Scientific Research Publishing

Applied Mathematics, 2023, 14, 173-181
https://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

Secret Sharing Scheme Based on the Differential Manifold

Bin Li

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

How to cite this paper: Li, B. (2023) Secret Sharing Scheme Based on the Differential Manifold. *Applied Mathematics*, **14**, 173-181.
https://doi.org/10.4236/am.2023.143010

Received: February 2, 2023
Accepted: March 17, 2023
Published: March 20, 2023

Abstract

In this paper, the concepts of topological space and differential manifold are introduced, and it is proved that the surface determined by function $F(x_1, x_2, \cdots, x_t)$ of class C^r in Euelidean R^t is a differential manifold. Using the intersection of the tangent plane and the hypernormal of the differential manifold to construct the shared master key of participants, an intuitive, secure and complete (t, n)-threshold secret sharing scheme is designed. The paper is proved to be safe, and the probability of successful attack of attackers is only $1/p^{t-1}$. When the prime number p is sufficiently large, the probability is almost 0. The results show that this scheme has the characteristics of single-parameter representation of the master key in the geometric method, and is more practical and easy to implement than the Blakley threshold secret sharing scheme.

Keywords

Topological Space, Differential Manifold, Secret Sharing, Tangent Plane, Hypernormal

1. Introduction

Secret sharing is an important research topic in key management and an important research direction in cryptography. Especially with the rapid development of computer network technology, it has become more and more common to store important files and communications electronically, and then the management of various keys has become an urgent problem that must be solved. Therefore, no matter in theory or in practice, secret sharing is of great significance to the security of computers and networks. Secret sharing is a way to distribute a

secret information in a set of participants and share it together, so that each authorized subset in the set can recover the secret. Since the secret sharing system was proposed by Shamir [1] and Blakley [2] in 1979, the research on secret sharing has received extensive attention.

In fact, secret sharing technology achieves the goal of "not putting eggs in the same basket", so that when a participant cheats or loses the key in his hand, the master key can still be recovered. This is actually to improve the reliability of data services by introducing redundancy. At the same time, most secret sharing can also achieve unconditional security, that is, its security is not based on a difficult calculation problem, but can be proved from the perspective of Shannon information theory that there is no information leakage. Even if the attacker has unlimited computing resources and time, cannot obtain any information of the master key.

Because of the above advantages, secret sharing has been widely studied and applied, and people have made fruitful research results in this area. The (t,n)-threshold secret sharing scheme can be constructed by using mathematical knowledge in different fields, among which the more famous ones are the Lagrange interpolation polynomial scheme based on finite fields in document [1], the Blakley scheme constructed by using hyperplane in finite fields in document [2], the threshold scheme based on Red-Solomon code in document [3], and the Asmuth-Blom scheme based on Chinese remainder theorem in document [4], and so on. According to different application requirements, people use different mathematical tools to improve and innovate the above threshold schemes, and propose a variety of threshold schemes [5]-[10].

The basic idea of Balakley Scheme is to use points in multidimensional space to establish a threshold scheme. The shared master key is regarded as the coordinates of a point in the *t*-dimensional space. Each subkey is the equation of the $t-1$-dimensional hyperplane containing this point. The coordinates of the intersection of any t $t-1$-dimensional hyperplanes just determine the shared master key, while the $t-1$ subkey can only determine its intersection line, so no information about the shared master key can be obtained. However, the shared masterkey in the scheme is only the *t*-dimension coordinates of a point in the *t*-dimension space, not the number of cells. To solve this problem, this paper proposes a threshold scheme that can solve the problem of unit number master key sharing using differential manifolds.

According to the idea of secret sharing, this paper uses the intersection of the tangent plane of the differential manifold hypersurface and the hypernormal in R^t to construct the master key, and designs a secure, complete and easy to implement (t,n)–threshold secret sharing scheme. The structure of the paper is as follows: Part 2 introduces some concepts, symbols and related theorems used in this paper; the third part introduces the proposed secret sharing scheme; the fourth part analyzes and discusses the proposed scheme; finally, it is a simple summary of this article.

2. Definitions and Preliminaries

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

Definition 1. [11] Let M be a set, and the subset family of M is represented by $\sum$, when $\sum$ meets the following conditions:

1) Let M and empty set ϕ belong to $\sum$,

2) Let K and L belong to $\sum$, then intersection $K \bigcap L$ also belongs to $\sum$,

3) Let $\{Y\}$ be a subset family belonging to M, then their union $\bigcup Y$ also belongs to $\sum$.

At this time, $\sum$ is called a topological structure of M. When set M has this topological structure, $(M, \sum)$ is called a topological space.

Definition 2. [11] For topological space $(M, \sum)$, the condition is satisfied: for points $P, Q \in M$, $P \neq Q$, if there is neighborhood U of P and neighborhood V of Q, and $U \bigcap V = \phi$, then $(M, \sum)$ is called Hausdorff space.

Definition 3. [11] Let $\{U_\lambda\}$, where λ is the element of the index set Λ of the set family, and Λ is not limited to a countable set. For any $P \in M$, if there is $\lambda \in \Lambda$ of $P \in U_\lambda$, that is, $M = \bigcup_{\lambda \in \Lambda} U_\lambda$, then $\{U_\lambda\}$ is called the cover of M. If U_λ is an open set, $\{U_\lambda\}, (\lambda \in \Lambda)$ is called the open cover of M.

Definition 4. [11] Let B be the open set family of the topological space. If any open set of M can be expressed as the union of the open set in B, then B is called the base of M. If the topological space M has a base composed of at most countable open sets, it is said that M satisfies the second countable axiom.

Definition 5. [12] In the n-dimensional Euclidean space R^n, $\left(u^1, u^2, \cdots, u^n\right)$ is its coordinate, and the set of points $\left(u^1, u^2, \cdots, u^n\right)$ satisfying

$$\left(u^1\right)^2 + \left(u^2\right)^2 + \cdots + \left(u^n\right)^2 < a^2$$

Is called the n–dimensional open ball with radius a.

Definition 6. [12] A Hausdorff space M satisfies the following conditions:

1) The second countable axiom is satisfied.

2) Its points have homeomorphic neighborhoods with the open ball in R^n, so M is called an n-dimensional topological manifold.

3) In the open covering $\{(U_\lambda, \varphi_\lambda)\}(\lambda \in \Lambda)$ (local coordinate is $u^i_{(\lambda)}$) of M formed by the coordinate neighborhood, for each $\lambda, \mu \in \Lambda$ of $U_\lambda \bigcap U_\mu \neq \phi$, when the n functions $u^i_{(\mu)} = u^i_{(\mu)}\left(u^1_{(\lambda)}, u^2_{(\lambda)}, \cdots, u^n_{(\lambda)}\right)$ $(i = 1, 2, \cdots, n)$ representing the homeomorphic mapping $\varphi_\mu \circ \varphi_\lambda^{-1}$ are all differentiable functions of class $C^r(r \geq 1)$, M is called an n-dimensional class C^r differential manifold.

Let $F = F\left(x_1, x_2, \cdots, x_t\right)$ be a function defined in Euclidean R^t, and the point set M satisfying equation $F\left(x_1, x_2, \cdots, x_t\right) = 0$ is called hypersurface. Let F be a function of class $C^r(r \geq 1)$, and $F_{x_1}, F_{x_2}, \cdots, F_{x_t}$ are not all zero at any point on M, so the tangent plane of any point $Q_0\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_t^{(0)}\right)$ is uniquely determined, that is,

$$\left(F_{x_1}\right)_0\left(x_1 - x_1^{(0)}\right) + \left(F_{x_2}\right)_0\left(x_2 - x_2^{(0)}\right) + \cdots + \left(F_{x_t}\right)_0\left(x_t - x_t^{(0)}\right) = 0$$

Is determined, which means that M itself has no singularity, and we can prove

that it is a $t-1$–dimensional differential manifold.

Theorem 1. The hypersurface represented by $F\left(x_1, x_2, \cdots, x_t\right)=0$ in Euclidean R^t is a differential manifold.

Proof. The introduction of R^t induced topology on M is obviously a Hausdorff space satisfying the second countable axiom. Suppose $Q_0 \in M$ has $\left(F_{x_t}\right)_0 \neq 0$, consider mapping $\psi: R^t \to R^t$, that is, $\left(x_1, x_2, \cdots, x_{t-1}, x_t\right) \to \left(x_1, x_2, \cdots, x_{t-1}, F\left(x_1, x_2, \cdots, x_{t-1}, 0\right)\right)$. Because $\left(F_{x_t}\right)_0 \neq 0$, according to the inverse function theorem, in the sufficiently small neighborhood W of $Q_0\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_t^{(0)}\right)$, its image $\psi(W)$ is in the neigh borhood of point $\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_{t-1}^{(0)}, F\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_t^{(0)}\right)\right)$, that is, $\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_{t-1}^{(0)}, 0\right)$, and ψ is the homeomorphism map of $\psi|W: W \to \psi(W)$ restricted by W.

Here, the hyperplane $\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_{t-1}^{(0)}\right)$ is represented by R^{t-1}, let $V=\psi(W) \cap R^{t-1}$, obviously $\left(\psi|W\right)^{-1}(V)=W \cap M$. Point $x_t\left(x_1, x_2, \cdots, x_{t-1}\right)$ of $\left(\psi|M\right)^{-1}(V)$ is recorded as $\left(x_1, x_2, \cdots, x_{t-1}, x_t\left(x_1, x_2, \cdots, x_{t-1}\right)\right)$ as a function defined on V, which satisfies

$$F\left(x_1, x_2, \cdots, x_{t-1}, x_t\left(x_1, x_2, \cdots, x_{t-1}\right)\right)=0, \quad x_t\left(x_1^{(0)}, x_2^{(0)}, \cdots, x_{t-1}^{(0)}\right)=x_t^{(0)}. \tag{1}$$

$\left(\psi|W\right)^{-1}$ Is the mapping that maps V into M, and $\psi|W$ is the homeomorphism mapping. Note that M has a relative topology, so V and the subset $\left(\psi|W\right)^{-1}(V)$ of M are homeomorphism. Thus, at each point Q of M, there is a homeomorphism neighborhood with the open set of R^{t-1}. Let $U=\left(\psi|W\right)^{-1}(V)$, take $\psi|U: U \to V \in R^{t-1}$, then $\left(U, \psi|U\right)$ is the coordinate neighborhood of point Q_0, and $\left(x_1, x_2, \cdots, x_{t-1}\right)$ is its local coordinate.

In the previous discussion, we assumed that there would be $\left(F_{x_t}\right)_0 \neq 0$ at Q_0, obviously there would also be $\left(F_{x_t}\right)_0 \neq 0$, so the coordinate neighborhood with $\left(x_1\left(x_2, x_3, \cdots, x_t\right), x_2, \cdots, x_t\right)$ as the coordinate around Q_0 can be taken. Because point Q_0 is an arbitrary point on M, M can be covered by such coordinate neighborhood. Now let (U, φ) and $\left(U', \varphi'\right)$ be the above two coordinate neighborhoods of M, and $U \cap U' \neq \phi$. If they take $\left(x_1, x_2, \cdots, x_{t-1}\right)$ as the local coordinate at the same time, the coordinate transformation in $U \cap U'$ is the identity transformation of $\psi\left(U \cap U'\right) \subset R^{t-1}$. If the local coordinate in (U, φ) is $\left(x_1, x_2, \cdots, x_{t-1}\right)$ and the local coordinate in $\left(U', \varphi'\right)$ is $\left(x_2, x_3, \cdots, x_t\right)$, then the coordinate transformation in $U \cap U'$ is

$$x_i = x_i\left(i=2,3, \cdots, t-1\right), \quad x_t = x_t\left(x_1, x_2, \cdots, x_{t-1}\right)$$

by using the function $x_t\left(x_1, x_2, \cdots, x_{t-1}\right)$ of (1), it is a differentiable function of class C^r. In the same way, it can be seen that

$$x_1 = x_1\left(x_2, x_3, \cdots, x_t\right), \quad x_i = x_i\left(i=2,3, \cdots, t-1\right)$$

is also a differentiable function of class C^r, and the same is true in other cases, so it is proved that M is a $t-1$-dimensional differential manifold of class C^r.

3. Programme Composition

3.1. Initialization

The objects of the system include: secret distributor D. n participants

$P=\{P_1,P_2,\cdots,P_n\}$, secret restorer, master key k to be shared, and a bulletin board for storing public information. All parties of the system can read the contents on the bulletin board, but only the secret distributor can write or update the contents on the bulletin board.

D performs the following initialization operation: select a large prime number p, finite field $F_p=\{0,1,2,\cdots,p-1\}$, and master key $k\in F_p$, and decompose the master key into $k=(k_1,k_2,\cdots,k_t)$, so that $k_1+k_2+\cdots+k_t=k(\mathrm{mod}\,p)$. Select the differential manifold $F(x_1,x_2\cdots,x_t)=0$ in Euclidean space R^t so that $F(k_1,k_2\cdots,k_t)=0$, that is , point $Q_0(k_1,k_2\cdots,k_t)$ is on the differential manifold.

3.2. Secret Distribution

The secret distributor D calculates the tangent plane π:

$$\left(F_{x_1}\right)_0(x_1-k_1)+\left(F_{x_2}\right)_0(x_2-k_2)+\cdots+\left(F_{x_t}\right)_0(x_t-k_t)=0 \tag{2}$$

of the differential manifold at point Q_0. The secret distributor D selects n different points $V_1,V_2,\cdots,V_n$ on π that are different from Q_0, so that any points in $V_1,V_2,\cdots,V_n$ can generate tangent plane π. If the coordinate of these t points are $V_{i_1}(v_{i_11},v_{i_12},\cdots,v_{i_1t}),V_{i_2}(v_{i_21},v_{i_22},\cdots,v_{i_2t}),\cdots,V_{i_t}(v_{i_t1},v_{i_t2},\cdots,v_{i_tt})$, then the equation of the tangent plane π generated by these t points is

$$\begin{vmatrix} x_1-v_{i_11} & x_2-v_{i_12} & \cdots & x_t-v_{i_1t} \\ v_{i_21}-v_{i_11} & v_{i_22}-v_{i_12} & \cdots & v_{i_2t}-v_{i_1t} \\ \vdots & \vdots & & \vdots \\ v_{i_t1}-v_{i_11} & v_{i_t2}-v_{i_12} & \cdots & v_{i_tt}-v_{i_1t} \end{vmatrix}=0 \tag{3}$$

Equation (2) and Equation (3) are tangent plane equations of differential manifold $F(x_1,x_2\cdots,x_t)=0$ at point Q_0, so they are the same equation, that is, Equation (2) and Equation (3) are equivalent on F_p.

Then the secret distributor D calculates the hypernormal ξ:

$$\frac{x_1-k_1}{\left(F_{x_1}\right)_0}=\frac{x_2-k_2}{\left(F_{x_2}\right)_0}=\cdots=\frac{x_t-k_t}{\left(F_{x_t}\right)_0} \tag{4}$$

of the differential manifold $F(x_1,x_2\cdots,x_t)=0$ at point Q_0.

Nest, the secret distributor D takes any point $Q(\xi_1,\xi_2,\cdots,\xi_t)$ on ξ then is different from Q_0, and publishes the coordinates of point Q on the bulletin board.

After determining the set of participants, the secret distributor D selects the subkey V_i for each participant P_i, and sends V_i to the participant P_i through the secure channel, and P_i keeps V_i secret.

3.3. Secret Recovery

During secret recovery, at least t participants need to submit their own subkeys. Any t participants $P_{i_1},P_{i_2},\cdots,P_{i_t}$ in the participant set $P=\{P_1,P_2,\cdots,P_n\}$ can

calculate the tangent plane π from the Formula (3) according to the subkeys $V_{i_1}, V_{i_2}, \cdots, V_{i_t}$ they hold, and obtain their corresponding normal vector $\boldsymbol{m} = (m_1, m_2, \cdots, m_t)$. Combined with the coordinate $(\xi_1, \xi_2, \cdots, \xi_t)$ of point on the bulletin board, find the corresponding hypernormal

$$\frac{x_1 - \xi_1}{m_1} = \frac{x_2 - \xi_2}{m_2} = \cdots = \frac{x_t - \xi_t}{m_t}. \tag{5}$$

Because Equation (4) and Equation (5) are hypernormal equations of the tangent plane π of differential manifold $F(x_1, x_2 \cdots, x_t) = 0$ at point Q_0, Equation (4) and Equation (5) are equivalent on F_p. Then the t participants use their Equation (3) and Equation (5) to jointly calculate the coordinate $(k_1, k_2, \cdots, k_t)$ of the intersection point Q_0, and calculate $k = k_1 + k_2 + \cdots + k_t$ on F_p to obtain the master key k.

Here is an example to illustrate.

Let $p = 13, k = 2 \in F_{13}, n = 6, t = 4$, the secret distributor D decompose the master key into $k = (1, 2, 12, 0)$, and select the differential manifold

$$F(x_1, x_2, x_3, x_4) = x_1^3 + 2x_1x_2 + 5x_1^2x_3 + 6x_2^2x_4 + 11x_3x_4^2 = 0$$

In R^4. Then calculate $(F_{x_1})_0 = 10, (F_{x_2})_0 = 2, (F_{x_3})_0 = 5, (F_{x_4})_0 = 11$ to obtain tangent plane π:

$$10x_1 + 2x_2 + 5x_3 + 11x_4 = 9$$

and hypernormal ξ:

$$\frac{x_1 - 1}{10} = \frac{x_2 - 2}{2} = \frac{x_3 - 12}{5} = \frac{x_4}{11}.$$

The secret distributor D select 6 points $V_1 = (0, 0, 0, 2)$, $V_2 = (1, 0, 0, 7)$, $V_3 = (1, 0, 1, 3)$, $V_4 = (0, 1, 0, 3)$, $V_5 = (1, 1, 0, 8)$, $V_6 = (0, 1, 1, 12)$ on π that are different from Q_0, which can verify that the 15 vectors generated between any two points of the 6 points are linearly independent. Secret distributor D secretly distributes V_i to participant $P_i\ (1 \le i \le 6)$.

The secret distributor orders

$$\frac{x_1 - 1}{10} = \frac{x_2 - 2}{2} = \frac{x_3 - 12}{5} = \frac{x_4}{11} = u$$

to get

$$\begin{cases} x_1 = 1 + 10u, \\ x_2 = 2 + 2u, \\ x_3 = 12 + 5u, \\ x_4 = 11u. \end{cases}$$

take $u = 3$ to get point $Q(5, 8, 1, 7)$ on hypernormal ξ, and the secret distributor D writes the coordinates $(5, 8, 1, 7)$ of point Q on the bulletin board.

Now, four of the participants (let's suppose P_2, P_3, P_5, P_6) recover the master key k together. They take out their subkeys V_2, V_3, V_5, V_6 to calculate the equation

$$\begin{vmatrix} x_1+12 & x_2 & x_3 & x_4+6 \\ 0 & 0 & 1 & 9 \\ 0 & 1 & 0 & 1 \\ 12 & 1 & 1 & 5 \end{vmatrix} = 0$$

of tangent plane π. The simplified equation is

$$5x_1 + x_2 + 9x_3 + 12x_4 = 11.$$

And calculate the supernomal ξ:

$$\frac{x_1-5}{5} = \frac{x_2-8}{1} = \frac{x_3-1}{9} = \frac{x_4-7}{12}$$

based on the information on the bulletin board. Combine the above formula to obtain the equation group

$$\begin{cases} 5x_1 + x_2 + 9x_3 + 12x_4 = 11, \\ \dfrac{x_1-5}{5} = \dfrac{x_2-8}{1} = \dfrac{x_3-1}{9} = \dfrac{x_4-7}{12}, \end{cases}$$

and solve the equation group to obtain the coordinate $(x_1, x_2, x_3, x_4) = (1, 2, 12, 0)$ of point Q_0, so as to recover the master key $k = 1+2+12+0 \equiv 2 \pmod{13}$.

4. Analysis and Discussion

4.1. Safety Analysis

Theorem 2. This scheme conforms to the threshold rules of the threshold secret sharing scheme and can prevent the active attack of attackers.

Proof. A secret sharing scheme must meet two basic requirements. One is that the cooperation of participants in any authorized subset can easily calculate the shared secret. The other is that the cooperation of participants in unauthorized subsets cannot obtain any information of the secret. In the process of secret reconstruction of the scheme in this paper, to determine Equation (3), we need to know t points that satisfy Equation (2) and can form a linear independent vector, and after determining Equation (3), we can determine the hypernomal in combination with the bulletin board information. Without determining Equation (3), it is impossible to obtain hypernormal Equation (4) only from bulletin board information. The participants of the unauthorized subset can only get at most $t-1$ points on the tangent plane, while the t point can only be obtained by guess. Since the system works on the finite field F_p, the probability of guessing the success of point t is only $1/p^{t-1}$. When p is large enough, the success probability of this attack is close to zero. Therefore, the scheme proposed in this paper meets the security requirements and rules of secret sharing.

4.2. Performance Analysis

This scheme has very important application value, pecially when sharing large secret, it is more effective than other schemes on general access structure. This scheme can divide the master key into t components first, and then realize the sharing of the components, so the length of the module p is 512 bits. The secret

distribution process and secret reconstruction process of this scheme only need to be executed once. It can be seen that this scheme is more effective than other existing schemes when sharing large secrets.

In addition, the operations involved in this scheme mainly include the operation of linear equation of equal proportion and the calculation of determinant. Obviously, the performance of the scheme mainly depends on the calculation of determinant. The calculation and realization of determinant is very convenient, and Wiedemann proposes a probability algorithm for the calculation of determinant, which can effectively improve the calculation of m order determinant on the finite field F_p. The algorithm using Wiedemann will improve the operational performance of the proposed scheme.

To sum up, the idea of the (t,n)-threshold secret sharing system in this paper is to use the intersection of the tangent plane and the hypernomal of the differential manifold to determine the master key. However, any $t-1$ points cannot determine the tangent plane, so the master key cannot be obtained. Therefore, this scheme meets the requirements of reconstruction and security of secret sharing, and is an effective and easy to implement secret sharing system.

5. Concluding Remark

Using differential manifold method to construct secret sharing system has a relatively intuitive advantage. Because of the difficulty of this method, there are few achievements in this field. The famous Blakley threshold secret sharing scheme is designed using geometric method. Its basic idea is to select the coordinates of a point in the multi-dimensional space as the master key, and find n $t-1$-dimensional hyperplanes passing through the point. The secret distributor distributes the n hyperplanes to n different participants. As long as t participants are together, the master key point can be found. However, less than t participants can only find the line or plane passing through the main key point together, so the coordinates of the main key point cannot be obtained. However, Blakley geometry method has a fatal weakness, that is, its shared master key can only be a point in the t-dimension space, that is, a coordinate in the t-dimension, while the key in reality is often a number of cells, so Blakley method is not practical. In this paper, the threshold secret sharing system based on differential manifolds overcomes this weakness. It uses the intersection of the tangent plane of the differential manifolds and the hypernormal to construct the master key. Because the combination of the intersection coordinates on F_p is the master key. Thus forming the master key is shown by a unit number on the finite field F_p. From this point of view, this scheme is more practical and easy to implement than the Blakley scheme.

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] Blakleey, G.B. (1979) Safeguarding Cryptographic Keys. *Proceedings of* 1979 *International Workshop on Managing Requirements Knowledge*, **48**, 313-318. https://doi.org/10.1109/MARK.1979.8817296

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

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

[5] Li, B. (2019) Bipartite Threshold Muti-Secret Sharing Scheme Based on Hypersphere. *American Journal of Computational Mathematics*, **9**, 207-220. https://doi.org/10.4236/ajcm.2019.94016

[6] 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

[7] Bogdanov, A., Guo, S. and Konargodski, H. (2020) Threshold Secret Sharing Require a Linear-Size Alphabet. *Theory of Computing*, **16**, 1-18. https://doi.org/10.4086/toc.2020.v016a002

[8] Ma, Z., Ma, Y., Huang, X.H., *et al.* (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

[9] 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

[10] 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

[11] Su, B.Q. and Hu, H.S. (1980) Differential Geometry. Higher Education Press, Beijing.

[12] Chen, S.S. and Chen, W.H. (1983) Lectures on Differential Geometry. Peking University Press, Beijing.