Scientific Research Publishing

Applied Mathematics, 2021, 12, 1021-1030
https://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

Verifiable Secret Sharing Scheme Based on the Plane Parametric Curve

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 the Plane Parametric Curve. *Applied Mathematics*, **12**, 1021-1030.
https://doi.org/10.4236/am.2021.1211066

Received: October 11, 2021
Accepted: November 27, 2021
Published: November 30, 2021

Abstract

Verifiable secret sharing is a special kind of secret sharing. In this paper, A secure and efficient threshold secret sharing scheme is proposed by using the plane parametric curve on the basis of the principle of secret sharing. And the performance of this threshold scheme is analyzed. The results reveal that the threshold scheme has its own advantage of one-parameter representation for a master key, and it is a perfect ideal secret sharing scheme. It can easily detect cheaters by single operation in the participants so that the probability of valid cheating is less than $1/p$ (where p is a large prime).

Keywords

Plane Parameter Curve, Threshold Scheme, Verifiable Secret Sharing, Cheater, Information Rate, Participating Members

1. Introduction

In the field of information security, as an important means of key management, the basic principle of secret sharing is to split the master key into many subkeys, and then distribute these subkeys to all members of the set $P=\{P_1,P_2,\cdots,P_n\}$ composed of a limited number of participants. After some members of the authorization set show their subkeys, they can reconstruct the original master key through a series of calculations. But other members of the unauthorized set cannot recover the master key. Therefore, in essence, secret sharing is an operation process for the distribution, preservation and recovery of secret keys. Using the secure sharing scheme in the secret system can not only reduce the burden of the key holder due to the loss and damage of the system key, but also reduce the success rate of the adversary's malicious attack on the key.

The earliest secret sharing is (r,n)-threshold secret sharing, which was pro-

posed by Shamir [1] and Blakley [2] respectively in 1979. Their (r,n)-threshold secret sharing schemes are based on the (r,n)-threshold access structure on the authorization set composed of at least r members. The difference is the (r,n)-threshold scheme of Shamir is realized by constructing a polynomial function over a finite field, and distributing each numerical point coordinate on the function curve as a subkey to the members of each authorization set, and taking the constant term of the polynomial as the master key; The (r,n)-threshold scheme of Blakley is realized by constructing n common hyperplanes in multidimensional space, the coordinates of each hyperplane are regarded as a subkey and distributed to the members of each authorization set, and the coordinates of the common intersection of these hyperplanes are regarded as the master key. The results show that the Shamir scheme with the algebraic method is a complete and ideal scheme, while the Blakley scheme with geometric method is a complete and nonideal scheme. Therefore, the information rate of the Blakley scheme is lower than that of the Shamir scheme, but it has the advantage that any subkey vector that can determine the master key point is linearly independent of each other, so it is difficult to guess. In addition to the number method proposed by Shamir and the shape method proposed by Blakley, the methods of constructing (r,n)-threshold secret sharing scheme are followed by the method of Asmuth-Bloom [3] based on Chinese remainder theorem, the method of Karnin-Green-Hellman [4] based on matrix multiplication, and the design ideas of the above-mentioned threshold schemes are improved according to different application requirements, and a variety of variants of threshold schemes are proposed [5] [6] [7] [8].

The efficiency of a secret sharing scheme depends on its information rate. It is often said that the information rate of the secret sharing scheme is the ratio of the information amount of the master key to the information amount of the subkeys owned by the participating members. When the amount of information of the master key is a fixed value, from the standpoint of the dealer in charge of the master key, the less the amount of information given to the participating members, the better the security of the secret sharing scheme can be maintained. From the perspective of participants, it is easier to keep the subkey with less information than that with more information. Therefore, a good secret sharing scheme can reduce the amount of subkey information as much as possible. It can be seen that a high information rate is the pursuit of cryptographers. The higher the information rate of the secret sharing scheme, the smaller the degree of data diffusion is. Therefore, people hope to build a secret sharing scheme with the highest information rate. When the information rate reaches the value 1, the corresponding secret sharing scheme will become an ideal secret sharing scheme.

As a technical means, the secret sharing scheme based on a certain mathematical thinking method mentioned above can only solve the most basic problems in key management, but in the actual application environment, it cannot judge whether there is cheating behavior, and it is difficult to prevent some members

of the secret sharing scheme from cheating by using a fake subkey to participate in the construction of the master key. Whether it is the cheating of a single member or the collusion of multiple members, it will cause other honest members to get the wrong master key, which will bring great threat and damage to the secret sharing scheme. Therefore, in order to solve the problem of cheating, people need to study how to set up the anti-cheating function of the secret sharing scheme.

As early as 1981, McEliece and Sarwate [9] designed a threshold secret sharing scheme to prevent cheating by using error-correcting code theory. This scheme enables $r+2e$ members with at most e cheaters to correctly construct the master key. If some parameter conditions are given, then the cheating prevention secret sharing scheme can detect the cheating behavior with high probability [10] [11] [12] [13]. If the cheater has supercomputing power, but the probability of success is not more than a small fixed percentage, so we can say that the secret sharing scheme is unconditionally secure in preventing deception [14]. At present, for the existing secret sharing schemes which can detect deception, when a member reconstructs and recovers the master key, it is generally necessary to use some mathematical verification formula to test the subkeys provided by all members one by one. In this way, we can find out which members are cheaters, but when all members are honest, the cost of the verification process is not reduced, which leads to unnecessary waste of resources. This paper proposes a verifiable secret sharing scheme based on the plane parameter curve. It only needs to put the subkeys provided by each member together and check once to determine whether there are cheaters in these members. If it exists, it will terminate the reconstruction immediately, otherwise, it will continue, which greatly improves the efficiency of the secret sharing scheme.

2. Design of the Secret Sharing Scheme

Let F_p be a finite field of p elements and p be a large prime number, let:

$$F_p = \{0,1,2,\cdots,p-1\},\quad F_p^* = F_p - \{0\}.$$

The parametric curve Γ on affine plane $A^2(F_p)$ is introduced:

$$\Gamma: \begin{cases} x = f(t), \\ y = g(t), \end{cases}$$

where $f(t)$ and $g(t)$ are polynomials on F_p.

The parametric curve Γ satisfies the following additional conditions:

1) For any $t \in F_p$, there is $(x,y) \in F_p^* \times F_p^*$.

2) For any $t_1, t_2 \in F_p$, let:

$$\begin{cases} x_1 = f(t_1), \\ y_1 = f(t_1), \end{cases} \qquad \begin{cases} x_2 = f(t_2), \\ y_2 = f(t_2). \end{cases}$$

If $t_1 \neq t_2$, then $x_1^{-1} y_1 \neq x_2^{-1} y_2$.

Let D be the distributor of the subkeys, that is, the dealer, and $P=\{P_1,P_2,\cdots,P_n\}$ be the set of n participating members.

Firstly, the dealer D secretly chooses the master key $k\in F_p$, decomposes k into r different numbers $k_1,k_2,\cdots,k_r$ on F_p^*, that is, $k=k_1+k_2+\cdots+k_r$, $\{k_1,k_2,\cdots,k_r\}\subset F_p^*$, and then constructs the homogeneous formula:

$$\begin{aligned} z=\varphi(t)&=k_1x^{r-1}+k_2x^{r-2}y+k_3x^{r-3}y^2+\cdots+k_ry^{r-1}\\ &=k_1f^{r-1}(t)+k_2f^{r-2}(t)g(t)+k_3f^{r-3}(t)g^2(t)+\cdots+k_rg^{r-1}(t)\end{aligned}$$

The dealer D secretly selects n different parameters on F_p to calculate $z_i=\varphi(t_i)\bmod p$ so that any r numbers of $z_1,z_2,\cdots,z_n$ are mutually prime, that is, $\gcd(z_{i_1},z_{i_2},\cdots,z_{i_r})=1$.

The dealer D distributes z_i to the corresponding i-th member $P_i\,(1\le i\le n)$ as his subkey.

If r participating members $P_{i_1},P_{i_2},\cdots,P_{i_r}$ are going to reconstruct the master key k, they show their subkeys $z_{i_1},z_{i_2},\cdots,z_{i_r}$ respectively, and establish the following linear equations on F_p,

$$\begin{cases} k_1x_{i_1}^{r-1}+k_2x_{i_1}^{r-2}y_{i_1}+k_3x_{i_1}^{r-3}y_{i_1}^2+\cdots+k_ry_{i_1}^{r-1}=z_{i_1},\\ k_1x_{i_2}^{r-1}+k_2x_{i_2}^{r-2}y_{i_2}+k_3x_{i_2}^{r-3}y_{i_2}^2+\cdots+k_ry_{i_2}^{r-1}=z_{i_2},\\ \vdots\\ k_1x_{i_r}^{r-1}+k_2x_{i_r}^{r-2}y_{i_r}+k_3x_{i_r}^{r-3}y_{i_r}^2+\cdots+k_ry_{i_r}^{r-1}=z_{i_r}. \end{cases} \tag{1}$$

where $x_{i_j}=f(t_{i_j}),y_{i_j}=g(t_{i_j}),1\le j\le r$.

The system of equations is a linear system of equations consisting of r equations with r variables $(k_1,k_2,\cdots,k_r)$ and the coefficient matrix H is a generalized Vander monde matrix on F_p, obviously, under the additional condition of parameter curve Γ, the matrix $H\ne 0$. Since $\gcd(H,p)=1$, the system of equations has a unique solution on F_p, that is:

$$k_j=H_jH^{-1}\bmod p,1\le j\le r$$

where:

$$H=\begin{vmatrix} x_{i_1}^{r-1} & x_{i_1}^{r-2}y_{i_1} & \cdots & y_{i_1}^{r-1}\\ x_{i_2}^{r-1} & x_{i_1}^{r-2}y_{i_2} & \cdots & y_{i_2}^{r-1}\\ \vdots & \vdots & \ddots & \vdots\\ x_{i_r}^{r-1} & x_{i_r}^{r-2}y_{i_r} & \cdots & y_{i_r}^{r-1} \end{vmatrix},\quad H_j=\begin{vmatrix} x_{i_1}^{r-1} & z_{i_1} & \cdots & y_{i_1}^{r-1}\\ x_{i_2}^{r-1} & z_{i_2} & \cdots & y_{i_2}^{r-1}\\ \vdots & \vdots & \ddots & \vdots\\ x_{i_r}^{r-1} & z_{i_r} & \cdots & y_{i_r}^{r-1} \end{vmatrix}$$

$\uparrow$

column j

Then the r participating members calculate:

$$k=(k_1+k_2+\cdots+k_r)\bmod p,$$

to recover the master key.

For this (r,n)-threshold scheme, a problem can be raised: whether there are members who provide false subbeys in the stage of r participating members re-

constructing the master key, that is, how each member can judge whether someone in other members has cheated and provided untrue subkeys, which requires the dealer to give parameter or parameter groups for verification, Let's first introduce the following two lemmas.

Lemma 1. Let $r \geq 2$, N and $a_i \left(i = 1, 2, \cdots, r\right)$ be positive integers, and $\gcd\left(a_1, a_2, \cdots, a_r\right) = 1$. There is a positive integer $\phi\left(a_1, a_2, \cdots, a_r\right)$ only related to $a_1, a_2, \cdots, a_r$ when $N > \phi\left(a_1, a_2, \cdots, a_r\right)$ the equation:

$$a_1 b_1 + a_2 b_2 + \cdots + a_r b_r = N \tag{2}$$

has a set of nonnegative integer solutions $\left(b_1, b_2, \cdots, b_r\right)$.

Proof. Mathematical induction is used for r.

When $r = 2$ we choose $\phi\left(a_1, a_2\right) = \left(a_1 - 1\right)\left(a_2 - 1\right) - 1$, because:

$$a_1 b_1 + a_2 b_2 = N, \tag{3}$$

where $\gcd\left(a_1, a_2\right) = 1$, all solutions of Equation (3) can be expressed as:

$$\begin{cases} b_1 = b_1' + a_2 u, \\ b_2 = b_2' - a_1 u, \end{cases}$$

where b_1', b_2' are a group of special solutions of Equation (3), and u is any integer.

Obviously, u can be taken so that $0 \leq b_2 = b_2' - a_1 u < a_1$, *i.e.* $0 \leq b_2' - a_1 u \leq a_1 - 1$ when $N > \phi\left(a_1, a_2\right) = a_1 a_2 - a_1 - a_2$, the following is true:

$$\left(b_1' + a_2 u\right) a_1 = N - \left(b_2' - a_1 u\right) a_2 > a_1 a_2 - a_1 - a_2 - \left(a_1 - 1\right) a_2 = -a_1,$$

that is:

$$b_1' + a_2 u > -1.$$

Therefore, for the above u, there is:

$$b_1 = b_1' + a_2 u \geq 0.$$

So when $N > a_1 a_2 - a_1 - a_2$ there is an integer solution $b_1 \geq 0, b_2 \geq 0$ in (3).

Let's suppose that the lemma holds for $r - 1$ elements. It is proved that the lemma holds for r elements.

Let $\gcd\left(a_1, a_2, \cdots, a_{r-1}\right) = d$, $a_i = a_i' d \left(1 \leq i \leq r - 1\right)$, and $\gcd\left(d, a_r\right) = 1$ be obtained from $\gcd\left(a_1, a_2, \cdots, a_r\right) = 1$, therefore there exists $0 \leq c_r \leq d - 1$ such that $a_r c_r \equiv N \bmod d$.

Let $b_r = c_r$, and from (2) we can get:

$$a_1' b_1 + a_2' b_2 + \cdots + a_{r-1}' b_{r-1} = \frac{N - a_r c_r}{d} \tag{4}$$

Since $\gcd\left(a_1', a_2', \cdots, a_r'\right) = 1$, by inductive assumption, there is an integer $\phi'\left(a_1', a_2', \cdots, a_{r-1}'\right)$, when $\frac{N - a_r c_r}{d} \geq \frac{N - a_r\left(d - 1\right)}{d} > \phi'\left(a_1', a_2', \cdots, a_{r-1}'\right)$, the indefinite Equation (4) has a set of nonnegative integer solutions:

$$b_1 = c_1 \geq 0,\ b_2 = c_2 \geq 0,\ \cdots,\ b_{r-1} = c_{r-1} \geq 0$$

That is, when $N > d\phi'(a_1', a_2', \cdots, a_{r-1}') + a_r(d-1) = \phi(a_1, a_2, \cdots, a_r)$, the indefinite Equation (2) has a set of nonnegative integer solutions $(b_1, b_2, \cdots, b_r)$.

This completes the proof.

If we take $a_j = z_{i_j}\ (1 \le j \le r), N = 1 + m(p-1)$, where m is a sufficiently large positive integer such that $N > \phi(z_{i_1}, z_{i_2}, \cdots, z_{i_r})$ then the indefinite equation:

$$z_{i_1} b_1 + z_{i_2} b_2 + \cdots + z_{i_r} b_r = 1 + m(p-1) \tag{5}$$

has a set of nonnegative integer solution $b_1 \ge 0, b_2 \ge 0, \cdots, b_r \ge 0$.

Dealer D selects a primitive root g of module p calculates:

$$\delta_1 \equiv g^{b_1} \bmod p, \delta_2 \equiv g^{b_2} \bmod p, \cdots, \delta_r \equiv g^{b_r} \bmod p.$$

and then exposes array $(g, \delta_1, \delta_2, \cdots, \delta_r)$ as the verification parameter group of participants.

Lemma 2. If a is the primitive root of module n, then $a^s \equiv a^t \bmod n$ if and only if $s \equiv t \bmod \varphi(n)$, where $\varphi(n)$ is an Euler function, and $\varphi(p) = p-1$ when n is a prime p.

Proof. From the condition, we get $a^{s-t} \equiv 1 \bmod n$, so there is $\delta_n(a) \mid s-t$ where $\delta_n(a)$ is the exponent of a to module n, thus we get:

$$s \equiv t \bmod \delta_n(a).$$

Since a is the primitive root of module n, that is $\delta_n(a) = \varphi(n)$, thus:

$$s \equiv t \bmod \varphi(n).$$

The above proof process is reverible, which completes the proof of **Lemma 2**.

According to these two lemmas, we can get the following judgment theorem.

Theorem 1. For the subkey group $(\overline{z}_{i_1}, \overline{z}_{i_2}, \cdots, \overline{z}_{i_r})$ provided by the participating member in P, if $\delta_1^{\overline{z}_{i_1}} \delta_2^{\overline{z}_{i_2}} \cdots \delta_r^{\overline{z}_{i_r}} \bmod p \ne g$, then there must be cheaters in the participating member set.

Proof.

$$z_{i_1} b_1 + z_{i_2} b_2 + \cdots + z_{i_r} b_r \equiv 1 \bmod (p-1)$$

can be obtained, and:

$$g^{z_{i_1} b_1 + z_{i_2} b_2 + \cdots + z_{i_r} b_r} \bmod p = g$$

can be obtained from **Lemma 2**.

If there is no cheater in the members, then:

$$(\overline{z}_{i_1}, \overline{z}_{i_2}, \cdots, \overline{z}_{i_r}) = (z_{i_1}, z_{i_2}, \cdots, z_{i_r}),$$

thus:

$$\delta_1^{\overline{z}_{i_1}} \delta_2^{\overline{z}_{i_2}} \cdots \delta_r^{\overline{z}_{i_r}} \bmod p = g^{z_{i_1} b_1 + z_{i_2} b_2 + \cdots + z_{i_r} b_r} \bmod p = g.$$

According to the equivalent logical relationship between the original proposition and its converse proposition, we get that if the subkey group $(\overline{z}_{i_1}, \overline{z}_{i_2}, \cdots, \overline{z}_{i_r})$ provided by the participating members satisfies $\delta_1^{\overline{z}_{i_1}} \delta_2^{\overline{z}_{i_2}} \cdots \delta_r^{\overline{z}_{i_r}} \bmod p \ne g$, then $(\overline{z}_{i_1}, \overline{z}_{i_2}, \cdots, \overline{z}_{i_r}) \ne (z_{i_1}, z_{i_2}, \cdots, z_{i_r})$, it means that there must be cheaters in the participating members. This completes the proof of **Theorem 1**.

For example, let $g=13, p=19$, when $z_{i_1}=7, z_{i_2}=3, z_{i_3}=11$, there is $b_1=15, b_2=23, b_3=17$, so that $z_{i_1}b_1+z_{i_2}b_2+z_{i_3}b_3=361\equiv 1(\mathrm{mod}18)$.

At this time, there is:

$$\delta_1=g^{b_1}=13^{15}\equiv 8(\mathrm{mod}19),$$

$$\delta_2=g^{b_2}=13^{23}\equiv 14(\mathrm{mod}19),$$

$$\delta_3=g^{b_3}=13^{17}\equiv 3(\mathrm{mod}19)$$

and:

$$\delta_1^{z_{i_1}}\delta_2^{z_{i_2}}\delta_3^{z_{i_3}}=8^7\cdot 14^3\cdot 3^{11}\equiv 13=g(\mathrm{mod}19).$$

If P_{i_2} in the participant submits a false subkey $\overline{z}_{i_2}=2$, then:

$$\delta_1^{z_{i_1}}\delta_2^{\overline{z}_{i_2}}\delta_3^{z_{i_3}}=8^7\cdot 14^2\cdot 3^{11}\equiv 5\neq g(\mathrm{mod}19).$$

3. Performance Analysis of the Secret Sharing Scheme

Theorem 2. The (r,n)-threshold scheme is a complete and ideal secret sharing scheme.

Proof. If any r members $P_{i_1}, P_{i_2}, \cdots, P_{i_r}$ take out their respective subkeys together, then we can build linear Equations (1). Obviously, there are r variables in this system of equations.

According to the corresponding relationship of each subkey, it is necessary for r members to join together to construct a linear system of equations containing r equations, so as to obtain the unique solution containing the master key and this solution also satisfies the equation generated by the subkeys held by other members. Therefore, at least members must be together to recover the shared master key k and less than r members cannot find the unique solution of the linear equations, so no information of the master key k can be obtained. In conclusion, the (r,n)-threshold scheme is a complete secret sharing scheme.

Let $S=F_p$, master key $k\in S$, since each participant has only one subkey of secret value, and all values are in S, we can calculate the information rate [15]:

$$\rho=\frac{\log_2|S|}{\log_2|S|}=1.$$

So the (r,n)-threshold scheme is also an ideal secret sharing scheme. It's over.

Theorem 3. For this (r,n)-threshold secret sharing scheme, the probability of success of h ($1\le h<r$) cheaters in the participating members is $\frac{1}{p}-\frac{1}{p^h}$.

Proof. Suppose r members $P_{i_1}, P_{i_2}, \cdots, P_{i_r}$ are about to reconstruct and recover the master key k in which there are h ($1\le h<r$) cheaters.

Let $P_{i_1}, P_{i_2}, \cdots, P_{i_h}$ be cheaters and $P_{i_{h+1}}, P_{i_{h+2}}, \cdots, P_{i_r}$ be honest people. If $P_{i_1}, P_{i_2}, \cdots, P_{i_h}$ use false data $z'_{i_1}, z'_{i_2}, \cdots, z'_{i_h}$ to impersonate the real subkeys $z_{i_1}, z_{i_2}, \cdots, z_{i_h}$ respectively, and $P_{i_{h+1}}, P_{i_{h+2}}, \cdots, P_{i_r}$ show their correct subkeys, then

the equations to obtain the reconstructed master key k from the public information become:

$$\begin{cases} k_1 x_{i_1}^{r-1} + k_2 x_{i_1}^{r-2} y_{i_1} + k_3 x_{i_1}^{r-3} y_{i_1}^2 + \cdots + k_r y_{i_1}^{r-1} = z'_{i_1}, \\ \vdots \\ k_1 x_{i_h}^{r-1} + k_2 x_{i_h}^{r-2} y_{i_h} + k_3 x_{i_h}^{r-3} y_{i_h}^2 + \cdots + k_r y_{i_h}^{r-1} = z'_{i_h}, \\ k_1 x_{i_{h+1}}^{r-1} + k_2 x_{i_{h+1}}^{r-2} y_{i_{h+1}} + k_3 x_{i_{h+1}}^{r-3} y_{i_{h+1}}^2 + \cdots + k_r y_{i_{h+1}}^{r-1} = z_{i_{h+1}}, \\ \vdots \\ k_1 x_{i_r}^{r-1} + k_2 x_{i_r}^{r-2} y_{i_r} + k_3 x_{i_r}^{r-3} y_{i_r}^2 + \cdots + k_r y_{i_r}^{r-1} = z_{i_r}, \\ \delta_1^{z'_{i_1}} \cdots \delta_2^{z'_{i_h}} \delta_2^{z_{i_{h+1}}} \cdots \delta_r^{z_{i_r}} \bmod p = g. \end{cases} \tag{6}$$

Because the system of Equations (6) contains $z'_{i_1}, z'_{i_2}, \cdots, z'_{i_h}$, $k_1, k_2, \cdots, k_r$ total of $h + r$ unknown variables and $r + 1$ equations, so there are $h - 1$ free variables, so the system of Equations (6) has p^{h-1} different solutions. Since all the possible subkey sets of cheaters $P_{i_1}, P_{i_2}, \cdots, P_{i_h}$ contain p^h elements, the probability of successful deception of $P_{i_1}, P_{i_2}, \cdots, P_{i_h}$ is:

$$\frac{p^{h-1} - 1}{p^h} = \frac{1}{p} - \frac{1}{p^h} < \frac{1}{p}.$$

It's over.

It can be seen from Theorem 3 that for the threshold secret sharing scheme, when $h = 1$ the probability of success of deception is 0, that is, a single cheater will not succeed in deception; With the increasing number of success is also increasing; However, no matter how many cheaters there are, the probability of success of cheaters will not exceed $1/p$.

4. Conclusion

At present, among some verifiable secret sharing schemes that have been published, the secret sharing schemes described in references [10] [11] are complete, but not ideal. Although the secret sharing scheme designed in references [12] [13] is perfect and ideal, it needs to test the subkeys of each participant one by one, resulting in the inefficiency of the scheme itself. In this paper, the plane parameter curve is used to construct the threshold secret sharing scheme, which can make the curve coordinates and the homogeneous formula of determining the master key expressed by the same parameter t, thus showing the advantages of the single parameter representation of the master key, reducing the amount of information contained in the subkeys, increasing the information rate, and making the secret sharing scheme more practical and easy to implement. The results show that the threshold scheme is not only complete, but also ideal; at the same time, it has verifiability. Through the one-time operation, we can judge whether there are cheaters in the participating members, and the probability of successful deception of the cheater will not exceed $1/p$. Therefore, the secret sharing scheme is effective and unconditionally secure in preventing deception. Secret sharing has very important theoretical and practical significance in key management.

We plan to study the next research topic. We will study the construction of a higher standard secret sharing scheme based on the parametric elliptic curve equation [16] [17] to further strengthen the security and effectiveness of secret sharing.

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.R. (1979) Safeguarding Cryptographic Key. In: *Proceedings of the National Computer Conference*, AFIPS Press, Montvale, 313-317. https://doi.org/10.1109/MARK.1979.8817296

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

[4] 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

[5] Chen, Q., Pei, D.Y., Tang, C.M., *et al.* (2013) A Note on Ramp Secret Sharing Schemes from Error-Correcting Codes. *Mathematical and Computer Modelling*, **57**, 2695-2702. https://doi.org/10.1016/j.mcm.2011.07.024

[6] Zablocki, A. (2014) Admissible Tracks in Lai-Ding's Secret Sharing Scheme. *Finite Fields and Their Applications*, **27**, 72-87. https://doi.org/10.1016/j.ffa.2013.12.006

[7] Kamer, K. and Selcuk, A.A. (2014) Sharing DSS by the Chinese Remainder Theorem. *Journal of Computational and Applied Mathematics*, **259**, 495-502. https://doi.org/10.1016/j.cam.2013.05.023

[8] 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

[9] Bogdanov, A., Guo, S. and Komargodski, H. (2020) Threshold Secret Sharing Requires a Linear-Size Alphabet. *Theory of Computing*, **16**, 168-172.

[10] 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

[11] Samaneh, M. and Massoud, H.D. (2015) Two Verifiable Multi Secret Sharing Schemes Based on Nonhomogeneous Linear Recursion and LFSR Public-Key Cryptosystem. *Information Sciences*, **294**, 31-40. https://doi.org/10.1016/j.ins.2014.08.046

[12] 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**, 42. https://doi.org/10.1186/s13640-020-00529-z

[13] Chen, L.Q., Laing, T.M. and Martin, K.M. (2016) Efficient, XOR-Based, Ideal (t, n)-Threshold Schemes. In: *The* 15*th International Conference on Cryptology and Network Security*, Springer, Berlin, 467-483. https://doi.org/10.1007/978-3-319-48965-0_28

[14] Wang, F. (2010) A Novel Verifiable Dynamic Multi-Policy Secret Sharing Scheme. In: *The* 12*th International Conference on Advanced Communication Technology* (*ICACT*2010), ACM Press, New York, 1474-1479.

[15] 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

[16] Wu, Z. (2020) A New Two-Parameter Heteromorphic Elliptic Equation: Properties and Applications. *World Journal of Engineering and Technology*, **8**, 642-657. https://doi.org/10.4236/wjet.2020.84045

[17] 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