

КОМПЛЕКСНОЕ УМНОЖЕНИЕ С ПОМОЩЬЮ ИЗОГЕНИИ СТЕПЕНИ 3

Предлагается способ умножения точки эллиптической кривой на число, основанный на замене удвоения точек комплексным умножением с помощью изогении степени 3. На основе формул Велу для изогении степени 3 показано, что существуют два варианта комплексного умножения: на целое квадратичное число дискриминанта 3 и 11. Предлагаемые формулы комплексного умножения позволяют повысить скорость вычислений почти на 15%.

Rostovtsev A.G., SPbSPU

COMPLEX MULTIPLICATION BY ISOGENY OF DEGREE 3

Fast scalar multiplication method for elliptic curve points is suggested. The method is based on using complex multiplication by isogeny of degree 3 instead of point doubling. According to Velu's formulas for isogeny of odd degree it is shown that there exist two variants of complex multiplication with imaginary quadratic integer exponent of discriminant 3 and 11. Complex multiplication formulas are presented, that allows to increase the rate about 15%.

1. Эллиптические кривые и их изогении

Эллиптические кривые над простыми конечными полями широко используются в криптографии с открытым ключом. На эллиптических кривых реализованы отечественный ГОСТ Р 34.10–2001 и американский ECDSA стандарты подписи.

Эллиптическая кривая в форме Вейерштрасса $E(K)$ над полем K характеристики p задана полиномом

$$Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3, \quad (1)$$

при этом частные производные этого полинома по X , Y , Z не обращаются в нуль одновременно ни в одной точке кривой.

Если поле K конечно, то справедлива теорема Хассе: $|\#K + 1 - \#E(K)| \leq 2\sqrt{\#K}$. Число точек эллиптической кривой может быть определено по методике работы [2].

Точки эллиптической кривой — пары $(X/Z, Y/Z)$, являющиеся корнями уравнения (1), и бесконечно удаленная точка P_∞ с нулевой Z -координатой. Точки эллиптической кривой образуют абелеву группу с геометрическим законом сложения. Поэтому определена операция умножения точки на целое число, определяющая циклическую подгруппу.

Пусть $E_1(K)$ и $E_2(K)$ — две эллиптические кривые с одинаковым числом точек. Тогда существует изогения φ — алгебраическое над конечным расширением поля K отображение одной кривой в другую, такое, что $\varphi(P_\infty) = P_\infty$. Изогения задает гомоморфизм эллиптических кривых как абелевых групп. В

общем случае изогения не является биекцией и характеризуется ядром $\text{Ker}(\varphi)$, которое определяется как ядро гомоморфизма групп. Мощность ядра называется степенью изогении. Если точка $P \in \text{Ker}(\varphi)$ и $P \neq P_\infty$, то и $nP \in \text{Ker}(\varphi)$ для всех целых n . Поскольку степень изогении конечна, то ядро изогении является циклической подгруппой точек порядка l .

Изогения задает гомоморфизм групп $E_1(K)/\text{Ker}(\varphi) \rightarrow E_2(K)$, который в общем случае не является ни инъективным (ядро отлично от P_∞), ни сюръективным (не все точки $E_2(K)$ являются образами кривой $E_1(K)$). Однако если $E_1(K)$ содержит циклическую подгруппу порядка r , взаимно простого со степенью изогении, то изогения степени l является изоморфизмом подгрупп порядка r . Каждая изогения степени l имеет дуальную изогению той же степени, при этом композиция дуальных изогений отображает эллиптическую кривую в себя и соответствует умножению точки на l .

Изогения степени 1 является изоморфизмом эллиптических кривых, при этом изогения является биекцией. Эллиптические кривые с точностью до изоморфизма характеризуются инвариантом j , который является алгебраической функцией коэффициентов уравнения (1). Если $l > 1$, то j -инвариант под действием изогении меняется. Далее будут рассматриваться изогении, отличные от изоморфизмов.

Если $\varphi: E_1(K) \rightarrow E_2(K)$ — изогения степени l , то эллиптические кривые $E_1(K)$ и $E_2(K)$ называются изогенными. Бинарное отношение, определяющее изогенные кривые симметрично, рефлексивно и транзитивно, то есть является эквивалентностью.

При переходе к алгебраическому расширению L поля K выполняется включение $E(L) \supset E(K)$. При этом справедливо отображение Фробениуса $\pi: E(L) \rightarrow E(L): (X, Y, Z) \rightarrow (X^p, Y^p, Z^p)$, удовлетворяющее характеристическому уравнению

$$\pi^2 - T\pi + p = 0, \quad (2)$$

где $T = p + 1 - \#E(\mathbb{F}_p)$.

Уравнение (2) характеризуется дискриминантом $D = T^2 - 4p = f^2 D_0$, где D_0 свободно от квадратов. Если $p = a^2 + Db^2$ или $p = \frac{D+1}{4}a^2 + Dab + Db^2$, то число точек на кривой равно $p + 1 \pm 2a$ или $p + 1 \pm a$ соответственно для дискриминантов $D = \{1, 2, 3, 4, 7, 11, 12, 19, 27, 28, 43, 67, 163\}$ [2].

Для эллиптической кривой с инвариантом j_0 и изогении степени l можно определить j -инварианты изогенных эллиптических кривых как корни над K симметрического модулярного полинома $\Phi_l(u, v) | v = j_0$. Φ_l имеет степень $l + 1$ по каждой переменной. Для нечетного l модулярный полином не имеет корней, если $\left(\frac{D}{l}\right) = -1$, имеет два корня, если $\left(\frac{D}{l}\right) = 1$, и имеет 1 или $l + 1$ корень, если $\left(\frac{D}{l}\right) = 0$.

Если модулярный полином удовлетворяет условию $\Phi_l(j, j) = 0$, то изогения ϕ отображает эллиптическую кривую в себя. Это случай соответствует комплексному умножению. При этом $\phi(P) = \alpha P$, где α — целое квадратичное число отрицательного дискриминанта с нормой l .

Недостатком криптосистем на эллиптических кривых (как и всех криптосистем с открытым ключом) является низкая скорость обработки информации. Наиболее трудоемкой операцией является умножение точки на число. Традиционно эта операция выполняется путем сложения и удвоения точек. Операция удвоения точек требует 12 операций модульного умножения в поле K , операция сложения точек — 15 операций модульного умножения. Поэтому увеличение скорости вычислений возможно лишь при замене операций сложения или удвоения точек другими более быстрыми операциями. В качестве такой замены предлагается использовать комплексное умножение вместо удвоения точек.

Ранее [4] рассматривался случай замены удвоения точек комплексным умножением на целые квадратичные числа $\sqrt{-2}$ и $\frac{1+\sqrt{-7}}{2}$, которое задается изогений степени 2. В данной статье рассматривается арифметика эллиптических кривых, в которой комплексное умножение на целое квадратичное число задается изогенией степени 3.

2. Эллиптическая кривая с точкой кручения порядка 3

Изогения степени 3 в качестве ядра содержит группу, образованную точкой порядка 3. Если на кривой (1) положить $a_2 = a_4 = a_6 = 0$, получим эллиптическую кривую

$$y^2 + axy + by = x^3 \quad (3)$$

точка $R = (0, 0)$ является точкой кручения порядка 3. Инвариант этой кривой равен $j = \frac{(a^4 - 24ab)^3}{b^3(a^3 - 27b)}$.

Изогения степени 3, ядро которой определяется точкой $(0, 0)$: $(y^2 + axy + by) = (x^3 \rightarrow v^2 + auv + bv = u^3 + a_4u + a_6)$ задается формулами Велу [3]:

$$g_x(R) = 3x_R^2 - ay_R = 0;$$

$$g_y(R) = -2y_R - ax_R - b = -b;$$

$$t_R = 2g_x(R) - ag_y(R) = -ab;$$

$$s_R = g_y(R)^2 = b^2;$$

$$w = s_R + x_R t_R = b^2;$$

$$a_4 = -5t_R = -5ab;$$

$$a_6 = -a^3b - 7b^2;$$

$$u = x + \frac{t_R}{x} + \frac{s_R}{x^2};$$

$$v = y - \left(\frac{s_R(2y + ax + b)}{x^3} + \frac{t_R(ax + y)}{x^2} + \frac{as_R - g_x(R)g_y(R)}{x^2} \right);$$

После упрощения получаем

$$u = x + \frac{b}{x} \left(-a + \frac{b}{x} \right); \quad (4)$$

$$v = y - \frac{b}{x^2} \left(\frac{b(2y + ax + b)}{x} - a(ax + y - b) \right). \quad (5)$$

В проективной форме формулы для комплексного умножения имеют вид: $(U, V, W) = \alpha \cdot (X, Y, Z)$, где α — целое квадратичное число мнимого дискриминанта, такое что $\alpha\bar{\alpha} = 3$.

$$W = X^3Z;$$

$$U = X(X^3 + bZ^2(X + bZ));$$

$$V = -bZ^2(X + bZ)^2 + Y(X^3 - bZ^2(X + 2bZ)).$$

Таким образом, для комплексного умножения требуется 10 модульных умножений, тогда как формулы для удвоения точек требуют 12 модульных умножений.

Проверка показывает, что точка (u, v) лежит на новой кривой, с ненулевыми коэффициентами при x и x^0 . С учетом формул для a_4, a_6 как функций от a, b , получаем формулы для j -инвариантов эллиптической кривой. Для исходной кривой $j = \frac{(a^4 - 24ab)^3}{b^3(a^3 - 27b)}$, для ее образа $j = \frac{(a^4 + 216ab)^3}{b(a^3 - 27b)^3}$. Из равенства

j -инвариантов, получаем условия изоморфизма эллиптических кривых. Всего имеется 18 комплексных корней $a = a(b)$, из них тройной корень $a = 0$. Отбрасывая их, получаем 15 нетривиальных корней:

$$a = -3 \cdot (-2)^{2/3} b^{1/3}; a = 3 \cdot 2^{2/3} b^{1/3}; a = -3 \cdot (-1)^{2/3} \cdot 2^{1/3} \cdot b^{1/3};$$

$$a = -(-2)^{1/3} \cdot b^{1/3} (2 - 5 \cdot (-2)^{1/2})^{1/3}; a = 2^{1/3} \cdot b^{1/3} (2 - 5 \cdot (-2)^{1/2})^{1/3};$$

$$a = (-1)^{2/3} \cdot 2^{1/3} \cdot b^{1/3} (2 - 5 \cdot (-2)^{1/2})^{1/3};$$

$$a = -(-2)^{1/3} \cdot b^{1/3} (2 + 5 \cdot (-2)^{1/2})^{1/3}; a = 2^{1/3} \cdot b^{1/3} (2 + 5 \cdot (-2)^{1/2})^{1/3};$$

$$a = (-1)^{2/3} \cdot 2^{1/3} \cdot b^{1/3} (2 + 5 \cdot (-2)^{1/2})^{1/3};$$

$$a = 2 \cdot b^{1/3} (4 - (-11)^{1/2})^{1/3}; a = -2 \cdot (-1)^{1/3} \cdot b^{1/3} (4 - (-11)^{1/2})^{1/3};$$

$$a = 2 \cdot (-1)^{2/3} \cdot b^{1/3} (4 - (-11)^{1/2})^{1/3};$$

$$a = 2 \cdot b^{1/3} (4 + (-11)^{1/2})^{1/3}; a = -2 \cdot (-1)^{1/3} \cdot b^{1/3} (4 + (-11)^{1/2})^{1/3};$$

$$a = 2 \cdot (-1)^{2/3} \cdot b^{1/3} (4 + (-11)^{1/2})^{1/3};$$

Любая эллиптическая кривая $y^2 = x^3 + Ax + B$ над алгебраически замкнутым полем (и даже на квадратичном расширении исходного поля) изоморфна кривой $y^2 = x^3 + 3kx + 2k$. Сведем кривую в форме Вейерштрасса $y^2 = x^3 + 3kx + 2k$ к кривой (3). Для этого используем аффинную обратимую замену переменных:

$$u = x + \frac{c^2}{3}, \quad v = cx + y + \frac{c^4 + 9k}{6c}.$$

С учетом указанной замены переменных новое уравнение кривой имеет вид

$$-\frac{c^6}{108} - 2k - \frac{c^2k}{2} + \frac{9k^2}{4c^2} - x^3 + \frac{c^3y}{3} + \frac{3ky}{c} + 2cxy + y^2 = 0.$$

Решением уравнения относительно c можно получить нулевой свободный член, по крайней мере для кривых с дискриминантом 3, 11, 2. Условие нулевого свободного члена при заданном k задает коэффициенты a, b эллиптической кривой. Это условие задается уравнением степени 8, которое имеет 8 комплексных корней. Если кривая обладает комплексным умножением, то хотя бы один из этих 8 корней должен давать изоморфизм (сохранение j -инварианта) для одного из 15 указанных выше случаев.

Если кривая имеет комплексное умножение с помощью изогении степени 3, то показатель комплексного умножения является целым алгебраическим числом с нормой 3. Возможные показатели: $\sqrt{-3}, 1 + \sqrt{-2}, \frac{1 + \sqrt{-11}}{2}$.

3. Комплексное умножение для кривой с дискриминантом 3

Кривая имеет параметр $k = -125/121$ и $j = 54000$. В этом случае уравнение исходной эллиптической кривой с точкой кручения $(0, 0)$ порядка 3 имеет 8 различных вариантов, определяемых коэффициентами a и b . Например,

$$y^2 + 6\sqrt{-\frac{5}{11}}xy - \frac{20}{11}\sqrt{-\frac{5}{11}}y = x^3.$$

Тогда уравнение изогенной кривой и параметры изогении имеют вид:

$$v^2 + 6\sqrt{-\frac{5}{11}}uv - \frac{20}{11}\sqrt{-\frac{5}{11}}v = u^3 - \frac{3000}{121}u - \frac{122000}{1331};$$

$$g_x(R) = 3x_R^2 - ay_R = 0;$$

$$g_y(R) = -2y_R - ax_R - b = \frac{20}{11}\sqrt{-\frac{5}{11}};$$

$$t_R = 2g_x(R) - ag_y(R) = -ab = \frac{600}{121};$$

$$s_R = g_y(R)^2 = b^2 = -\frac{2000}{1331};$$

$$w = s_R + x_R t_R = b^2 = -\frac{2000}{1331};$$

$$a_4 = -5t_R = -5ab = -\frac{3000}{121};$$

$$a_6 = -a^3b - 7b^2 = -\frac{122000}{1331}.$$

Изогения степени 3 имеет вид:

$$u = \frac{1331x^3 + 6600x - 2000}{1331x^2};$$

$$v = \frac{-400\sqrt{-55}(-10 + 33x)^2 + 121y(-20 + 11x)(-200 + 220 + 121x^2)}{161051x^3}.$$

Для того чтобы существовало комплексное умножение на $\sqrt{-3}$, нужно чтобы изогенный образ кривой имел то же j , что исходная кривая, то есть хотя бы один из 15 корней $a(b)$ должен давать $a_6 = 0$.

Проверка показала, что для $c = 3\sqrt{\frac{-5}{11}}$ получается $a = 6\sqrt{\frac{-5}{11}}$, $b = -\frac{20}{11}\sqrt{\frac{-5}{11}}$, при этом $a = 3(-1)^{2/3}2^{1/3}b^{1/3}$ задает искомый изоморфизм. Для $c = -3\sqrt{\frac{-5}{11}}$ получается $a = -6\sqrt{\frac{-5}{11}}$, $b = \frac{20}{11}\sqrt{\frac{-5}{11}}$, при этом $a = -3(-1)^{2/3}2^{1/3}b^{1/3}$ задает искомый изоморфизм. Других решений, кроме этих сопряженных случаев, нет. В случае $D = 2$ и $D = 27$ изоморфизмов нет.

Уравнение для комплексного умножения имеет вид: $(u, v) = \sqrt{-3}(x, y)$,

$$u = \frac{x^3 + b(ax + b)}{x^2}, \quad v = \frac{-b(ax + b)^2 + y(x^3 - b(ax + 2b))}{x^3}.$$

С помощью изоморфизма эллиптических кривых можно получить $a = 1$, тогда условию $j = 54000$ соответствует $b = 1/54$. Получаем формулы для комплексного умножения

$$u = \frac{x^3 + \frac{1}{54}\left(x + \frac{1}{54}\right)}{x^2}, \quad v = \frac{-\frac{1}{54}\left(x + \frac{1}{54}\right)^2 + y\left(x^3 - \frac{1}{54}\left(x + \frac{2}{54}\right)\right)}{x^3}.$$

4. Комплексное умножение для кривой с дискриминантом 11

В случае кривой с дискриминантом 11 $k = -2^9/(11 \cdot 7^2)$. В этом случае уравнение исходной эллиптической кривой с точкой кручения $(0, 0)$ имеет 8 различных вариантов, задаваемых условием нулевого свободного члена.

Для того чтобы существовало комплексное умножение на $\frac{1 + \sqrt{-11}}{2}$ (или на сопряженное число) нужно чтобы изогенный образ кривой имел то же j -инвариант, что исходная кривая, то есть хотя бы один из 15 корней $a(b)$ должен соответствовать нулевому свободному члену.

Проверка показала, что

1. Для $c = \sqrt{\frac{-24}{7} + \frac{24}{7\sqrt{-11}}}$ получается:

$$a = \frac{308\sqrt{462 - 42\sqrt{-11}} - 308\sqrt{-462 + 42\sqrt{-11}}}{539(-11\sqrt{-1} + \sqrt{11})},$$

$$b = \frac{-352\sqrt{-462 - 42\sqrt{-11}} + 32\sqrt{-11(462 - 42\sqrt{-11})}}{539(-11\sqrt{-1} + \sqrt{11})}, \text{ при этом}$$

$$a = -2 \cdot (-1)^{1/3} (4b - \sqrt{-11}b)^{1/3}.$$

2. Для $c = -\sqrt{\frac{-24}{7} + \frac{24}{7\sqrt{-11}}}$ получается:

$$a = \frac{-308\sqrt{462 - 42\sqrt{-11}} + 308\sqrt{-462 + 42\sqrt{-11}}}{539(-11\sqrt{-1} + \sqrt{11})},$$

$$b = \frac{352\sqrt{-462 - 42\sqrt{-11}} - 32\sqrt{-11(462 - 42\sqrt{-11})}}{539(-11\sqrt{-1} + \sqrt{11})}, \text{ при этом}$$

$$a = 2 \cdot (-1)^{1/3} (4b - \sqrt{-11}b)^{1/3}.$$

3. Для $c = -\sqrt{\frac{-24}{7} - \frac{24}{7\sqrt{-11}}}$ получается:

$$a = \frac{-308\sqrt{462 - 42\sqrt{-11}} - 308\sqrt{-462 + 42\sqrt{-11}}}{539(11\sqrt{-1} + \sqrt{11})},$$

$$b = \frac{352\sqrt{-462 - 42\sqrt{-11}} + 32\sqrt{-11(462 - 42\sqrt{-11})}}{539(11\sqrt{-1} + \sqrt{11})}, \text{ при этом}$$

$$a = -2 \cdot (-1)^{1/3} (4b + \sqrt{-11}b)^{1/3}.$$

4. Для $c = \sqrt{\frac{-24}{7} - \frac{24}{7\sqrt{-11}}}$ получается:

$$a = \frac{-308\sqrt{462 - 42\sqrt{-11}} + 308\sqrt{-462 + 42\sqrt{-11}}}{539(11\sqrt{-1} + \sqrt{11})},$$

$$b = \frac{352\sqrt{-462 - 42\sqrt{-11}} + 32\sqrt{-11(462 - 42\sqrt{-11})}}{539(11\sqrt{-1} + \sqrt{11})}, \text{ при этом}$$

$$a = 2 \cdot (-1)^{1/3} (4b + \sqrt{-11}b)^{1/3}.$$

Рассмотренные четыре случая соответствуют комплексному умножению на показатели $\frac{\pm 1 \pm \sqrt{-11}}{2}$. Комплексное умножение выполняется по формулам (4), (5).

Других случаев комплексного умножения с помощью изогении степени 3, в частности, для $D = 2$ или $D = 27$, нет.

На практике для умножения точки на число используется окно размера 4 бита. При этом сначала вычисляются всевозможные произведения точки на 14 элементов окна, затем эти произведения складываются в соответствии с весом текущего окна. При этом согласно ГОСТ Р34.10–2001 требуется 63 сложения точек и 255 удвоений точек, то есть 4005 модульных умножений. В данном случае требуется 3495 модульных умножений, что соответствует увеличению скорости вычислений на 14,5%.

5. Представление показателя в системе счисления с комплексным основанием

Пусть порядок циклической группы, образованной точкой Q , является простым числом r . Согласно ГОСТ Р 34.10–2001 длина числа r равна 254–256 бит, согласно ESDSA — 160 бит. Для замены операции удвоения точек операцией комплексного умножения при умножении точки Q на показатель $k \in \mathbb{Z}/r\mathbb{Z}$ необходимо перевести этот показатель в систему счисления, основание которой равно показателю α комплексного умножения. Пусть κ — представление k в новой системе счисления. Тогда должно выполняться условие $\kappa \equiv k \pmod{r}$.

Если $\alpha = \sqrt{-3}$, то существует разложение порядка группы на простые множители в $\mathbb{Z}[\alpha]$:

$$r = \rho\bar{\rho} = (a + b\sqrt{-3})(a - b\sqrt{-3}).$$

Это разложение единственно, несмотря на то, что кольцо $\mathbb{Z}[\alpha]$ не является факториальным. Разложение может быть выполнено алгоритмом Полларда и

Шнорра согласно [1]. Выбором значения $\sqrt{-3} \pmod{r}$ можно обеспечить равенство $\rho \equiv 0 \pmod{r}$, при этом идеал (ρ) максимален. Тогда имеет место изоморфизм конечных полей $\mathbb{Z}/(r) \cong \mathbb{Z}[\alpha]/(a + b\sqrt{-3})$. Перевод в систему счисления с основанием α основан на переходе от поля $\mathbb{Z}/(r)$ к полю классов вычетов по идеалу (ρ) .

Два комплексных числа ξ и η сравнимы по идеалу (ρ) , если существует такое $\gamma \in \mathbb{Z}[\alpha]$, что $\xi = \eta + \gamma\rho$.

Перевод в систему счисления с основанием α выполняется следующим образом.

1. Найти представление $k \equiv k_0 + k_1\sqrt{-3} \pmod{\rho}$, такое, что норма представления как комплексного числа минимальна. При этом обеспечивается неравенство $k_0^2 + 3k_1^2 < r$. Для этого вычислить оптимальную длину n_0 шага в вещественном направлении, для которого норма числа $k' = k - n_0\rho$ минимальна. Затем вычислить оптимальную длину n_1 шага в мнимом направлении, для которого норма числа $k' - \alpha n_1\rho$ минимальна. Поскольку вещественное и мнимое направления ортогональны, требуется всего два шага для минимизации.
2. Найти представление k_0, k_1 в троичной системе счисления с цифрами $\{0, 1, -1\}$: $k_0 = \sum_{i=0}^h K_i^0 3^i$, $k_1 = \sum_{i=0}^h K_i^1 3^i$. Тогда искомое представление имеет вид $k = K_0^0 + K_0^1\sqrt{-3} - K_1^0\sqrt{-3}^2 - K_1^1\sqrt{-3}^3 + \dots$.

Аналогично выполняется переход в случае $\alpha = \frac{1 + \sqrt{-11}}{2}$. При этом можно использовать равенство $\alpha\bar{\alpha} = 3$, то есть следует использовать смешанную систему счисления с основаниями α и $\bar{\alpha}$. В этом случае на первом этапе нужно найти представление $r = \rho\bar{\rho} = (a + b\alpha)(a + b\bar{\alpha})$ и выбрать $\rho \equiv 0 \pmod{r}$. Затем найти представление $k \equiv k_0 + k_1\alpha \pmod{\rho}$ с минимальной нормой. При этом может потребоваться несколько итераций, так как направления минимизации 1 и α неортогональны. Для сокращения числа итераций можно сначала выполнять минимизацию в ортогональных направлениях 1 и $\sqrt{-11}$, затем при необходимости провести еще одну итерацию для направлений 1 и α . Далее показатели k_0, k_1 представить в троичной системе счисления, положив $\alpha\bar{\alpha} = 3$. В полученном представлении как полиноме от комплексного основания числа α и $\bar{\alpha}$ должны чередоваться.

Литература

1. **Ростовцев А. Г.** Алгебраические основы криптографии. — СПб.: Мир и Семья, Интерлайн, 2000.
2. **Ростовцев А. Г., Маховенко Е. Б.** Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
3. **Atsushi Sato.** On certain extensions of number fields obtained from elliptic curves with rational torsion points, October, 1, 2001 (Internet publication).
4. **Rostovtsev A.G., Makhovenko E.B.** Elliptic Curve Point Multiplication // International Association for Cryptologic Research. Cryptology ePrint Archive // <http://eprint.iacr.org/2003/088/>.