Applied and Computational Mathematics
2019; 8(6): 88-94
http://www.sciencepublishinggroup.com/j/acm
doi: 10.11648/j.acm.20190806.11
ISSN: 2328-5605 (Print); ISSN: 2328-5613 (Online)

Group Structure of Special Parabola and Its Application in Cryptography

Bin Li

School of Mathematics, Chengdu Normal University, Chengdu, China

Email address:
1145398209@qq.com

To cite this article:
Bin Li. Group Structure of Special Parabola and Its Application in Cryptography. *Applied and Computational Mathematics.* Vol. 8, No. 6, 2019, pp. 88-94. doi: 10.11648/j.acm.20190806.11

Received: November 5, 2019; **Accepted**: November 28, 2019; **Published**: December 9, 2019

Abstract: Public key cryptography is one of the most important research contents in modern cryptography. Curve-based public key cryptosystems have attracted widespread attention in recent years because they have more obvious advantages in speed and key length than general public key cryptosystems. People have done a lot of research on elliptic cryptosystem, among which the realization of elliptic cryptosystem is a key content. In this paper, the definition of special parabola in algebraic closed domain is proposed, the group structure of special parabola in finite field is studied, and several forms of public key cryptosystem based on this parabola are given. The results show that the parabola, together with the additive operations defined above, form an Abelian group. The radix of this parabola can be easily determined, so that the factors it contains can be large prime. The security of its public key cryptosystem is based on the difficulty of solving the discrete logarithm problem on this parabola. Moreover, these parabolic public key cryptosystems are easy to code and decode in plaintext, and easier to design and implement than elliptic curve public key cryptosystems.

Keywords: Special Parabola, Group Structure, Public Key Cryptosystem, Finite Field, Discrete Logarithm

1. Introduction

Public key cryptography is a kind of cryptography proposed in 1970s. The most important characteristic of its algorithm is that it uses two non-reciprocal keys to control the process of encryption and decryption respectively. The key used for encryption is public, called public key, and the key used for decryption is used exclusively by users and needs to be kept secret, called private key. It is computationally impossible for anyone to obtain the decryption key only knowing the cryptographic algorithm and encryption key. Public key cryptosystem is especially suitable for use in computer network environment. It has the functions of information encryption, key management and digital signature. It can guarantee the integrity, confidentiality and non-repudiation of information. So far, the security of the proposed public key cryptography is based on a mathematical problem. The mathematical problem mentioned here is that there is no polynomial time algorithm to solve this mathematical problem. For example, factorization large integers, discrete logarithms over finite fields and elliptic curve discrete logarithms, etc. These problems are difficult to solve as long as the parameters are properly selected under the existing theoretical and technical conditions, so they lay the foundation for the security of the corresponding public key cryptography. Any significant progress in solving these problems mathematically will have a tremendous impact on the use of the corresponding public key cryptography.

The most common public key cryptosystems used to be RSA public key cryptosystem [1] and Diffie-Hellman public key cryptosystem exchange algorithm [2]. RSA was broken on August 22, 1999, so the key had to be lengthened. In order to achieve the security level of 128 bits of symmetric key, NIST recommended using 3072 bits RSA key. Obviously, this increase in key length will undoubtedly aggravate RSA's slow computing speed [3, 4]. Miller [5] and Koblitz [6] independently proposed elliptic curve public key cryptography in the mid-1980s. This is another new application of elliptic curve theory in cryptography after the primality test of Goldwasser and Kilian [7] and the large number decomposition of Lenstra [8] based on elliptic curve. Its idea is still to use elliptic curves over finite fields to analogize multiplication groups over finite fields in various public key cryptosystems involving multiplication groups

over finite fields, so as to obtain similar public key cryptosystems. The security of this kind of system is based on the difficulty of solving the discrete logarithm problem on elliptic curve. At present, no sub-exponential time algorithm has been found to solve this problem. The advantage of elliptic curve cryptosystem is that it can use a shorter key length to achieve the same security requirements as the cryptosystem based on finite field, so that it can complete encryption and decryption operations at a faster speed. However, elliptic curve cryptosystem has many unsatisfactory aspects in plaintext coding and cardinality calculation. To solve this problem, we find an algebraic curve which is better than elliptic curve in these aspects, namely special parabola, which can be used to design special parabolic public key cryptosystem. This special parabolic cryptosystem satisfies the basic requirement of easy encryption and decryption. It can not only make plaintext encoding and decoding very easy, but also make it easier to design and implement than elliptic curve cryptosystem. In addition, we can easily calculate the radix of special parabola, which can make the factors contained in special parabola become large primes, so as to improve the computational complexity of discrete logarithm, thus ensuring the security of the cryptosystem.

2. The Concept of Special Parabola

We know that parallel projection usually maps square to parallelogram, so after parallel projection of rectangular coordinate system in plane, the angle between coordinate axis is no longer rectangular, and the measuring units on two coordinate axes will become different. Such a coordinate system is called affine coordinate system. Specifically, an affine frame is formed by selecting a point O and two non-collinear vectors e_1 and e_2 on the plane, which are denoted as $\delta=[O;\ e_1,\ e_2]$. The directed lines passing through the origin O along e_1 and e_2 are called x-axis and y-axis respectively. For any point M on the plane, if its corresponding decomposition formula of $\overrightarrow{OM}$ for e_1 and e_2 is $\overrightarrow{OM}=x\boldsymbol{e}_1+y\boldsymbol{e}_2$, then its ordered number pair (x,y) is called the affine coordinates of point M with respect to frame δ. If the affine frame δ is given on the plane, then according to the above provisions, the set of all points on the plane has a one-to-one correspondence with the set of all ordered real number pairs. Thus, an affine coordinate system O-xy is established on the plane. Since the affine coordinate system is completely determined by the calibrated frame δ, we directly call frame $\delta=[O;\ e_1,\ e_2]$ an affine coordinate system, where O is the origin, e_1 and e_2 are called basic vectors. The plane which has established the affine coordinate system is called the affine plane, which is recorded as $A^2(K)$, where K denotes an algebraic closed field.

Let $\delta=[O;\ e_1,\ e_2]$ be an affine coordinate system on the plane. Under δ, an ordered real array $(x_1,x_2,x_3)\neq(0,0,0)$ satisfying the following conditions is called a homogeneous affine coordinate of points on the plane.

(1) If $\rho\neq 0$, then $(\rho x_1,\rho x_2,\rho x_3)$ and (x_1,x_2,x_3) are homogeneous affine coordinates of the same points.

(2) If $x_3\neq 0$, then (x_1,x_2,x_3) is a homogeneous affine coordinate of a common point whose nonhomogeneous affine coordinates are $x=\dfrac{x_1}{x_3}, y=\dfrac{x_2}{x_3}$.

(3) Points with homogeneous affine coordinates $(x_1,x_2,0)$ are called infinite points. The set of infinite points on a plane is an infinite straight line ξ_∞ with equation $x_3=0$.

Let x be an arbitrary point on an affine plane, and for its homogeneous affine coordinate (x_1,x_2,x_3), it can be decomposed into

$$(x_1,x_2,x_3)=x_1(1,0,0)+x_2(0,1,0)+x_3(0,0,1) \tag{1}$$

Since (1, 0, 0), (0, 1, 0) are coordinates of infinite points $O_\infty^{(1)},O_\infty^{(2)}$ on the x-axis and y-axis of the affine coordinate system respectively, (0, 0, 1) is coordinates of the origin O of the affine coordinate system. In this way, formula (1) tells us that the homogeneous affine coordinate of a point is an ordered array of decomposition about coordinate three arrays of point $O_\infty^{(1)},O_\infty^{(2)},O$. Thus, in order to obtain the homogeneous affine coordinates, we must take the homogeneous affine frame $\delta=\left[O_\infty^{(1)},O_\infty^{(2)},O;e\right]$ composed of four points which are not collinear with each three points, in which $O_\infty^{(1)},O_\infty^{(2)}$ are infinite points. The function of e point is to restrict the coordinate three array of $O_\infty^{(1)},O_\infty^{(2)},O$ by expression $(e)=(O_\infty^{(1)})+(O_\infty^{(2)})+(O)$, which is determined by any coordinate (e) of e point.

In a homogeneous affine coordinate system, given a nondegenerate quadratic curve

$$\Gamma(K):\ (x_1,x_2,x_3)\begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=0,\quad \det(a_{ij})\neq 0. \tag{2}$$

We classify quadratic curves by the position relationship between quadratic curves and infinite straight lines. The quadratic curves intersecting with ξ_∞ at two different points is called hyperbola, the quadratic curve tangent with ξ_∞ is called parabola, and the quadratic curve without intersection with ξ_∞ is called ellipse.

Obviously, the coordinates of the intersection point of infinite straight line ξ_∞ and curve $\Gamma(K)$ satisfy the following equations:

$$\begin{cases}a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2=0\\x_3=0\end{cases} \tag{3}$$

Record as $A_{33}=\begin{vmatrix}a_{11}&a_{12}\\a_{12}&a_{22}\end{vmatrix}$, when $A_{33}=0$, curve $\Gamma(K)$ is tangent to infinite straight line ξ_∞, and then $\Gamma(K)$ is a

parabola, and vice versa.

The parabola studied in this paper is a special quadratic curve which satisfies the following conditions:

$$a_{33}=0,\ A_{33}=0,\ \det(a_{ij})\neq 0. \tag{4}$$

That is

$$\Gamma(K):\ a_{11}x_1^2+a_{22}x_2^2+2a_{12}x_1x_2+2a_{13}x_1x_3+2a_{23}x_2x_3=0 \tag{5}$$

where $a_{12}^2-a_{11}a_{22}=0$, $\det(a_{ij})\neq 0$.

In affine coordinate system $\delta=[O;\ e_1,\ e_2]$, formula (5) becomes the following form:

$$\Gamma(K):\ a_{11}x^2+a_{22}y^2+2a_{12}xy+2a_{13}x+2a_{23}y=0. \tag{6}$$

3. Group Structure of Special Parabola over Finite Fields

Let algebraic closed field $K=F_p$ be a finite field of p elements, p be a large prime number, and F_p^* be a multiplier group of F_p. May wish to set up

$$F_p=\{0,1,2,\cdots\cdots,p-1\},\quad F_p^*=F_p\setminus\{0\}. \tag{7}$$

The coefficients in formula (6) are as follows:

$$a_{11}=a,\ a_{22}=c,\ 2a_{12}=b,\ 2a_{13}=-d,\ 2a_{23}=-e. \tag{8}$$

In affine coordinate system $\delta=[O;\ e_1, e_2]$, we consider the following non-degenerate special parabola on affine plane $A^2(F_p)$:

$$\Gamma(F_p):\ ax^2+bxy+cy^2-dx-ey=0 \tag{9}$$

where $a,b,c,d,e\in F_p^*$, $b^2-4ac=0$.

Obviously, origin O (0, 0) is on $\Gamma(F_p)$.

If $x\neq 0$, let $y=xt$, then

$$x=\frac{d+et}{a+bt+ct^2}, \tag{10}$$

$$y=\frac{t(d+et)}{a+bt+ct^2} \tag{11}$$

can be deduced from formula (9).

We use $P(t)$ to denote the points determined by formula (10) and (11) on $\Gamma(F_p)$. Origin O is denoted as $P(t_\infty)$, that is, $P(t_\infty)=(0,0)$.

Obviously t_∞ satisfies

$$d+et_\infty=0, \tag{12}$$

that is

$$t_\infty\equiv -de^{-1} \bmod p. \tag{13}$$

Since

$$a+bt+ct^2=c\left[t^2+bc^{-1}t+b^2(4c^2)^{-1}\right]=c\left[t+b(2c)^{-1}\right]^2, \tag{14}$$

we get

$$a+bt+ct^2\neq 0\Leftrightarrow t\neq -b(2c)^{-1}. \tag{15}$$

Let $R=\left\{t\in F_p\mid t\neq\alpha\right\}$, where $\alpha\equiv -b(2c)^{-1} \bmod p$, then (10) and (11) give a one-to-one mapping $P:R\to\Gamma(F_p)$ between R and $\Gamma(F_p)$.

Now let's define the addition operation "$\oplus$" of points on $\Gamma(F_p)$. For any $P(t)\in\Gamma(F_p)$, where $t\in R$, defines

$$P(t)\oplus P(t_\infty)=P(t_\infty)\oplus P(t)=P(t). \tag{16}$$

Obviously, $P(t_\infty)$ is the zero element to "$\oplus$".

Let $P(t_1),P(t_2)\in\Gamma(F_p)$, where $t_1,t_2\in R$, and $t_1,t_2\neq t_\infty$, define

$$P(t_1)\oplus P(t_2)=P(\bar{t}), \tag{17}$$

where

$$\bar{t}=\begin{cases}\dfrac{t_1t_2+\alpha^2}{t_1+t_2} & if\ t_1+t_2\neq 0,\\ t_\infty & if\ t_1+t_2=0.\end{cases} \tag{18}$$

With this addition operation "$\oplus$", we can get the following theorem.

Theorem 1. Let F_p be a finite field of p elements and $\Gamma(F_p)$ be a special parabola over F_p, then $(\Gamma(F_p),\oplus)$ is an Abel group.

Proof. Easy to verify, for arbitrary $t_1,t_2\in R$, when $t_1+t_2\neq 0$, there is

$$a+b\bar{t}+c\bar{t}^2=\frac{c(t_1-\alpha)^2(t_2-\alpha)^2}{(t_1+t_2)^2}\neq 0, \tag{19}$$

so $\bar{t}\in R$;

when $t_1+t_2=0$, there is $P(\bar{t})=P(t_\infty)$;

hence $P(\bar{t})\in\Gamma(F_p)$,

that is closed to "$\oplus$".

Obviously, operation "$\oplus$" is commutative.

There are also negative elements for $P(t)\in\Gamma(F_p)$, which are defined as follows:

$$-p(t)=\begin{cases}p(t_\infty) & if\ t=t_\infty,\\ p(-t) & if\ t\in R\ and\ t\neq t_\infty.\end{cases} \tag{20}$$

Obviously satisfy

$$P(t_\infty)\oplus(-P(t_\infty))=P(t_\infty)\oplus P(t_\infty)=P(t_\infty), \tag{21}$$

$$P(t)\oplus(-P(t))=P(t)\oplus P(-t)=P(t_\infty). \tag{22}$$

The following proves that operation "$\oplus$" can be combined, namely arbitrary $P(t_i)\in\Gamma(F_p)$, where $t_i\in R, i=1,2,3$, there is

$$\big(P(t_1)\oplus P(t_2)\big)\oplus P(t_3)=P(t_1)\oplus\big(P(t_2)\oplus P(t_3)\big). \tag{23}$$

When one of $t_i\ (i=1,2,3)$ is t_∞, it is easy to verify that formula (23) holds.

When $t_i\neq t_\infty\ (i=1,2,3)$, the following situations are discussed.

If $t_1+t_2\neq 0$, then

$$\big(P(t_1)\oplus P(t_2)\big)\oplus P(t_3)=P\left(\frac{t_1t_2+\alpha^2}{t_1+t_2}\right)\oplus P(t_3)$$

$$=\begin{cases}p\left(\dfrac{t_1t_2t_3+\alpha^2(t_1+t_2+t_3)}{t_1t_2+t_1t_3+t_2t_3+\alpha^2}\right) & if\ \ t_1t_2+t_1t_3+t_2t_3+\alpha^2\neq 0,\\ p(t_\infty) & if\ \ t_1t_2+t_1t_3+t_2t_3+\alpha^2=0.\end{cases} \tag{24}$$

If $t_2+t_3\neq 0$, then

$$P(t_1)\oplus\big(P(t_2)\oplus P(t_3)\big)=P(t_1)\oplus P\left(\frac{t_2t_3+\alpha^2}{t_2+t_3}\right)$$

$$=\begin{cases}p\left(\dfrac{t_1t_2t_3+\alpha^2(t_1+t_2+t_3)}{t_1t_2+t_1t_3+t_2t_3+\alpha^2}\right) & if\ \ t_1t_2+t_1t_3+t_2t_3+\alpha^2\neq 0,\\ p(t_\infty) & if\ \ t_1t_2+t_1t_3+t_2t_3+\alpha^2=0.\end{cases} \tag{25}$$

So, if $t_1+t_2\neq 0$ and $t_2+t_3\neq 0$, then formula (23) holds.

If $t_1+t_2=0$ and $t_2+t_3\neq 0$, then

$$\big(P(t_1)\oplus P(t_2)\big)\oplus P(t_3)=P(t_\infty)\oplus P(t_3)=P(t_3), \tag{26}$$

$$P(t_1)\oplus\big(P(t_2)\oplus P(t_3)\big)=P(-t_2)\oplus P\left(\frac{t_2t_3+\alpha^2}{t_2+t_3}\right)$$

$$=P\left(\frac{t_3(\alpha^2-t_2^2)}{\alpha^2-t_2^2}\right)=P(t_3). \tag{27}$$

At this time, formula (23) holds, the same can be proved when $t_1+t_2\neq 0$ and $t_2+t_3=0$, formula (23) also holds.

If $t_1+t_2=0$ and $t_2+t_3=0$, then

$$\big(P(t_1)\oplus P(t_2)\big)\oplus P(t_3)=P(t_\infty)\oplus P(t_3)=P(t_3), \tag{28}$$

$$\begin{aligned}&P(t_1)\oplus\big(P(t_2)\oplus P(t_3)\big)=P(t_1)\oplus P(t_\infty)\\ &=P(t_1)=P(-t_2)=P(t_3).\end{aligned} \tag{29}$$

At this time, formula (23) holds.

In summary, $(\Gamma(F_p),\oplus)$ forms an Abel group.

Theorem 2. Let F_p be a finite field of p elements and $\Gamma(F_p)$ be a special parabola over F_p, then the cardinal number of $\Gamma(F_p)$ is

$$|\Gamma(F_p)|=p-1. \tag{30}$$

Proof. For arbitrary $t_1,t_2\in R$, set up $p(t_1)=(x_1,y_1)$, $p(t_2)=(x_2,y_2)$,

then formula (10) and (11) give

$$\begin{cases}x_1=\dfrac{d+et_1}{a+bt_1+ct_1^2},\\ y_1=\dfrac{t_1(d+et_1)}{a+bt_1+ct_1^2};\end{cases} \tag{31}$$

$$\begin{cases}x_2=\dfrac{d+et_2}{a+bt_2+ct_2^2},\\ y_2=\dfrac{t_2(d+et_2)}{a+bt_2+ct_2^2}.\end{cases} \tag{32}$$

If $t_1=t_2$, then $p(t_1)=p(t_2)$.

Conversely, if $p(t_1)=p(t_2)$, namely $(x_1,y_1)=(x_2,y_2)$, there is

$$\begin{cases}\dfrac{d+et_1}{a+bt_1+ct_1^2}=\dfrac{d+et_2}{a+bt_2+ct_2^2},\\ \dfrac{t_1(d+et_1)}{a+bt_1+ct_1^2}=\dfrac{t_2(d+et_2)}{a+bt_2+ct_2^2}.\end{cases} \tag{33}$$

From this we can get $t_1=t_2$, so $t_1=t_2$ is the necessary and sufficient condition of $p(t_1)=p(t_2)$, according to the thought of anti-evidence, that is

$$t_1\neq t_2\Leftrightarrow p(t_1)\neq p(t_2). \tag{34}$$

Since $P:R\to\Gamma(F_p)$ is a one-to-one mapping, we get

$$|\Gamma(F_p)|=|R|=p-1. \tag{35}$$

4. Special Public Key Cryptosystem

4.1. Discrete Logarithm Problem of Special Parabola

In order to use special parabola to construct cryptosystem, it is necessary to find out the difficult mathematical problem on special parabola. Give the following notation first:

$$nP(t) = \underbrace{P(t) \oplus P(t) \oplus \cdots\cdots \oplus P(t)}_{n}. \tag{36}$$

where $P(t) \in \Gamma(F_p)$, $t \in R$, $n < p$.

Let $P(t)$ be a point on special parabola $\Gamma(F_p)$.

If there is a smallest positive integer n such that $nP(t) = P(t_\infty)$, then n is the order of point $P(t)$, denoted as $n_{P(t)}$, that is

$$n_{P(t)} = \min\{nP(t) = P(t_\infty), n \in N\}. \tag{37}$$

If there is no such positive integer n, then point $P(t)$ is called infinite order and is recorded as $n_{P(t)} = \infty$.

We know that if $E(F_p)$ is an elliptic curve over finite field F_p, P is the generator of a cyclic subgroup on $E(F_p)$, and $Q \in E(F_P)$, the only integer n ($0 \le n \le ord(P) - 1$) satisfying $nP=Q$ is a discrete logarithm problem on elliptic curve, which is a difficult mathematical problem.

Similarly, the mathematical difficulty of special parabola is the parabolic discrete logarithm problem. That is know special parabola $\Gamma(F_p)$ and point $P(t_1)$, where point $P(t_1)$ is the generator of a cyclic subgroup of group $(\Gamma(F_p), \oplus)$. Random selection of an integer $n < p$ make it easy to calculate $P(t_2) = nP(t_1)$, but given $P(t_1)$, $P(t_2) \in \Gamma(F_p)$, it is very difficult to calculate n.

In order to implement cryptosystem on special parabola, we also need to establish a reversible embedding mapping from plaintext message space M to special parabola to encode plaintext. That is

$$P: M \to \Gamma(F_p), \quad P: m \to P(m), \tag{38}$$

where $m \in F_p$, $P(m)$ is called plain code, which is encoded by plaintext m.

Specific coding algorithms are as follows: For $m \in F_p$, calculate

$$\begin{cases} x_m \equiv (d + em)(a + bm + cm^2)^{-1} \bmod p, \\ y_m \equiv m(d + em)(a + bm + cm^2)^{-1} \bmod p, \end{cases} \tag{39}$$

then there is

$$P(m) = (x_m, y_m). \tag{40}$$

Reverse encoding as

$$P^{-1}: \Gamma(F_p) \to M, \quad P^{-1}: P(m) \to m, \tag{41}$$

that is

$$m \equiv y_m x_m^{-1} \bmod p. \tag{42}$$

For example, in order to facilitate calculation, a finite field of $F_{11} = \{0, 1, 2 \cdots\cdots, 10\}$, a special parabola of

$$\Gamma(F_{11}): 9x^2 + xy + 4y^2 - 5x - 7y = 0, \tag{43}$$

and a plaintext of $m = 8 \in F_{11}$ are set.

We can see $a = 9, b = 1, c = 4, d = 5, e = 7$.

From formula (39), we get

$$\begin{aligned} x_8 &\equiv (5 + 7 \times 8)(9 + 8 + 4 \times 8^2)^{-1} \bmod 11 = 8, \\ y_8 &\equiv 8 \times 8 \bmod 11 = 9. \end{aligned} \tag{44}$$

So $P(8) = (8, 9)$, on the contrary, when $P(8) = (8, 9)$ is known, the anti-coding process is

$$m \equiv 9 \times 8^{-1} \bmod 11 = 8. \tag{45}$$

Special parabolic cryptosystems are based on the difficulty of solving the discrete logarithm problem defined on the group of curve points. Like the discrete logarithm problem of elliptic curve, in order to make the calculation of discrete logarithm on $\Gamma(F_p)$ more difficult, it is necessary to select the prime number p to be very large. When the factor of $p - 1$ contains a large prime q, the computational complexity of the discrete logarithm algorithm is $O(q \log(p + 1))$ [9], which can ensure the security of special parabolic cryptosystem. Here we present three cryptosystems based on special parabolic group structure.

4.2. Key Exchange Protocol Based on Special Parabola

The key exchange protocol enables multiple users in an insecure channel to obtain common secret information, which may be used as the private key of a symmetric cryptosystem, while the attacker cannot obtain the secret information.

Choosing a large prime $p > 2^{180}$, a special parabola $\Gamma(F_p)$, and the base point $P(t)$ on $\Gamma(F_p)$, the order $n_{P(t)}$ of $P(t)$ is a large prime number.

(1) User A chooses random number a, calculates $Q_A = aP(t)$, and sends it to user B.

(2) User B chooses random number b, calculates $Q_B = bP(t)$, and sends it to user A.

(3) User A calculates the shared key $k = aQ_B = abP(t)$.

(4) User B calculates the shared key $k = bQ_A = abP(t)$.

Obviously, the security of the system is based on the difficulty of solving the discrete logarithm of special parabola:

$$Q_A = xP(t), Q_B = yP(t). \tag{46}$$

4.3. Encryption and Decryption Cryptosystem Based on Special Parabola

Scheme 1:

Let $\Gamma(F_p)$ be a special parabola, $P(t) \in \Gamma(F_p)$, the order of $P(t)$ is large prime number $n_{P(t)}$.

(1) User A selects the private key d_A and calculates the public key $Q_A = d_A P(t)$.

(2) In order to send information m to user A, user B first

codes m to $P(m)=(x_m,y_m)$, then selects random number k to send $\left(kP(t),P(m)+kQ_A\right)$ to user A.

(3) User A decryption process is: first calculate

$$\left(P(m)+kQ_A\right)-d_A\left(kP(t)\right)=P(m)=(x_m,y_m), \tag{47}$$

then use formula (42) to calculate $m\equiv y_m x_m^{-1} \bmod p$.

Obviously, if an attacker wants to restore plaintext m, he must calculate d_A with knowledge of $P(t)$ and Q_A, or k with knowledge of $P(t)$ and $kP(t)$. Because $|\Gamma(F_p)|=p-1$ contains a large prime factor, such a calculation is very difficult.

Scheme 2:

Choose a large prime number p, suppose $\Gamma(F_p)$ is a special parabola over finite field F_p, then $|\Gamma(F_p)|=p-1$.

(1) User A selects a public key e_A to satisfy $1<e_A<p-1$ and calculates the private key d_A through $e_A d_A\equiv 1 \bmod p$.

(2) User B selects a public key e_B to satisfy $1<e_B<p-1$ and calculates the private key d_B through $e_B d_B\equiv 1 \bmod p$.

(3) User A encodes message m as $P(m)=(x_m,y_m)$, calculates $c_1=e_A P(m)$, and sends c_1 to user B.

(4) User B calculates $c_2=e_B c_1$ and sends c_2 to user A.

(5) User A calculates $c_3=d_A c_2$ and sends c_3 to user B.

(6) User B calculates.

$$\begin{aligned} &d_B c_3=d_B d_A c_2=d_B d_A e_B c_1\\ &=d_B d_A e_B e_A P(m)=\left(e_A d_A\right)\left(e_B d_B\right)P(m)=P(m). \end{aligned} \tag{48}$$

That is, user B obtains the plaintext $P(m)=(x_m,y_m)$ sent by user A, and then decode the plaintext message $m\equiv y_m x_m^{-1} \bmod p$.

5. Conclusions

Since the birth of elliptic curve public key cryptosystem, people have made a lot of achievements in the research of elliptic curve cryptography. There are not only theoretical research on elliptic curve cryptography [10-12], but also application research on elliptic curve cryptography [13-19]. The security of this cryptosystem is based on the difficulty of the elliptic curve discrete logarithm problem. Similarly, the security of the special parabolic curve public cryptosystem proposed in this paper is based on the difficulty of solving the special parabolic discrete logarithm problem. This paper has done some basic research work on special parabola. In the future, people can further study the special parabolic curve public cryptosystem according to the research ideas of elliptic curve public cryptosystem, and popularize and innovate it. Therefore, the establishment of special parabolic public key cryptosystem has very important theoretical and practical value and a more far-reaching development prospects. In addition, the special parabolic public key cryptosystem has the same advantages as the elliptic curve public key cryptosystem, such as higher security, smaller key volume and better flexibility. However, there are still many problems in the embedding and implementation of plaintext in the elliptic curve public key cryptosystem. Relatively speaking, the special parabolic public key cryptosystem shows that plaintext coding is very easy and decoding is very simple. So in the future, people should feel that the special parabolic public key cryptosystem is simpler and easier to implement than the elliptic curve public key cryptosystem and the improved RSA public key cryptosystem [20].

References

[1] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21 (1978), 120-126.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transaction on Information Theory, 22 (1976), 644-654.

[3] L. H. Gong, K. D. Qin and C. Z. Deng, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," Optics and Lasers in Engineering, 121 (2019), 169-180.

[4] Y. C. Wang, Y. Ikematsu and D. N. Duong, "The secure parameters and efficient decryption algorithm for multivariate public key cryptosystem EFC" IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, E102A (2019), 1028-1036.

[5] V. S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology-CRYPTO 1985, Berlin: Springer-Verlag, 417-426, 1986.

[6] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computiation, 48 (1987), 203-209.

[7] S. Goldwasser and J. Kilian, "Almost all primes can be quickly certified," Proceeding of the 18th STOC of the ACM. Berkeley: AFIPS press, 316-329, 1986.

[8] H. W. Lenstra, "Factoring integers with elliptic curves," Annals of Mathematatics, 126 (1987), 649-673.

[9] H. C. Tilborg, "An introduction to cryptology," Boston: Kluwer Academic Publishers, 1988.

[10] G. Frey, M. Müller and H. Rück, "The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," IEEE Transaction on Information Theory, 45 (1999), 1717-1719.

[11] S. Erickson, M. J. Jacobson and N. Shang, "Explicit formulas for real hyperelliptic curves of genus 2 in affine representation," WAIFI 2007, New York: Springer-Verlag, 202-218, 2007.

[12] J. Miret, R. Moreno and J. Pujolas, "Halving for the 2-Sylow subgroup of genus 2 curves over binary fields," Finite Fields Applicatae, 15 (2009), 569-579.

[13] N. Smart, "A comparison of different finite fields for elliptic curve cryptosystems," Computers and Mathematics with Applications, 42 (2001), 91-100.

[14] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," Quantum Information and Computation, 3 (2003), 317-344.

[15] N. Philip and D. Steven, "Point compression for Koblitz elliptic curves," Advances in Mathematics of Communications, 5 (2011), 1-10.

[16] H. B. Zhao, L. Y. Qian and L. F. Jin, "A new mceliece cryptosystem based on subfield subcode of elliptic curve code," Computer Applications and Softwre, 36 (2019), 317-322.

[17] C. Y. Wang, G. A. Xu and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," Sensors, 17 (2017), 1018-1027.

[18] Z. Y. Liu, T. C. Xia and J. B. Wang, "Fractional two-dimensional discrete chaotic map and its applications to the information security with elliptic-curve public key cryptography," Journal of Vibration and Control, 24 (2018), 4797-4824.

[19] L. D. Han, X. Tan and S. B. Wang, "An efficient and secure three-factor based authenticated key exchange scheme using elliptic curve cryptosystems," Peer-to-peer Networking and Applications, 11 (2018), 63-73.

[20] B. Li, "The solution structure of multivariate linear indeterminate equation and its application," Journal of Anhui University (NES), 39 (2015), 6-12.