the following calculation.

$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \end{pmatrix} = A^{-1} \begin{pmatrix} 2 \\ 7 \\ 5 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \\ 10 \\ 3 \\ 7 \end{pmatrix}. \tag{22}$$

From the geometric meaning of point plane combination, the hyperplane beam equation with point $x(2,7,5,1,3)$ as the beam center is

$$2\xi_1 + 7\xi_2 + 5\xi_3 + \xi_4 + 3\xi_5 = 0. \tag{23}$$

In formula (23), we take four linearly independent vectors about $(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5)$, which are $(1,0,0,0,3)$, $(0,1,0,0,5)$, $(0,0,1,0,2)$, $(0,0,0,1,7)$ respectively, and then we get a system of equations of hyperplane intersecting line passing through point x.

$$\begin{cases} x_1 + 3x_5 = 0, \\ x_2 + 5x_5 = 0, \\ x_3 + 2x_5 = 0, \\ x_4 + 7x_5 = 0. \end{cases} \tag{24}$$

Take a 2-residue of this equations

$$\begin{cases} x_1 = 8x_5, \\ x_2 = 6x_5, \end{cases} \tag{25}$$

its corresponding 2-residual vector is $\boldsymbol{c} = (8,6)$.

We know that 2 is the original root of module 11. Take $g = 2$ and calculate $2^5 \bmod 11 \equiv 10$, $2^9 \bmod 11 \equiv 6$, $2^{10} \bmod 11 \equiv 1$, $2^3 \bmod 11 \equiv 8$, $2^7 \bmod 11 \equiv 7$ respectively, so as to construct the verification information vector $\boldsymbol{y} = (10,6,1,8,7)$.

After the above preparations, the dealer distributes $k_1 = 5$, $k_2 = 9$, $k_3 = 10$, $k_4 = 3$, $k_5 = 7$ as subkeys to five participants P_1, P_2, P_3, P_4, P_5, and publishes the prime number $p = 11$, the original root $g = 2$, the threshold value $t = 3$, the transformation matrix A, the 2-residual vector $\boldsymbol{c} = (8,6)$ and the verification information vector $\boldsymbol{y} = (10,6,1,8,7)$ on the BB.

In the reconstruction phase of the master key, any three members of the five participants gather together. Let's assume that P_1, P_3, P_4 gather together. They first verify whether the key k_1, k_3, k_4 they have taken out is true. They only need to calculate $2^{k_1} \bmod p$, $2^{k_3} \bmod p$, $2^{k_4} \bmod p$ separately and compare the calculation results with the corresponding components in the verification information vector $\boldsymbol{y}$ to see whether the three corresponding quantities are consistent. If the three corresponding quantities are all consistent, then k_1, k_3, k_4 is true. If there is inconsistency, then the corresponding members provide false subkey.

In the case of verifying that all the subkeys provided are correct, these three people use projective transformation (1) to list the following matrix equation,

$$A\begin{pmatrix}5\\k_2\\10\\3\\k_5\end{pmatrix}=\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}. \tag{26}$$

Turn (26) into a system of linear equations

$$\begin{cases}4k_2+2k_5=x_1+4,\\10k_5=x_2+8,\\2k_2+3k_5=x_3+1,\\7k_2+6k_5=x_4+5,\\6k_2+8k_5=x_5+8.\end{cases} \tag{27}$$

After eliminating k_2, k_5 from (27), we get the following system of equations about the unknown number x_1, x_2, x_3, x_4, x_5,

$$\begin{cases}6x_1+9x_2+10x_3=4,\\x_1+8x_2+x_4=4,\\7x_1+6x_2+10x_5=9.\end{cases} \tag{28}$$

Combined with the 2-residual vector $\boldsymbol{c}=(8,6)$ on the BB extened system of Equations (28):

$$\begin{cases}6x_1+9x_2+10x_3=4,\\x_1+8x_2+x_4=4,\\7x_1+6x_2+10x_5=9,\\x_1=8x_5,\\x_2=6x_5.\end{cases} \tag{29}$$

These three members solve the system of Equations (29), get $x_1=2$, $x_2=7$, $x_3=5$, $x_4=1$, $x_5=3$, and then calculate $\sum_{i=1}^{5}x_i=7$ to get the master key $S=7$.

4. Analysis of the Scheme

Under the premise that the dealer is reliable in subkey distribution, the following conclusions are drawn.

Theorem 3. The scheme is a complete secret sharing scheme, and the information rate can be up to 1.

Proof. Any t participants can establish a system of equations by presenting their subkeys. According to theorem 2. This system of equations can uniqely determine the coordinate $(x_1,x_2,\cdots,x_n)$ of shadow subkey point x. If less than t participants gather togetuer to provide their subkeys. The number of equations in the system of equations with structure (20) is less than the number n of the unknown number $x_1,x_2,\cdots,x_n$, such a system of equations has numerous solutions, and it is difficult to find the shadow subkey point x. So less than t participants can not recover the master key. The information rate of a secret sharing scheme is defined as $\rho=\min(\rho_i:1\le i\le n)$ where $\rho_i=\frac{\lg|Z_p|}{\lg|S_i|}$, and

$S_i\ (1 \le i \le n)$ is the set of all possible subkeys that the participant $P_i\ (1 \le i \le n)$ may receive [24]. In this scheme, each participant only needs to save a subkey belonging to Z_p, at this time, the information rate can reach the maximum value of 1. Certificate completion.

Theorem 4. The probability that the fraudster obtains the master key through public information is $1/p$.

Proof. According to the design requirements of the scheme, the public information that fraudsters can obtain includes n–order nonzero $(n-t)$-submatrix A, large prime number p and its original root g, verification vector $\boldsymbol{y}$, and $(n-t)$-residual vector $\boldsymbol{c}$. If a fraudster solves $g^{k_i} \bmod p = y_i$, he will encounter a difficult discrete logarithm problem, If the fraudster passes the $(n-t)$–residual system of equation (16) corresponding to the $(n-t)$–residual vector, but the rank of the coefficient matrix of this system of equations is $n-t$, which is smaller than the number n of unknown numbers of the system of equations, then the fraudster cannot determin its unique solution. In conclusion, it is impossible for the fraudster to obtain the subkey of the participant, and thus the master key S. In this way, the only way for fraudsters to obtain the master key S is to guess randomly from Z_p, according to the knowledge of probability theory, it can be considered that the master key S is selected with equal probability in Z_p, so the probability of guess success is very small, which is $1/p$. Certificate completion.

In the practical scheme, the selected p is a large prime number and $1/p$ is almost zero. According to Theorem 4, it is impossible to recover the master key S only through the information on the BB. In addition, the fraud detection of this scheme is based on the difficulty of discrete logarithm problem. Anyone can verify whether the subkey provided by himself or others is correct through the verification vector $\boldsymbol{y}$, so this scheme is secure and antifraud.

When we analyze the efficiency of the scheme, we mainly depend on the number of power operations performed in the scheme. The less the number of power operations is, the higher the efficiency is. The design of this scheme is unique. In addition to the t power operations in the verification process, other calculations are mainly some basic linear operations, matrix operations and determinant operations. The performance of the main body of the scheme mainly depends on the calculation of the determinant, which is also very convenient. Moreover, Wiedemann [25] proposes a kind of determinant probability algorithm, which can effectively improve the calculation of the determinant over the finite field. The algorithm using Wiedemann's will further improve the operation performance of this scheme.

5. Conclusion

Verifiable secret sharing scheme is an important part of secure cryptographic protocol and an effective method to solve the safe storage, legal recovery and utilization of important sensitive information. Therefore, the research on verifiable

secret sharing and its application has an important theoretical and application value. Based on the projective transformation in n-dimensional projective space, a verifiable (t,n)-threshold secret sharing scheme is proposed by using the structure of solutions of linear equations and the difficulty of discrete logarithm problem. Each participant can verify the correctness of the subkey provided by other participants before the master key is restored. The scheme can effectively identify the fraudsters, and the fraudsters can only cheat by guessing. The probability of successful fraud is only $1/p$, and the maximum information rate of the scheme can be 1. Compared with the existing secret sharing scheme, the scheme has the advantages of exquisite design, small computation complexity and less secret information. The analysis shows that the scheme is a secure and effective scheme with practical application value. This scheme is based on the threshold access structure, how to use the idea of this paper to design its secure secret sharing scheme remains to be further explored.

Conflicts of Interest

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

References

[1] Brickell, E.F. and Daveport, D.M. (1991) On the Classification of Idea Secret Sharing Scheme. *Journal of Cryptology*, **4**, 123-134. https://doi.org/10.1007/BF00196772

[2] Fouque, P.A., Poupard, G. and Stern, J. (2000) Sharing Decryption in the Context of Voting or Lotteries. In: *Proceeding of Financial Cryptography* 2000, Springer Verlag, Berlin, 90-94. https://doi.org/10.1007/3-540-45472-1_7

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

[4] Blakley, G. (1979) Safeguarding Cryptographic Keys. *Conference Proceedings* 1979 *National Computer Conference*, New York, 4-7 June 1979, 242-268. https://doi.org/10.1109/MARK.1979.8817296

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

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

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

[8] Liu, H.P. and Lv, X.Q. (2004) General Secret Sharing Schemes Based on One-Way Function. *Journal of China Institute of Communications*, **25**, 39-44.

[9] Li, B. (2015) Threshold Scheme for Different Access Clusters Based on Vector Space. *Journal on Communications*, **36**, 67-72.

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

[11] Bouyuklieva, S. and Varbanov, Z. (2011) Some Connections between Self-Dual Codes, Comlinatorial Designs and Secret Sharing Schemes. *Advances in Mathematics of Communications*, **5**, 191-198. https://doi.org/10.3934/amc.2011.5.191

[12] Li, B. (2016) A Geometric Design of Threshold Secret Sharing Scheme on Dual Colonies. *Computer Applications and Software*, **33**, 314-318.

[13] Lin, K.S., Lin, C.H. and Chen, T.H. (2014) Distortionless Visual Multi-Secret Sharing Based on Random Grid. *Information Sciences*, **288**, 330-346. https://doi.org/10.1016/j.ins.2014.07.016

[14] Shao, J. (2014) Efficient Verifiable Multi-Secret Sharing Scheme Based on Hash Function. *Information Sciences*, **278**, 104-109. https://doi.org/10.1016/j.ins.2014.03.025

[15] Pei, Q.Q., Ma, J.F. and Pang, L.J. (2010) An Identity (ID)-Based and Self-Certified Secret Sharing Scheme. *Chinese Journal of Computers*, **33**, 152-156. https://doi.org/10.3724/SP.J.1016.2010.00152

[16] Tian, Y.L., Ma, J.F. and Peng, C.G. (2011) Information Theoretic Secure Verifiable Secret Sharing Scheme on Elliptic Curve Group. *Journal on Communications*, **32**, 96-102.

[17] Liu, Y., Hao, Y.J. and Pang, L.J. (2010) Verifiable Secret Sharing Scheme Based on ELGamal Cryptosystem. *Computer Science*, **37**, 80-82.

[18] Zhang, X. (2013) Verifiable Multi-Secret Sharing Scheme Based on Linear One-Way Function. *Journal of Computer Applications*, **33**, 1391-1393. https://doi.org/10.3724/SP.J.1087.2013.01391

[19] Tan, X.Q. and Wang, Z.G. (2009) A Verifiable Multiple Secret Sharing Scheme Based on Hermite Interpolation Polynomial. *Journal of Mathematics* (*PRC*), **29**, 367-372.

[20] Wang, F. and Zhang, J.Z. (2008) Dynamic Verified Threshold Multi-Secret Sharing Scheme Based on RSA Cryptosystem. *Application Research of Computers*, **25**, 1806-1811.

[21] Ma, Z., Ma, Y. and Huang, X.H. (2020) Applying Cheating Identifiable Secret Sharing Scheme in Multimedia Security. *EURASIP Journal on Image and Video Processing*, **2020**, Article No. 42. https://doi.org/10.1186/s13640-020-00529-z

[22] Lu, Y.J. (2020) Quantum Secret Sharing via Cavity QED. *International Journal of Theoretical Physics*, **59**, 3324-3328. https://doi.org/10.1007/s10773-020-04591-1

[23] Li, B. (2019) Group Structure of Special Parabola and Its Application in Cryptography. *Applied and Computational Mathematics*, **8**, 88-94. https://doi.org/10.11648/j.acm.20190806.11

[24] Maarek, Y.S., Berry, D.M. and Kaiser, G.E. (1991) An Information Retrieval Approach for Automatically Constructing Software Libraries. *IEEE Transactions on Software Engineering*, **17**, 800-814. https://doi.org/10.1109/32.83915

[25] Wiedemann, D.H. (1981) Solving Sparse Linear Equations over Finite Fields. *IEEE Transaction on Information Theory*, **32**, 54-62. https://doi.org/10.1109/TIT.1986.1057137