Public-key cryptosystem based on isogenies

Alexander Rostovtsev and Anton Stolbunov

Saint-Petersburg State Polytechnical University, Department of Security and Information Protection in Computer Systems, Russia
rostovtsev@ssl.stu.neva.ru
stolbunov@fromru.com

Abstract. A new general mathematical problem, suitable for public-key cryptosystems, is proposed: morphism computation in a category of Abelian groups. In connection with elliptic curves over finite fields, the problem becomes the following: compute an isogeny (an algebraic homomorphism) between the elliptic curves given. The problem seems to be hard for solving with a quantum computer. ElGamal public-key encryption and Diffie-Hellman key agreement are proposed for an isogeny cryptosystem. The paper describes theoretical background and a public-key encryption technique, followed by security analysis and consideration of cryptosystem parameters selection. A demonstrative example of encryption is included as well.

public-key cryptography, elliptic curve cryptosystem, cryptosystem on isogenies of elliptic curves, isogeny star, isogeny cycle, quantum computer

1 Introduction

Security of the known public-key cryptosystems is based on two general mathematical problems: determination of order and structure of a finite Abelian group, and discrete logarithm computation in a cyclic group with computable order. Both of the problems can be solved in polynomial time using Shor's algorithm for a quantum computer [1]. Thus, most of the current public-key cryptosystems will become insecure when size of a quantum register is sufficient. Development of cryptosystems, which would be strong against a quantum computer, is necessary.

A mathematical problem, which is hypothetically strong against a quantum computer, is proposed. It consists in searching for an isogeny (an algebraic homomorphism) between elliptic curves over a finite field. The problem is a special case of morphism computation in an Abelian groups category. A method of public-key algorithm construction is proposed as well.

The paper describes theoretical background and a public-key encryption technique, followed by security analysis and consideration of cryptosystem parameters selection. A demonstrative example of encryption is included as well.

2 Elliptic curve

By symbols $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p, R[x], \#M$ we denote the ring of integers, the fields of rational and complex numbers, the finite field having p elements, the ring of polynomials with coefficients from the ring R, and the power of the set M, respectively.

Let K be a field with characteristic different from 2 and 3. *A projective plane* $\mathbb{P}^2_K$ is a set of triplets $(X, Y, Z) \in K^3 \setminus (0, 0, 0)$ with equivalence relation $(X, Y, Z) = (uX, uY, uZ)$ for an arbitrary $u \in K^*$. The line $Z = 0$ is called *the line of infinity*, and the points on it are *the infinite points.*

An elliptic curve $E(K)$ is a nonsingular curve, given in $\mathbb{P}^2_K$ by

$$Y^2 Z = X^3 + AXZ^2 + BZ^3. \tag{1}$$

The curve (1) intersects the line of infinity in the point $P_\infty = (0, 1, 0)$ with multiplicity 3. For all the other points we can assume $Z = 1$, and $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$. Then the equation (1) can be written as

$$y^2 = x^3 + Ax + B. \tag{2}$$

The prime polynomial $y^2 - (x^3 + Ax + B)$, which gives the elliptic curve (2), generates a maximal ideal of $K[x, y]$ and specifies *the function field of the curve*:

$$K(E) = K[x, y] \setminus (y^2 - (x^3 + Ax + B)).$$

A geometric addition law on the curve $E(K)$ is defined. It converts $E(K)$ into an Abelian group, where P_∞ is a null element [2].

Many cryptoalgorithms are built on elliptic curves over finite fields, e.g., digital signature schemes ECDSA and GOST R 34.10-2001 (a Russian standard).

3 Elliptic curves over $\mathbb{C}$ and modular functions

Let a lattice $L = [\omega_1, \omega_2]$ over $\mathbb{C}$ with the basis $[\omega_1, \omega_2]$, $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$, be the free group $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. The lattice stays fixed if its basis is multiplied by a matrix from the group $SL_2(\mathbb{Z})$ of matrices of integer elements having determinant 1. The group $SL_2(\mathbb{Z})$ is generated by the matrices $S = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. As long as L is a subgroup of $\mathbb{C}$, the additive factor group $\mathbb{C}/L$ is defined.

The meromorphic Weierstrass function

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

satisfies the equation

$$\wp'(z, L)^2 = 4\wp(z, L)^3 - g_2(L)\wp(z, L) - g_3(L),$$

where

$$g_2(L) = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}$$

and

$$g_3(L) = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6}$$

are complex numbers.

It is shown in [2], that the functions $(\wp(z,L), \wp'(z,L))$ specify the isomorphism of the groups $\mathbb{C}/L \cong E_L(\mathbb{C})$, and the set of lattices over $\mathbb{C}$ bijectively corresponds to the set of elliptic curves $E(\mathbb{C})$.

Lattices L and M are isomorphic (homomorphic), if a number $\alpha \in \mathbb{C}$ with the property that $\alpha L = M$ ($\alpha L \subseteq M$, respectively) exists. Isomorphism of lattices induces isomorphism of corresponding elliptic curves.

For a lattice L, the function

$$j(L) = \frac{1728 g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2}$$

is defined. A necessary and sufficient condition of isomorphism of elliptic curves and lattices is $j(E) = j(L)$ [2].

For a lattice L, isomorphism of lattices lets us turn from the basis $[\omega_1, \omega_2]$ to the basis $[\tau, 1]$, where $\tau = \frac{\omega_1}{\omega_2}$, $\mathrm{Im}(\tau) > 0$, and L is defined by τ accurate within isomorphism. Then we can assign $j(L) = j(\tau)$.

A matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, acting on the basis of a lattice, transforms the argument τ in the following way:

$$A(\tau) = \frac{a\tau + b}{c\tau + d}.$$

For computational convenience of the function $j(\tau)$, the argument τ is replaced by the Fourier-image $q = \exp(2\pi i \tau)$.

A meromorphic function of a complex variable τ is called *modular*, if it is not changed by action of $SL_2(\mathbb{Z})$. The function $j(\tau)$ is modular. Any modular function is representable by a fraction of polynomials in $j(\tau)$.

Homomorphism of lattices $\alpha L \subseteq M$ induces algebraic homomorphism of elliptic curves $E_L(\mathbb{C}) \to E_M(\mathbb{C})$, called *an isogeny.* A non-unit isogeny φ has its finite kernel $\ker(\varphi)$, that is the set of points mapped to P_∞.

Each isogeny $\varphi : E_L(\mathbb{C}) \to E_M(\mathbb{C})$ has its *dual isogeny* $\hat{\varphi} : E_M(\mathbb{C}) \to E_L(\mathbb{C})$.

If there is an isogeny $E_L(\mathbb{C}) \to E_M(\mathbb{C})$, then the curves are called *isogenous.*

An isogeny $\varphi : E_L(\mathbb{C}) \to E_M(\mathbb{C})$ induces injective homomorphism of the function fields $\mathbb{C}(E_M) \to \mathbb{C}(E_L)$. The extension degree of the field $\mathbb{C}(E_L)$ over $\mathbb{C}(E_M)$ is called *the isogeny degree*:

$$\deg(\varphi) = \deg(\hat{\varphi}) = \#\ker(\varphi).$$

Composition of the mappings $\varphi, \hat{\varphi}$ corresponds to multiplication by $\deg(\varphi) \in \mathbb{Z}$. According to the theorem on homomorphisms of groups, an isogeny is fully determined by its kernel.

For elliptic curve isogenies

$$E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\psi} E_3 \xrightarrow{\chi} E_4,$$

composition

$$\psi\varphi : E_1 \to E_3$$

is defined, where

$$\deg(\psi\varphi) = \deg(\psi)\deg(\varphi), \tag{3}$$

and

$$\widehat{\psi\varphi} = \hat{\varphi}\hat{\psi}.$$

Isogenies have associative property:

$$(\chi\psi)\varphi = \chi(\psi\varphi). \tag{4}$$

Let $M_2^l(\mathbb{Z})$ be a set of 2×2 matrices of coprime integer elements and determinant l. If $M \in M_2^l(\mathbb{Z})$, and $A, B \in SL_2(\mathbb{Z})$, then $AMB \in M_2^l(\mathbb{Z})$. Therefore we can define the cosets of the set $M_2^l(\mathbb{Z})$ to the group $SL_2(\mathbb{Z})$. The number of the cosets is

$$\psi(l) = l\prod_{p|l}\left(1 + \frac{1}{p}\right),$$

where product is over all the prime divisors of l.

Let $\{M_i\}$ be a set of representatives of right cosets of $M_2^l(\mathbb{Z})$ to the group $SL_2(\mathbb{Z})$, where $1 \le i \le \psi(n)$. *A modular polynomial* of order l is

$$\Phi_l(X, j) = \prod_{i=1}^{\psi(l)}\left(X - j(M_i(\tau))\right), \tag{5}$$

where $\Phi_l(X, j) = \Phi_l(j, X) \in \mathbb{Z}[X, j]$. The roots of the polynomial $\Phi_l(X, j)$ give the j-invariants of all the elliptic curves, l-degree isogenous to a curve with invariant j.

4 Elliptic curves over $\mathbb{F}_p$

Let the equation (2) of a curve $E(\bar{\mathbb{F}}_p)$ have the coefficients from $\mathbb{F}_p$. Then the map

$$\pi : (x, y) \to (x^p, y^p)$$

specifies *the Frobenius endomorphism* of the curve $E(\bar{\mathbb{F}}_p)$, which leaves the points of $E(\mathbb{F}_p)$ still. A Frobenius map satisfies its characteristic equation over $\mathbb{C}$:

$$\pi^2 - T\pi + p = 0, \tag{6}$$

where $T = p - \#E(\mathbb{F}_p)$ - *a Frobenius trace*. As long as $T^2 < 4p$ and $|T| < 2\sqrt{p}$, the discriminant of (6) is negative. If the characteristic of the field is representable as (7a) or (7b):

$$p = a^2 + |D|b^2, \tag{7a}$$

$$p = \frac{|D|+1}{4}a^2 + |D|ab + |D|b^2, \tag{7b}$$

then the number of points is evaluated, respectively,

$$\#E(\mathbb{F}_p) = p + 1 \pm 2a, T = \pm 2a, \tag{8a}$$

$$\#E(\mathbb{F}_p) = p + 1 \pm a, T = \pm a. \tag{8b}$$

The discriminant D_π of the Frobenius equation (6) for the case (7a, 8a) equals

$$D_\pi = T^2 - 4p = 4Db^2,$$

and for the case (7b, 8b) equals

$$D_\pi = T^2 - 4p = D(a + 2b^2).$$

Theorem 1. *Elliptic curves are isogenous over $\mathbb{F}_p$ if and only if they have equal number of points.*

Proof. See [6].

Theorem 2. *Let an elliptic curve $E(\mathbb{F}_p)$ have the Frobenius discriminant D_π, and $\left(\frac{D_\pi}{l}\right)$ be a Kronecker symbol for some l-degree isogeny. If $\left(\frac{D_\pi}{l}\right) = -1$, then there are no l-degree isogenies; if $\left(\frac{D_\pi}{l}\right) = 1$, then two l-degree isogenies exist; if $\left(\frac{D_\pi}{l}\right) = 0$, then 1 or $l+1$ l-degree isogenies exist.*

Proof. See [6].

Let $E(\mathbb{F}_p)$ has a subgroup with prime order $r \neq p$, and $\#E(\mathbb{F}_p) \not\equiv 0 \pmod{r^2}$. Then a finite extension $\mathbb{F}_{p^m}$ with the property that $\#E(\mathbb{F}_{p^m}) \equiv 0 \pmod{r^2}$ exists. $E(\mathbb{F}_{p^m})$ contains *the r-torsion points subgroup* $E[r]$, which is direct sum of two cyclic groups:

$$E[r] \cong \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z}.$$

A Weil pairing e_r is a computable group homomorphism

$$E[r] \times E[r] \to \mathbb{F}^*_{p^m}$$

with the following properties (see [5]):

– bilinearity:

$$\begin{aligned} e_r(S_1 + S_2, T) &= e_r(S_1, T)e_r(S_2, T), \text{ and} \\ e_r(S, T_1 + T_2) &= e_r(S, T_1)e_r(S, T_2); \end{aligned} \tag{9}$$

– alternating: $e_r(S, T) = e_r(T, S)^{-1}$;
– if σ is the automorphism field of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$, then $e_r(S, T)^\sigma = e_r(S^\sigma, T^\sigma)$.

5 Class number

In order to homomorphism of elliptic curves $E(\mathbb{C}) \to E(\mathbb{F}_p)$ be computable, it should be algebraic, and $j(\tau)$ should be an algebraic number. If τ is an element of a quadratic imaginary field $K = \mathbb{Q}[\sqrt{D}]$, $D < 0$, then $j(\tau)$ is an integer [3].

K is not being changed by multiplying its discriminant D by square of an integer (a conductor). If $D_1 = a^2 D$, $D_2 = b^2 D_1$, where $a, b \in \mathbb{Z}$, then, for the rings (the quadratic imaginary orders), it can be written $O_D \supset O_{D_1} \supset O_{D_2}$. Therefore, a maximal order exists, and it is determined by D, which is free of squares.

Any ideal $\mathbf{A}$ of the quadratic imaginary order of discriminant $D \equiv 0, 1 \pmod 4$ can be specified as $\mathbf{A} = a\mathbb{Z} + \mathbb{Z}(b + \xi)$, where $a, b \in \mathbb{Z}$, and a number $c \in \mathbb{Z}$ with the property that $D = b^2 - 4ac$, $\gcd(a, b, c) = 1$, exists [4]. The set of the ideals is multiplication closed.

Ideals $\mathbf{A}$ and $\mathbf{B}$ of a quadratic order O_D are equivalent, if nonzero $\alpha, \beta \in O_D$ such that $\alpha\mathbf{A} = \beta\mathbf{B}$ exist. The set of the ideals is decomposed to the equivalence classes. Let us denote A, B as a classes, where ideals $\mathbf{A}$ and $\mathbf{B}$ are situated. Then the class AB corresponds to product of the ideals $\mathbf{AB}$. The set of the ideal classes is the Abelian group of classes $\mathrm{Cl}(D)$. Its order h_D is called *a class number*. Each class contains a unique reduced ideal, which is defined by a triplet (a, b, c), where $-a < b \leq a$ and $a \leq c$, and also $b \geq 0$ when $a = c$.

Let O_D be a quadratic imaginary order, K - its field of quotients, and $L = [\tau, 1]$ - a lattice in K. Then $K = \mathbb{Q}[\tau]$. As far as τ is a quadratic imaginary number, there exist coprime numbers $a, b, c \in \mathbb{Z}$, $a > 0$, such that $a\tau^2 + b\tau + c = 0$ and $\tau = \frac{-b+\sqrt{D}}{2a}$, where $D = b^2 - 4ac$.

For any class of ideals of a ring O_D, a bijectively corresponding lattice exists, which is homomorphic to a lattice $L = [\tau, 1]$. If $\tau_i = \frac{b_i+\sqrt{D}}{2a_i}$, $1 \leq i \leq h_D$, then $j(\tau_i)$ are integer numbers - roots of *the Hilbert polynomial* $H_D(X)$:

$$H_D(X) = \prod_{i=1}^{h_D} \left(X - j\left(\frac{b_i + \sqrt{D}}{2a_i} \right) \right) \in \mathbb{Z}[X].$$

Theorem 3. *There is bijection between the group of classes of an imaginary quadratic order O_{D_π} and the set of isogenous elliptic curves over $\mathbb{F}_p$ having discriminant D_π.*

Proof. The Hilbert polynomial degree equals the class number h_D. The polynomial is decomposed to linear factors over $\mathbb{F}_p$. Every Hilbert polynomial root specifies the j-invariant of an elliptic curve with equal number of points $\#E(\mathbb{F}_p)$.

Theorem 4. *If $D_\pi = f^2 D$, and D is a square-free quadratic form discriminant, then*

$$\frac{h_{D_\pi}}{w_{D_\pi}} = \frac{h_D}{w_D} f \prod_{k|f} \left(1 - \frac{\left(\frac{D}{k}\right)}{k} \right), \tag{10}$$

where product is over all the prime divisors k of the conductor f, w_D is a number of reversible elements in the imaginary quadratic order O_D ($w_D = 4$ when $D =$

−4; $w_D = 6$ when $D = -3$; and $w_D = 2$ in the other cases), and $\left(\frac{D_\pi}{k}\right)$ is a Kronecker symbol.

$$\left(\frac{D_\pi}{k}\right) = D_\pi^{\frac{k-1}{2}} \pmod{k} \textit{ for the odd } k;$$

$$\left(\frac{D_\pi}{2}\right) = \begin{cases} 0, & \textit{when } D_\pi \equiv 0 \pmod{2}, \\ (-1)^{\frac{D_\pi^2-1}{8}}, & \textit{when } D_\pi \equiv 1 \pmod{2}. \end{cases}$$

Proof. See [7].

Discriminants, which have a large prime class number, or their class number has a large prime divisor, are of special interest. According to [7], a class number asymptotically equals $h_{D_\pi} = O(\sqrt{D_\pi})$.

Corollary 1. *If a discriminant D of a positive definite quadratic form is a product of different odd prime numbers, then the class number can not be prime.*

Proof. Follows from theorem 4.

Lengths of coefficients of polynomials $H_D(X)$ and $\Phi_l(X)$ grow fast with increasing D and l, respectively. So, for $|D| > 10^9$ (or $l > 10^6$), calculation of a Hilbert polynomial (a modular polynomial, respectively) is practically infeasible.

6 Isogeny computation

For every prime isogeny degree l, the equivalent polynomial can be calculated (see [8], [12]):

$$G_l(X,Y) = \sum_{r=0}^{l+1} \sum_{k=0}^{v} a_{r,k} X^r Y^k \in \mathbb{Z}[X,Y]. \tag{11}$$

The equation (11) can be used for computation of j-invariants of isogenous elliptic curves. As compared to the modular polynomial (5), the equivalent polynomial has smaller degree and lengths of coefficients.

To compute an isogenous elliptic curve, the algorithm from p.111 of [12] can be used. It takes a source elliptic curve (A, B) with invariant j, an isogeny degree l, and a root of the equation $G_l(X, j) = 0$ as input, and gives a target elliptic curve (A', B') on output.

To compute an isogeny kernel, the algorithm from p.116 of [12] can be used. It gives the polynomial

$$K(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0 \in \mathbb{F}_p[X], \tag{12}$$

where $d = \frac{l-1}{2}$. The roots of $K(X)$ give all the x-coordinates of kernel points.

An l-degree isogeny $I : E(\mathbb{F}_p) \to E'(\mathbb{F}_p)$ is a pair of rational functions (see p.4 of [13]). It can be represented as

$$I(X,Y) = \left(\frac{G(X)}{K(X)^2}, \frac{J(X,Y)}{K(X)^3}\right), \tag{13}$$

where $G(X)$ is a polynomial of degree l, and $K(X)$ is the polynomial (12). To compute an isogeny, the algorithm from pp.3-4 of [13] can be used.

7 Isogeny star

Let $U = \{E_i(\mathbb{F}_p)\}$ be a set of elliptic curves with equal number of points, so that each element of U is uniquely determined by a j-invariant of an elliptic curve. According to the theorem 1 and the equation (4), we can consider U as a category, and the set of isogenies between elements of U as a set of morphisms of this category. Using the theorem 3, we can compute $\#U = h(D_\pi)$.

According to the equation (3), the set of isogenies between elements of U is specified by isogenies with prime degrees. For an elliptic curve with invariant j, number of isogenies having prime degree l equals number of roots of the modular polynomial (5). Exact number of isogenies can be determined using the theorem 2.

According to the theorem 2, if

$$\left(\frac{D_\pi}{l}\right) = 1, \tag{14}$$

then l-degree isogenies of elliptic curves from U form branchless cycles. Changing direction in a cycle means switching to dual isogenies. In [8] N. Elkies proposed to use such isogenies for counting points on elliptic curves over finite fields.

It is practically determined that, when $\#U$ is prime, all the elements of U form a single isogeny cycle. For further discussion, let $\#U$ be prime.

Let $l_1 \neq l$ be one more prime isogeny degree with the property that $\left(\frac{D_\pi}{l_1}\right) = 1$. In this case, l_1-degree isogenies form a cycle over U as well. Then we can put the l- and l_1-degree isogeny cycles over each other. Same can be done for other isogeny degrees of such kind.

Definition 1. *A graph, consisted of prime number of elliptic curves, connected by isogenies of degrees satisfying (14), is an isogeny star.*

The example of an isogeny star is shown on the figure 1. There are 7 elliptic curves over $\mathbb{F}_{83}$ having $T = 9$. Their j-invariants are noted in the nodes.

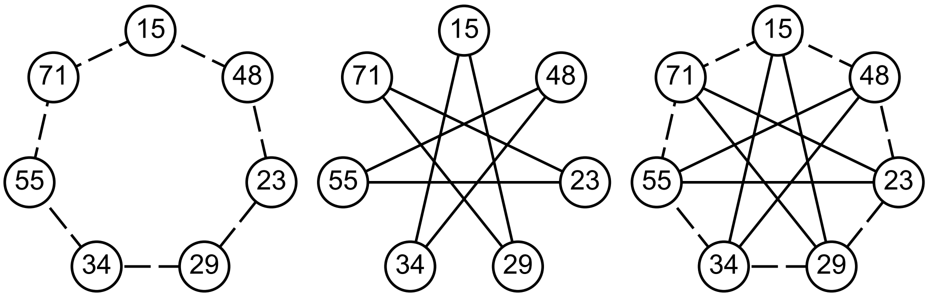

Fig. 1. 3- and 5-degree isogeny cycles, and the isogeny star.

If an isogeny star is wide enough, we can use it for cryptoalgorithm constructing. For that purpose, it is necessary to specify a direction on a cycle.

8 Direction determination on isogeny cycle

Let I_1 and I_2 be l-degree isogenies, where l satisfies the Elkies criterion (14), and

$$E_1(\mathbb{F}_p) \xleftarrow{I_1} E(\mathbb{F}_p) \xrightarrow{I_2} E_2(\mathbb{F}_p).$$

The torsion group $E[l]$ consists of $l+1$ subgroups of order l. Two of the subgroups are the kernels of I_1 and I_2. The case of $l = 3$ is shown on the figure 2. Infinite points are denoted here by 0.

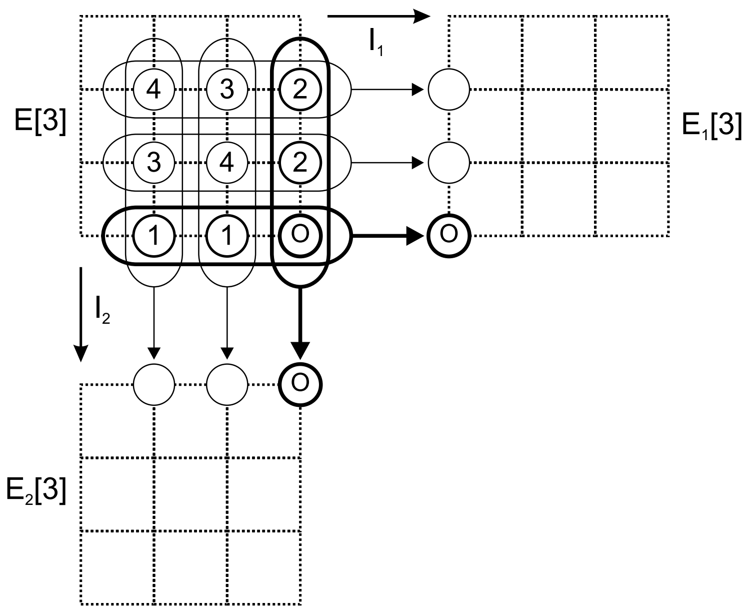

Fig. 2. Isogeny kernels mapping.

The method for direction determination on an isogeny cycle is mentioned in [9]. It uses impact of Frobenius endomorphism on an isogeny kernel. When $\left(\frac{D_\pi}{l}\right) = 1$, the Frobenius characteristic polynomial at the left side of (6), considered over $\mathbb{Z}/l\mathbb{Z}$, is decomposed to linear factors. Let $\pi_1, \pi_2 \in \mathbb{Z}/l\mathbb{Z}$ be roots of the polynomial. π_1 and π_2 are called *Frobenius eigenvalues.* Impact of Frobenius endomorphism on the kernel of an l-degree isogeny is equal to multiplication of a point by an eigenvalue:

$$(x^p, y^p) = \pi_i \cdot (x, y) \;\; \in \; \mathbb{F}_p\,[x, y] \,/\, \left(y^2 - x^3 - Ax - B,\; K_i(x)\right),$$

where $y^2 = x^3 + Ax + B$ is a curve equation, and $K_i(x)$ is a polynomial (12), which roots give the x-coordinates of the isogeny I_i kernel.

In this connection, π_1 corresponds to one cycle direction (say, positive), and π_2 - to the other one (negative).

9 Route on isogeny star

Let S be an isogeny star, $L = \{l_i\}$ - a set of Elkies isogeny degrees being used and $F = \{\pi_i\}$ - a set of Frobenius eigenvalues, which specify positive direction for every $l_i \in L$.

Definition 2. *A set $R = \{r_i\}$, where r_i is number of steps by the l_i-isogeny in the direction π_i, is a route on the isogeny star.*

For example, if we use the clockwise direction on the figure 1, then the route $R = \{2, 1\}$, being started from the node 15, follows through 48, 23 and leads to 55. We will denote it by $R(15) = 55$. Obviously, it doesn't matter, in which order we do steps of a route. The latter route can be evaluated by $15 - 48 - 34 - 55$ as well.

We can define composition of routes $A = \{a_i\}$ and $B = \{b_i\}$ as $AB = \{a_i + b_i\}$. Routes are commutative: $AB = BA$.

10 Public key encryption based on isogeny star

The ElGamal public-key encryption technique can be implemented on an isogeny star (see figure 3). You can also find an example of computations in appendix A.

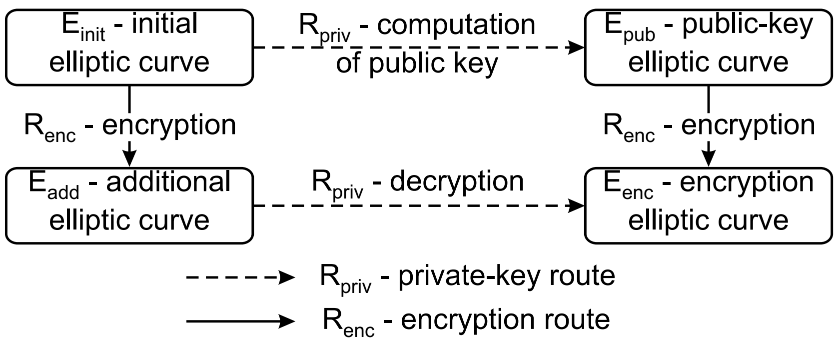

Fig. 3. Public-key encryption scheme on isogeny star.

10.1 Cryptosystem parameters

Common parameters :

- $\mathbb{F}_p$;
- E_{init} - an initial elliptic curve, specified by a pair of coefficients (A_{init}, B_{init}) of the equation (2) over $\mathbb{F}_p$;

- d - number of isogeny degrees being used;
- $L = \{l_i\},\ 1 \leq i \leq d,$ - a set of Elkies isogeny degrees being used;
- $F = \{\pi_i\},\ 1 \leq i \leq d$ - a set of Frobenius eigenvalues, which specify the positive direction for every $l_i \in L$;
- k - a limit for number of steps by one isogeny degree in a root. For any root $\{r_i\}$, numbers of steps are selected in $-k \leq r_i \leq k$.

Private key is a route R_{priv}.

Public key is an elliptic curve calculated as $E_{pub} = R_{priv}(E_{init})$. It is specified by (A_{pub}, B_{pub}).

10.2 Encryption

Input :

- common cryptosystem parameters;
- E_{pub} - a public key;
- $m \in \mathbb{F}_p$ - a cleartext;

Algorithm :

1. Choose the route R_{enc} randomly. If $R_{enc} = \{0, 0, ..., 0\}$, then repeat this step.
2. Compute $E_{enc} = R_{enc}(E_{pub})$.
3. Compute the ciphertext $s = m \cdot j_{enc} \pmod p$.
4. Compute $E_{add} = R_{enc}(E_{init})$.

Output :

- s - a ciphertext;
- E_{add} - an additional elliptic curve, specified by (A_{add}, B_{add}).

10.3 Decryption

Input :

- common cryptosystem parameters;
- R_{priv} - a private key;
- s - a ciphertext;
- E_{add} - an additional elliptic curve, specified by (A_{add}, B_{add}).

Algorithm :

1. Compute $E_{enc} = R_{priv}(E_{add})$.
2. Compute the cleartext $m = \dfrac{s}{j_{enc}} \pmod p$.

Output :

- m - a cleartext;

10.4 Encryption with point mapping

As a variant, mapping of a rational point can be used as well. The following additions should be made for that:

Cryptosystem parameters: $P_{init} \in E_{init}(\mathbb{F}_p)$ - a rational point on the initial elliptic curve is now added to common parameters. It is specified by a pair of coordinates (X_{init}, Y_{init}).

Public key: $P_{pub} \in E_{pub}(\mathbb{F}_p)$ - a rational point on the public-key curve. It is calculated as $P_{pub} = R_{priv}(P_{init})$. Thus, a whole public key is now specified by $\big((A_{pub}, B_{pub}), (X_{pub}, Y_{pub})\big)$.

Encryption :

- Additionally compute $P_{enc} = R_{enc}(P_{pub}) \in E_{enc}(\mathbb{F}_p)$.
- Compute the ciphertext now as $s = m \cdot X_{enc} \pmod p$.
- Additionally compute $P_{add} = R_{enc}(P_{init}) \in E_{add}(\mathbb{F}_p)$.
- Output of the encryption algorithm is now expanded with P_{add}.

Decryption :

- Input of the decryption algorithm is now expanded with P_{add}.
- Additionally compute $P_{enc} = R_{priv}(P_{add}) \in E_{enc}(\mathbb{F}_p)$.
- Compute the cleartext now as $m = \dfrac{s}{X_{enc}} \pmod p$.

11 Cryptosystem security

Strength of the cryptosystem proposed is based on the problem of searching for an isogeny between elliptic curves. For breaking the cryptosystem proposed in 10.2, searching for any isogeny between E_{init} and E_{pub} (or between E_{init} and E_{add}) is possible. For breaking the 10.4 cryptosystem, searching for a particular isogeny, which maps rational points in the same way as R_{priv} (or R_{enc}) does, is necessary.

The following techniques can be used for isogeny search:

- Brute-force.
  Using one isogeny degree, move from E_{init} until reaching E_{pub}.
  Another technique of such kind consists in enumerating all the possible routes from E_{init}, according to L, d and k restrictions (see 10.1), until reaching E_{pub}.
  Complexity of these attacks is estimated at $O(n)$ isogeny computations.
- Meet-in-the-middle.
  Let size of an isogeny star be n. When a star consists of one isogeny degree, average route length is $O(n)$. When a star consists of two isogeny degrees, length of such route is $O(\sqrt{n})$, since a step of one degree corresponds to some number of steps of the other one. When a star consists of m isogeny degrees, the length of such route is $S_m \approx O(mn^{\frac{1}{m}})$. It's not hard to notice, that the function $S_m(m)$ has its minimum $O(\log n)$, when $m \approx O(\log n)$.
  For the meet-in-the-middle attack, one selects $m \approx O(\log n)$ degrees of isogenies, satisfying the Elkies criterion. In this case, average length of a

route from E_{init} to E_{pub} does not exceed S_m. One constructs all the routes from E_{init}, not longer than $\frac{S_m}{2}$, and stores them in a database. Then one selects random routes with the same length criterion, applies them to E_{pub}, and looks for the result in the stored database. It should succeed with a high probability, according to the birthday paradox. Complexity of the attack is estimated at $O(\sqrt{n})$ isogeny computations.
- Method described in [14]. Its complexity is estimated at $O(\sqrt[4]{p})$.

A supposition about hardness of breaking the cryptosystem with a quantum computer relies on the following idea. Every isogeny computation at least includes solving of the equation (11). To compute a chain of q isogenies, one should consecutively solve these q equations, because of the equation parameter (j-invariant) is changed with every step. So one can't parallelize computations to avoid q steps. It relates to a quantum computer as well. For instance, the Shor's algorithm for logarithm computation implies a black box, which implements the group's multiplication operator on a quantum computer. So one cant't implement the black box with polynomial complexity. It is also noticed in [10], that the problem of breaking multivariate polynomial cryptosystem is hard for a quantum computer.

So, the strength of the cryptosystem on isogenies of elliptic curves over $\mathbb{F}_p$ is estimated at $O(\sqrt{n}) \approx O(\sqrt[4]{p})$. It is exponential from $\log p$.

12 Cryptosystem parameters selection

The section chiefly discusses selection of an initial elliptic curve E_{init}, which determines the isogeny star.

Some algorithms, e.g., the ElGamal digital signature, require computation of isogeny cycle length, what comes to a class number computation for D_π (see theorem 3).

According to the corollary 1, for obtaining a prime class number, prime discriminants should be used. Since modern algorithms compute a class number with sub-exponential complexity [7], selection of discriminants having a large prime class number is quite complicated.

In practice, a class number can be determined using analytical methods. In particular, a good approximation can be achieved by the formula from [11]:

$$h(D_\pi) \approx \frac{\sqrt{|D_\pi|}}{3,14159...} \prod_{p=2}^{P} \frac{p}{p - \left(\frac{D_\pi}{p}\right)}.$$

Product is over all the prime numbers up to some great prime P. Growth of P increases accuracy of estimation. The exact value can be achieved by brute-force search near the estimation.

The requirement of primality of $\#U$ (number of isogenous elliptic curves) can be replaced by the requirement of existence of a large prime divisor. Then cryptosystem strength will be estimated at $O(\sqrt{r})$, where r is the greatest prime divisor of $\#U$.

The method of cryptosystem parameters selection, which uses a large conductor for the discriminant D_π, is further discussed. According to the equation (10), for obtaining a large prime divisor of a class number, one should choose a prime conductor f and a discriminant D having a small class number, e.g., 1. In this case

$$h_{D_\pi} = h_D \left(f - \left(\frac{D}{f} \right) \right).$$

If $f = -D$ is prime, then

$$h_{D_\pi} = |D| h_D.$$

Bilinearity of Weil pairing (9) determines a relation between an isogeny degree and discrete logarithm in an extended field $\mathbb{F}_{p^m}$. Note that isogenous curves have equal number of points. Therefore, Weil pairing is a well-defined map between isogenous curves and one and the same field $\mathbb{F}_{p^m}$. Weil pairing computation allows determination of an isogeny degree. In order to it can't be used for reducing cryptosystem strength, it should be uncomputable (e.g., when $m \approx O(r)$).

For the cryptosystem proposed in section 10.4, E_{init} and the initial point P_{init} should be chosen in such a way that the elliptic curve discrete logarithm problem is hard. For isogeny degrees l_i with the property that $\#E_{init} \vdots l_i$, one should choose $\pi_i \neq 1$. Otherwise points of order $r \vdots l_i$ are mapped to points of order $\frac{r}{l_i}$.

For minimizing computational complexity of encryption, a number d of isogeny degrees should equal $O(\log \#U)$. In this case, a maximal number k of steps by one isogeny degree does not exceed 2 (normally equals 1).

For an elliptic curve $E(\mathbb{F}_p)$, computational complexity of an l-degree isogeny is $O(l(\log p)^2)$ [9]. Therefore, small-degree isogenies are effectively computable.

References

1. Boneh D., Lipton R. Quantum Cryptanalysis of Hidden Linear Functions. Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (LNCS 963), 1995, p. 424-437.
2. Lang S. Elliptic functions. Addison-Wesley, 1973.
3. Milne J.S. Modular functions and modular forms. `http://www.jmilne.org/math/CourseNotes/math678.pdf`.
4. Buchmann J. Algorithms for binary quadratic forms.
5. Silverman J. The arithmetic of elliptic curves. Springer-Verlag, 1986.
6. Kohel D. Endomorphism rings of elliptic curves over finite fields, PhD thesis, University of California, Berkeley, 1996.
7. Cohen H. A course in computational number theory. 3-rd edition, Springer-Verlag, 1996.

8. Elkies N. Elliptic and modular curves over finite fields and related computational issues. Pages 21-76 in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998).
9. Couveignes J.M., Dewaghe L., Morain F. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Ecole polytechnique, France, 1996.
`http://citeseer.ist.psu.edu/couveignes96isogeny.html`.
10. Ding, Schmidt. Multivariate public key cryptosystems.
`http://citeseer.ist.psu.edu/ding04multivariable.html`.
11. Shanks D., Class number, a theory of factorisation, and genera, Proceedings of the symposium on pure mathematics, vol. 20, AMS, 1971, pp. 415-440.
12. Muller V. Ein Algorithmus zur Bestimmung der Punktanzahl elliptisher Kurven uber endlichen Korpern der Charakteristik groser drei. Saarbrucken, 1995.
`http://www.informatik.tu-darmstadt.de/TI/Forschung/ECC`.
13. Lercier R., Morain F. Algorithms For Computing Isogenies Between Elliptic Curves. 1996.
`http://citeseer.ist.psu.edu/lercier96algorithm.html`.
14. S. Galbraith. Constructing isogenies between elliptic curves over finite fields, London Math. Soc., Journal of Computational Mathematics, Vol. 2, p. 118-138 (1999).
`http://www.lms.ac.uk/jcm/`

A Computation example

Here is an example of cryptosystem proposed in section 10.4. You can also get an example of cryptosystem 10.2 by leaving all the point operations out. For cryptosystem implementation, the algorithms from section 6 were used.

A.1 Cryptosystem parameters

Common parameters :

- $\mathbb{F}_{2038074743}$;
- $E_{init} = (840697433, 1239823203)$, $j_{init} = 938101947$, $T = -3891$, $-D_\pi = 8137159091$. The star size is $\#U = 55103$, - prime. $P_{init} = (4, 621053388)$, $\mathrm{ord}(P_{init}) = \#E_{init}(\mathbb{F}_{2038074743}) = 2038078635$;
- $d = 6$;
- $L = \{3, 5, 7, 11, 13, 17\}$;
- $F = \{2, 3, 2, 9, 10, 13\}$;
- $0 \leq r_i \leq 10$.

Private key $R_{priv} = \{1, 9, 5, 8, 6, 4\}$.

Public key $E_{pub} = (1849047379, 276869621)$, $j_{pub} = 1961855667$. $P_{pub} = (715302968, 227927300)$. See computation of E_{pub} and P_{pub} in table 1.

l_i	step	A	B	j	X	Y
3	1	5623338	1542326099	1184183258	735258627	1467464305
5	1	497969412	705106102	1984232860	493949346	454817148
	2	928881180	1027131125	1861937474	645370727	940759816
	3	1765734240	237516466	132956431	1502162866	1744063498
	4	1902364985	1753730248	1360958896	669541058	1833068083
	5	122819350	105454772	1483682133	1488158452	1410607222
	6	414929164	417976065	2964552	1651467709	482890778
	7	1432504470	316458305	1011356693	1230769732	1731963330
	8	172982329	1532737507	213868140	546324352	43067472
	9	1286997671	1821824507	1202857918	955414296	302107554
7	1	377485470	228798530	1061214014	68269357	1989452365
	2	742522274	500072457	1295398768	1669790941	603030735
	3	114269231	769856058	119913964	1880937108	29867989
	4	1939589665	1432757346	476536912	1810604710	1290215508
	5	857776181	845152502	1208772120	1279874638	2033873922
11	1	1150137508	1547533660	1283953029	1700025245	1634081966
	2	1401380203	1833945391	1893235954	84799743	183834053
	3	936943246	1119405533	588478707	984858414	1378736331
	4	1306360627	930962919	805177668	1085468620	61178743
	5	1265431763	842307568	1810888123	999994703	1908407076
	6	1795689391	261144439	1106469866	182737432	1233837156
	7	77599201	44132770	457404349	21348745	198235777
	8	2005860466	1029014684	1352512039	99442406	1653884660
13	1	1543793819	407283806	1817291036	1344779982	1251338105
	2	1081239924	526591467	779778495	292322478	1371605957
	3	301443158	1462045327	7714248	1336529219	1955112215
	4	2019266056	1428170059	728456393	1289680127	1920469797
	5	350948593	1340883979	322013003	1119331956	1359922373
	6	475151796	1822267465	148260912	497042363	47830495
17	1	485561054	373309690	776882232	926809325	904427639
	2	1804825631	273902413	1596279356	943458281	1286926623
	3	1661226518	357320951	1707571888	963365744	446877724
	4	1849047379	276869621	1961855667	715302968	227927300

Table 1. Computation of $(E_{pub}, P_{pub}) = R_{priv}(E_{init}, P_{init})$

l_i	step	A	B	j	X	Y
3	1	1208990544	595394248	869012729	190838460	1411383263
	2	1912521400	1688052158	964482545	1984577424	1437887221
5	1	496835268	1046532783	1247985431	899145936	1074739562
	2	88714467	448066583	193601777	353587638	1623558700
	3	1139324291	632896417	613835304	536102285	1869175128
	4	1684399050	595934546	952071356	385673120	398483212
	5	1535275944	584411538	731463788	471174314	1421294144
	6	426373764	298831248	987389217	1756561232	892905249
	7	1723254887	1809136854	1529350954	441077441	845510273
7	1	1883357505	1750748597	570602746	652546333	684954054
	2	1984860587	193084215	1598368280	487812879	454302397
	3	338351524	1285648029	1422624226	538375825	30722397
13	1	2027749523	367621897	1887486367	1041151951	1564663643
	2	1631964080	1321385215	204166526	629851264	1979857008
17	1	1502644223	1000537226	559761086	1995641973	327234176
	2	1938579915	966513714	187324713	587199285	298351326
	3	1380538716	1734438025	1879141590	263981249	409702314
	4	1246656604	1190541655	335103065	1296162698	1617646414
	5	1833569923	1928024282	1415862106	1087276245	1388984083

Table 2. Computation of $(E_{enc}, P_{enc}) = R_{enc}(E_{pub}, P_{pub})$

A.2 Encryption

Let the cleartext be $m = 1234567890$.

1. $R_{enc} = \{2, 7, 3, 0, 2, 5\}$.
2. $E_{enc} = (1833569923, 1928024282)$, $j_{enc} = 1415862106$. $P_{enc} = (1087276245, 1388984083)$. See the computation of E_{enc} and P_{enc} in table 2.
3. $s = 778556510 \equiv 1234567890 \cdot 1087276245 \pmod{2038074743}$.
   Or, without point mapping, $s = 52662893 \equiv 1234567890 \cdot 1415862106 \pmod{2038074743}$.
4. $E_{add} = (676584098, 780085609)$, $j_{add} = 2025917762$. $P_{add} = (177821233, 1165194771)$. See the computation of E_{add} and P_{add} in table 3.

A.3 Decryption

1. $E_{enc} = (1833569923, 1928024282)$, $j_{enc} = 1415862106$. $P_{enc} = (1087276245, 1388984083)$. See the computation of E_{enc} and P_{enc} in table 4.
2. $m = 1234567890 \equiv \dfrac{778556510}{1087276245} \pmod{2038074743}$.
   Or, without point mapping, $m = 1234567890 \equiv \dfrac{52662893}{1415862106} \pmod{2038074743}$.

l_i	step	A	B	j	X	Y
3	1	5623338	1542326099	1184183258	735258627	1467464305
	2	973906739	926996936	1423331616	1012656296	702593547
5	1	1485351990	1044206814	1920984729	1800183561	27610117
	2	557823387	1411529446	171171721	1991705438	1149200471
	3	1246587758	1820408125	1025448285	1815730124	850742163
	4	1304525980	891801068	1308456267	868039412	254751298
	5	1350957780	476165907	932243745	1876161440	753754367
	6	469172815	1174131630	69732628	631683592	1885710283
	7	963865851	1261117933	548896667	1227099569	2020086185
7	1	218338709	273241892	74905039	1144498937	804626961
	2	1601507492	1758313701	1165583981	1200163279	1238591775
	3	2036358308	119655713	726199613	2033866541	1257587595
13	1	535778255	1463139231	1786982245	1985838610	746457600
	2	560530122	1895982094	542575216	401751667	613273271
17	1	501928978	355829735	1030684883	785373941	796911410
	2	590570350	1072912890	251179082	1740362535	462965839
	3	1890451422	917411489	496953163	668146359	124231506
	4	1550872108	2022265167	940617213	214814991	1111122308
	5	676584098	780085609	2025917762	177821233	1165194771

Table 3. Computation of $(E_{add}, P_{add}) = R_{enc}(E_{init}, P_{init})$

l_i	step	A	B	j	X	Y
3	1	1936481645	1776242581	630090893	1660383176	1744476876
5	1	1430470609	40582855	1028483894	1898519995	372738423
	2	1148853434	1127149144	224623633	526627529	1697378396
	3	405336297	1972599311	1560624970	941978132	796336228
	4	1705910649	836961951	1345993982	1714476180	263372979
	5	650080839	38713955	641432302	419385819	1490749037
	6	4876965	1824767940	1796971660	960295277	444262786
	7	1700917220	1102900608	1549029437	853368709	1534148412
	8	80129380	895682551	604738146	401825005	1809855326
	9	333341281	1507034176	200892776	857256699	151494563
7	1	386817178	986873756	1596824085	1089063290	1200338454
	2	1163265600	1652382504	247666447	35486911	140709888
	3	1327348544	701069988	1525548901	1097445415	1244304879
	4	1872769466	876542223	1874683657	1839410064	1192237369
	5	929691044	10840617	85182430	62731743	1951339018
11	1	1379497730	338474024	612833687	873082374	168209298
	2	1383475737	1031214117	1721122710	215248691	819131015
	3	2007316327	1586858652	984201838	1032181901	716372884
	4	1092972726	1374833862	261894426	1895020752	1966433055
	5	463150383	1750328449	1685934326	1419219244	1706099551
	6	43375383	1961994791	927909690	1747038641	243009056
	7	1758645710	233863216	405123042	255784322	1288324737
	8	321948224	271622647	1996614972	1783240460	1060098696
13	1	1669193482	1770622733	1604030238	1598825265	983125723
	2	2026329675	917676361	579979385	551478229	1652437045
	3	1670631652	285103639	1654287755	1315332893	1330536855
	4	1852486988	1795498441	567185355	1304087342	1820840786
	5	25550017	1567778343	1082338500	638226480	1099370676
	6	1502644223	1000537226	559761086	1995641973	327234176
17	1	1938579915	966513714	187324713	587199285	298351326
	2	1380538716	1734438025	1879141590	263981249	409702314
	3	1246656604	1190541655	335103065	1296162698	1617646414
	4	1833569923	1928024282	1415862106	1087276245	1388984083

Table 4. Computation of $(E_{enc}, P_{enc}) = R_{priv}(E_{add}, P_{add})$