Math-Net.Ru

Общероссийский математический портал

О. Н. Василенко, О вычислении кратных точек на эллиптических кривых над конечными полями с использованием нескольких оснований систем счисления и новых видов координат, *Матем. вопр. криптогр.*, 2011, том 2, выпуск 1, 5–28

DOI: <https://doi.org/10.4213/mvk24>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.157.27.8

26 апреля 2023 г., 16:32:17

УДК: 512.742.72

**О вычислении кратных точек
на эллиптических кривых
над конечными полями
с использованием нескольких оснований
систем счисления и новых видов координат**

О. Н. Василенко

Лаборатория ТВП, Москва

Получено 22.IV.2010

В работе проведен обзор алгоритмов вычисления кратных точек на эллиптических кривых над конечными полями. Предложен новый эффективный алгоритм вычисления кратных точек на одном классе кривых с использованием эндоморфизмов, двух оснований систем счисления и кватернионов Якоби.

Ключевые слова: эллиптические кривые, кратные точки, системы счисления, вычислительные алгоритмы

Point multiplication on elliptic curves over finite fields using many-base number systems and new types of coordinates

O. N. Vasilenko

TVP Laboratory, Moscow

Abstract. We review a number of algorithms for point-by-scalar multiplication on elliptic curves over finite fields. A new effective algorithm is given for point-by-scalar multiplication on some classes of curves using endomorphisms, double-base number system and Jacobi quartics.

Key words: elliptic curves, elliptic curve point-by-scalar multiplication, double-base number system, computational algorithms

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 1, pp. 5–28 (Russian).

1. Введение

В работе изучаются способы использования новых видов координат на эллиптических кривых над конечными полями и нескольких оснований систем счисления для ускорения вычисления кратных точек на этих кривых. Мы предлагаем также способ вычисления кратных точек на эллиптических кривых одного класса, который в настоящее время имеет наилучшую оценку сложности по сравнению с имеющимися общими методами.

Информацию о традиционно использовавшихся видах координат на кривых и методах вычисления кратных точек можно найти в книгах [3, 11, 12] и статье [2] (см. также [1, гл. 4; 42, гл. 4]).

Мы будем обозначать через $\check{M}, \check{S}$ сложности одного умножения и возведения в квадрат в основном поле соответственно, а через $v_p(k)$ — кратность вхождения простого числа p в разложение натурального числа k на множители.

2. Координаты Хесса

Эллиптической кривой в форме Хесса над полем $\mathbb{K}$ называется кривая

$$u^3 + v^3 + 1 = 3Duv, \quad D \in \mathbb{K}, \quad D^3 \neq 1, \quad (1)$$

см. [25, 32, 39]. В проективных координатах она имеет вид

$$U^3 + V^3 + W^3 = 3DUVW. \quad (2)$$

Такая кривая изоморфна эллиптической кривой в стандартной форме Вейерштрасса

$$y^2 = x^3 - 27D(D^3 + 8)x + 54(D^6 - 20D^3 - 8); \quad (3)$$

изоморфизм задается формулами

$$x = -9D^2 + 12u(D^3 - 1)/(Du + v + 1), \quad y = 36(v - 1)(D^3 - 1)/(Du + v + 1).$$

Ноль кривой (2) — точка $O = (1 : -1 : 0)$. Обратной к точке $P = (U : V : W)$ является точка $-P = (V : U : W)$. Суммой точек $P = (U_1 : V_1 : W_1)$ и $Q = (U_2 : V_2 : W_2)$ является точка $R = (U_3 : V_3 : W_3)$, вычисляемая по формулам

$$U_3 = V_1^2 U_2 W_2 - V_2^2 U_1 W_1, \quad V_3 = U_1^2 V_2 W_2 - U_2^2 V_1 W_1, \quad W_3 = W_1^2 U_2 V_2 - W_2^2 U_1 V_1.$$

Удвоение точки вычисляется по аналогичной формуле:

$$2(U_1 : V_1 : W_1) = (W_1 : U_1 : V_1) + (V_1 : W_1 : U_1).$$

Для вычисления суммы точек и удвоения требуется 12 умножений и 3 вычитания в основном поле.

Использование координат Хесса на кривой противодействует некоторым видам атак с побочного канала. Действительно, при вычислении кратной точки dP для некоторого секретного ключа d замеры времени с побочного канала не позволят определить биты d , так как при очередной итерации удвоения и сложения различных точек проводятся по одним и тем же формулам и занимают примерно одинаковое время.

В работе [27] приведены новые формулы для сложения точек в модифицированных координатах Хесса. Такими координатами называется набор

$$(X : Y : Z : R : S : T : U : V : W) = \\ = (X : Y : Z : X^2 : Y^2 : Z^2 : 2XY : 2XZ : 2YZ).$$

Сложение

$$(X_3 : Y_3 : Z_3 : R_3 : S_3 : T_3 : U_3 : V_3 : W_3) = \\ = (X_1 : Y_1 : Z_1 : R_1 : S_1 : T_1 : U_1 : V_1 : W_1) + \\ + (X_2 : Y_2 : Z_2 : R_2 : S_2 : T_2 : U_2 : V_2 : W_2)$$

проводится по формулам

$$X_3 = S_1 V_2 - V_1 S_2, \quad Y_3 = R_1 W_2 - W_1 R_2, \quad Z_3 = T_1 U_2 - U_1 T_2, \\ R_3 = X_3^2, \quad S_3 = Y_3^2, \quad T_3 = Z_3^2, \\ U_3 = (X_3 + Y_3)^2 - R_3 - S_3, \quad V_3 = (X_3 + Z_3)^2 - R_3 - T_3, \\ V_3 = (Y_3 + Z_3)^2 - S_3 - T_3.$$

Сложность вычисления составляет $6\ddot{M} + 6\ddot{S}$.

Удвоение

$$(X_3 : Y_3 : Z_3 : R_3 : S_3 : T_3 : U_3 : V_3 : W_3) = \\ = 2(X_1 : Y_1 : Z_1 : R_1 : S_1 : T_1 : U_1 : V_1 : W_1)$$

проводится по формулам

$$X_3 = (U_1 - W_1)(V_1 + 2(R_1 + T_1)), \quad Y_3 = (V_1 - U_1)(W_1 + 2(S_1 + T_1)), \\ Z_3 = (W_1 - V_1)(U_1 + 2(R_1 + S_1)), \quad R_3 = X_3^2, \quad S_3 = Y_3^2, \quad T_3 = Z_3^2, \\ U_3 = (X_3 + Y_3)^2 - R_3 - S_3, \quad V_3 = (X_3 + Z_3)^2 - R_3 - T_3, \\ W_3 = (Y_3 + Z_3)^2 - S_3 - T_3.$$

Сложность вычисления составляет $3\ddot{M} + 6\ddot{S}$.

3. Координаты Лопеса – Дахаба

Здесь мы рассматриваем эллиптическую кривую над полем $GF(2^d)$ вида

$$y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0, \quad (4)$$

см. [33, 36]. В координатах Лопеса – Дахаба $(X : Y : Z)$, где $(x, y) = (X/Z, Y/Z^2)$, она имеет вид

$$Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4, \quad (5)$$

и нулем является точка $(1 : 0 : 0)$. Сложение точек $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ проводится по формулам

$$\begin{aligned} A_1 &= X_1Z_2, & A_2 &= X_2Z_1, & C &= A_1 + A_2, \\ B_1 &= A_1^2, & B_2 &= A_2^2, & D &= B_1 + B_2, \\ E_1 &= Y_1Z_2^2, & E_2 &= Y_2Z_1^2, & F &= E_1 + E_2, \\ G &= CF, & Z_3 &= Z_1Z_2D, & X_3 &= A_1(E_2 + B_2) + A_2(E_1 + B_1), \\ Y_3 &= (A_1G + E_1D)D + (G + Z_3)X_3. \end{aligned}$$

Сложность вычисления составляет $13\check{M} + 4\check{S} + 9\check{A}$, где $\check{A}$ – сложность одного сложения в основном поле. Удвоение точки $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ проводится по формулам

$$\begin{aligned} S &= X_1^2, & U &= S + Y_1, & T &= X_1Z_1, & Z_3 &= T^2, & T &= UT, \\ X_3 &= U^2 + T + aZ_3, & Y_3 &= (Z_3 + T)X_3 + S^2Z_3 \end{aligned}$$

со сложностью $4\check{M} + 4\check{S} + 5\check{A} + \check{a}$, где $\check{a}$ – сложность одного умножения на a .

При $a = 1$ можно также использовать формулы

$$\begin{aligned} S &= X_1^2, & T &= \sqrt{b}Z_1^2, & U &= X_1Z_1, & Z_3 &= U^2, \\ X_3 &= (S + T)^2, & Y_3 &= (US + (Y_1 + T)(S + T))^2 \end{aligned}$$

со сложностью $3\check{M} + 5\check{S} + 3\check{A} + \check{\sqrt{b}}$, где $\check{\sqrt{b}}$ – сложность умножения на $\sqrt{b}$. При $a = 0$ можно использовать формулы

$$\begin{aligned} S &= X_1^2, & T &= \sqrt{b}Z_1^2, & S &= S + T, & U &= X_1Z_1, & Z_3 &= U^2, \\ X_3 &= S^2, & Y_3 &= (UT + (Y_1 + T)S)^2 \end{aligned}$$

со сложностью $3\check{M} + 5\check{S} + 3\check{A} + \check{\sqrt{b}}$.

Мы видим, что удвоение в координатах Лопеса – Дахаба проводится эффективно; поэтому данные формулы рекомендуется использовать для вычисления кратных точек на эллиптических кривых над полями характеристики 2.

В работе [18] вводятся модифицированные координаты Лопеса – Дахаба на кривой

$$y^2 = x^3 + ux^2 + 16ux \quad (6)$$

над полем характеристики больше 2. Точка $(x, y) = (X/Z, Y/Z^2)$ представляется набором (X, Y, Z, Z^2) . Удвоение точки $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ проводится по формулам

$$\begin{aligned} A &= X_1^2, & B &= X_1^2 - 16uZ_1^2, & Y_t &= Y_1B, & X_3 &= B^2, & Z_3 &= 4Y_1^2, \\ C &= X_1^2(uZ_1^2), & D &= Z_3^2, & E &= u(Z_3 - 4C), & Y_3 &= Y_t(2X_3 + E + 256C) \end{aligned}$$

со сложностью $3\check{M} + 4\check{S} + 2\check{y}$, где $\check{y}$ — сложность одного умножения на u . Если u выбрано так, что сложность умножения на него невелика, то сложность удвоения фактически составит $3\check{M} + 4\check{S}$. Данные формулы получены путем разложения изогении удвоения точки в произведение двух дуальных изогений. Аналогичные результаты могут быть получены для кривых

$$y^2 = x^3 + 3u(x + 1)^2 \quad (7)$$

с использованием упрощенных координат Якоби – Чудновского, определение этих координат см. в [2]. Там же получены новые формулы для утроения точки путем разложения изогении утроения в произведение двух дуальных изогений и показано, что на кривых (6), (7) вычисление кратных точек указанными методами может быть проведено быстрее, чем с использованием NAF-методов или метода работы [13].

4. Координаты на эллиптических кривых в форме пересечения Якоби

Эллиптической кривой в форме пересечения Якоби над полем $\mathbb{K}$ называется кривая, задаваемая системой уравнений

$$\begin{cases} s^2 + c^2 = 1, \\ as^2 + d^2 = 1, \end{cases}$$

относительно переменных s, c, d , где $a \in \mathbb{K}$, $a \neq 1$, см. [7, 34]. Ноль кривой представим набором $(0, 1, 1)$. Обратной к точке (s, c, d) является точка $(-s, c, d)$.

Введем новые координаты $(S : C : D : T)$, $(s, c, d) = (S/T, C/T, D/T)$, $T \neq 0$. Расширим их до набора

$$(S : C : D : T : U : V) = (S : C : D : T : SC : DT).$$

Этот набор называется модифицированными координатами на пересечении Якоби (см. [27]). Сложение

$$\begin{aligned} & (S_3 : C_3 : D_3 : T_3 : U_3 : V_3) = \\ & = (S_1 : C_1 : D_1 : T_1 : U_1 : V_1) + (S_2 : C_2 : D_2 : T_2 : U_2 : V_2) \end{aligned}$$

проводится по формулам

$$\begin{aligned} E &= S_1 D_2, \quad F = C_1 T_2, \quad G = D_1 S_2, \quad H = T_1 C_2, \quad J = U_1 V_2, \quad K = V_1 U_2, \\ S_3 &= (H + F)(E + G) - J - K, \quad C_3 = (H + E)(F - G) - J + K, \\ D_3 &= (V_1 - a U_1)(U_2 + V_2) + a J - K, \quad T_3 = (H + G)^2 - 2K, \quad U_3 = S_3 C_3, \quad V_3 = D_3 T_3. \end{aligned}$$

Сложность вычисления составит $11\check{M} + \check{S} + 2\check{a}$, где $\check{a}$ — сложность умножения на a .

Удвоение

$$(S_3 : C_3 : D_3 : T_3 : U_3 : V_3) = 2(S_1 : C_1 : D_1 : T_1 : U_1 : V_1)$$

проводится по формулам

$$\begin{aligned} E &= V_1^2, \quad F = U_1^2, \quad G = aF, \quad T_3 = E + G, \quad D_3 = E - G, \\ C_3 &= 2(F + C_1^4) - T_3, \quad S_3 = (U_1 + V_1)^2 - E - F, \quad U_3 = S_3 C_3, \quad V_3 = D_3 T_3. \end{aligned}$$

Сложность вычисления составит $2\check{M} + 5\check{S} + \check{a}$.

Мы видим, что если сложность умножения на a невелика, то удвоение точек на эллиптической кривой в форме пересечения Якоби над конечным полем характеристики больше двух проводится более эффективно, чем в модифицированных координатах Лопеса – Дахаба на изоморфной ей кривой вида (6) из предыдущего параграфа.

5. Расширенные системы координат на кватриках Якоби

Эллиптической кривой в форме кватрики Якоби называется кривая вида

$$y^2 = x^4 + 2ax^2 + 1, \quad a^2 \neq 1, \quad (8)$$

определенная над полем $GF(p)$ (см. [7, 10, 22, 26, 27]). Эта кривая изоморфна эллиптической кривой в форме Вейерштрасса вида

$$2v^2 = u^3 - 2au^2 + (a^2 - 1)u. \quad (9)$$

Изоморфизм задается соотношениями

$$u = a + (y + 1)/x^2, \quad v = u/x.$$

Пусть $(x, y) = (X/Z, Y/Z^2), Z \neq 0$. Тогда мы можем рассматривать в качестве координат точки на кривой

$$Y^2 = X^4 + 2aX^2Z^2 + Z^4 \quad (10)$$

набор $(X : Y : Z)$.

Расширенная система координат на кватернике Якоби может быть определена разными способами (см. [7, 10, 22, 26, 27]). Мы будем следовать определению работы [27], в которой предложены наиболее эффективные формулы для сложения и удвоения точек. Мы будем называть расширенной системой координат на кватернике Якоби набор

$$(X : Y : Z : U : V : W) = (X : Y : Z : X^2 : Z^2 : XZ).$$

Сложение

$$\begin{aligned} & (X_3 : Y_3 : Z_3 : U_3 : V_3 : W_3) = \\ & = (X_1 : Y_1 : Z_1 : U_1 : V_1 : W_1) + (X_2 : Y_2 : Z_2 : U_2 : V_2 : W_2) \end{aligned}$$

проводится по формулам

$$\begin{aligned} A &= U_1U_2, \quad B = V_1V_2, \quad C = W_1W_2, \quad D = Y_1Y_2, \\ X_3 &= (W_1 + Y_1)(W_2 + Y_2) - C - D, \quad Z_3 = B - A, \quad U_3 = X_3^2, \quad V_3 = Z_3^2, \\ F &= A + B + 2C, \quad G = (U_1 + V_1)(U_2 + V_2) + kC + D, \quad H = U_3 + V_3, \\ Y_3 &= FG - H, \quad W_3 = ((X_3 + Z_3)^2 - H)/2, \end{aligned}$$

где $k = 2(a - 1)$. Сложность вычисления составит $7\check{M} + 3\check{S} + \check{k}$, где $\check{k}$ — сложность умножения на k .

Удвоение

$$(X_3 : Y_3 : Z_3 : U_3 : V_3 : W_3) = 2(X_1 : Y_1 : Z_1 : U_1 : V_1 : W_1)$$

проводится по формулам

$$A = U_1 + V_1, \quad X_3 = 2Y_1W_1, \quad Z_3 = A(V_1 - U_1), \quad U_3 = X_3^2, \\ V_3 = Z_3^2, \quad B = U_3 + V_3, \quad W_3 = ((X_3 + Z_3)^2 - B)/2, \quad Y_3 = 2(Y_1A)^2 - B.$$

Сложность вычисления составит $3\check{M} + 4\check{S}$. Можно также использовать формулы

$$X_3 = 2Y_1W_1, \quad Z_3 = (V_1 - U_1)(V_1 + U_1), \quad U_3 = X_3^2, \quad V_3 = Z_3^2, \\ W_3 = ((X_3 + Z_3)^2 - U_3 - V_3)/2, \quad Y_3 = 2Y_1^4 - aU_3 - V_3.$$

Сложность вычисления составит $2\check{M} + 5\check{S} + \check{a}$, где $\check{a}$ — сложность умножения на a .

В дальнейшем нам понадобятся формулы для утроения точек на кватриках Якоби. Утроение мы опишем, модифицируя результат [26] применительно к рассматриваемым координатам. Вычисление

$$(X_3 : Y_3 : Z_3 : U_3 : V_3 : W_3) = 3(X_1 : Y_1 : Z_1 : U_1 : V_1 : W_1)$$

проводится по формулам

$$A = (U_1)^2, \quad B = (V_1)^2, \quad C = 2((U_1 + V_1)^2 - (A + B)), \\ D = (a^2 - 1)C^2, \quad E = 4(A - B), \quad F = 2(A + B) + aC, \quad G = E^2, \\ H = F^2, \quad J = (E + F)^2 - (G + H), \quad K = 2(H - D), \\ X_3 = X_1(J - K), \quad Y_3 = Y_1(K^2 - 4GD), \quad Z_3 = Z_1(J + K), \\ U_3 = X_3^2, \quad V_3 = Z_3^2, \quad W_3 = X_3Z_3.$$

Сложность вычисления составит $7\check{M} + 10\check{S}$. При $a = 0$ (этот случай нам также понадобится) сложность вычисления составит $5\check{M} + 10\check{S}$.

По эффективности вычислений расширенная система координат на кватрике Якоби уступает в некоторых случаях лишь инвертированным координатам Эдвардса, описанным ниже, а во многих случаях превосходит их. Сравнение эффективности вычисления кратных точек в этих видах координат можно найти в работе [27].

Аналогичные результаты для кривых вида

$$y^2 = dx^4 + 2ax^2 + 1, \quad 256d(a^2 - d)^2 \neq 0, \quad (11)$$

были получены в работе [28].

6. Использование координат Эдвардса и их модификаций

В данном пункте мы будем использовать следующие обозначения: p — простое число, $p > 3$, E — эллиптическая кривая над $GF(p)$, задаваемая уравнением

$$y^2 = x^3 + ax + b, \text{ где } a, b \in GF(p), 4a^3 + 27b^2 \neq 0. \quad (12)$$

В работе [23] рассматриваются кривые вида

$$x^2 + y^2 = c^2(1 + x^2y^2). \quad (13)$$

Такие кривые называются кривыми Эдвардса. Показано, что кривая (12) изоморфна над некоторым расширением $GF(p)$ кривой (13) при некотором выборе c , $c^5 \neq c$. Это означает, что кривая (13) также является эллиптической. Кривые в форме Эдвардса зависят лишь от одного параметра c и симметричны по переменным x, y .

Закон сложения на кривой (13) задается формулами

$$(x, y) + (x', y') = \left(\frac{1}{c} \cdot \frac{xy' + yx'}{1 + xyx'y'}, \frac{1}{c} \cdot \frac{yy' - xx'}{1 - xyx'y'} \right).$$

В работе [8] рассматривается более общий класс кривых

$$x^2 + y^2 = c^2(1 + dx^2y^2), \quad (14)$$

и в этом классе — подкласс

$$x^2 + y^2 = 1 + dx^2y^2. \quad (15)$$

Кривые вида (14), (15) также называются кривыми Эдвардса. В [8] доказана следующая теорема.

Теорема 1. Пусть E — эллиптическая кривая над $GF(p)$, $p > 3$, и пусть в группе точек $E(GF(p))$ есть элемент порядка 4. Если в $E(GF(p))$ имеется единственный элемент порядка 2, то существует такой элемент $d \in GF(p)$, не являющийся квадратом, что E изоморфна над $GF(p)$ кривой $x^2 + y^2 = 1 + dx^2y^2$.

Построение изоморфизма проводится следующим образом. Пусть $P = (r_1, s_1)$ — точка порядка 4, $2P = (r_2, s_2)$. После линейной замены можно считать, что $2P = (0, 0)$, и уравнение кривой E имеет вид

$$y^2 = x^3 + a_2x^2 + a_4x.$$

Поскольку $s_1 \neq 0$ (иначе P — порядка 2), то и $r_1 \neq 0$. Из уравнения кривой тогда получаем, что $r_1^2 = a_4$ и $a_2 = s_1^2/r_1^2 - 2r_1$. Положим $d = 1 - 4r_1^3/s_1^2$. Тогда $a_2 = 2\frac{1+d}{1-d}r_1$. Очевидно, что $d \neq 0$, $d \neq 1$. Также d не является квадратом в $GF(p)$, иначе на кривой есть еще одна точка второго порядка $(r_1(\sqrt{d} + 1)/(\sqrt{d} - 1), 0)$. Кривая E изоморфна той из кривых

$$E': \frac{r_1}{1-d}y^2 = x^3 + a_2x^2 + a_4x, \quad (16)$$

$$E'': \frac{dr_1}{1-d}y^2 = x^3 + a_2x^2 + a_4x, \quad (17)$$

у которой коэффициент при y^2 является квадратом. При замене

$$u = x/r_1, \quad v = y/r_1$$

кривая E' переходит в кривую

$$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u, \quad (18)$$

а кривая E'' переходит в кривую

$$\frac{d}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u. \quad (19)$$

Кривая (15) изоморфна (18) (изоморфизм задается формулой $x = 2u/v$, $y = (u - 1)/(u + 1)$). Кривая $x^2 + y^2 = 1 + \frac{1}{d}x^2y^2$ изоморфна (19) (изоморфизм задается аналогичной формулой с заменой d, u на $1/d, -u$). Итак, мы описали построение изоморфизма и тем самым доказали теорему.

Сложение на кривой (14) задается формулой

$$(x, y) + (x', y') = \left(\frac{xy' + yx'}{c(1 + dxyx'y')}, \frac{yy' - xx'}{c(1 - dxyx'y')} \right). \quad (20)$$

Свойством этого закона сложения является то, что при параметре d , не являющемся квадратом в $GF(p)$, закон определен для любой пары точек кривой (14) без исключения (см. [8, теорема 3.3]).

Перейдем от кривой (14) к проективной кривой

$$(X^2 + Y^2)Z^2 = c^2(Z^4 + dX^2Y^2) \quad (21)$$

с нулевым элементом $(0 : c : 1)$. Обратным к элементу $(X : Y : Z)$ является элемент $(-X : Y : Z)$. Вычисление суммы точек

$$(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) \quad (22)$$

проводится по формулам

$$\begin{aligned} A &= Z_1 Z_2, \quad B = A^2, \quad C = X_1 X_2, \quad D = Y_1 Y_2, \\ E &= dCD, \quad F = B - E, \quad G = B + E, \\ X_3 &= AF((X_1 + Y_1)(X_2 + Y_2) - C - D), \\ Y_3 &= AG(D - C), \quad Z_3 = cFG. \end{aligned}$$

Если обозначить через $\check{c}, \check{d}, \check{A}$ сложности одного умножения на c , умножения на d и сложения-вычитания в основном поле соответственно, то сложность вычисления (22) составит $10\check{M} + \check{S} + \check{c} + \check{d} + 7\check{A}$.

Удвоение точки $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ проводится по формулам

$$\begin{aligned} B &= (X_1 + Y_1)^2; \quad C = X_1^2; \quad D = Y_1^2; \quad E = C + D; \quad H = (cZ_1)^2; \\ J &= E - 2H; \quad X_3 = c(B - E)J; \quad Y_3 = cE(C - D); \quad Z_3 = EJ. \end{aligned}$$

Сложность составит $3\check{M} + 4\check{S} + 3\check{c} + 5\check{A}$.

В работе [8] приведены таблицы, которые показывают, что вычисление суммы точек в координатах Эдвардса имеет меньшую сложность, чем в координатах Доче–Икарта–Кехеля, Якоби, координатах пересечения Якоби, проективных координатах, в некоторых видах координат на кватриках Якоби и в координатах Хесса. То же справедливо для удвоения точки и для сложения точек с использованием NAF-алгоритмов и «оконных» методов с длиной окна 4. Это означает, что применение координат Эдвардса для вычисления кратных точек на кривых имеет меньшую сложность, чем в других указанных координатах.

Теперь определим инвертированные координаты Эдвардса (см. [9]). Рассмотрим кривую (15). Инвертированными координатами Эдвардса называются координаты $(X : Y : Z)$,

$$(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4. \quad (23)$$

Для этих координат, как и для проективных, справедливо равенство

$$(X : Y : Z) = (\lambda X : \lambda Y : \lambda Z) \quad \text{при } \lambda \neq 0.$$

Здесь, однако, есть четыре исключительные точки $(0, 1)$, $(0, -1)$, $(1, 0)$, $(-1, 0)$ на (15), для которых следует использовать представления $(1 : 0 : 0)$,

$(-1 : 0 : 0)$, $(0 : -1 : 0)$, $(0 : 1 : 0)$; для этих точек происходит нарушение однородности. Вычисление суммы точек происходит по формулам

$$\begin{aligned} A &= Z_1 Z_2, & B &= dA^2, & C &= X_1 X_2, & D &= Y_1 Y_2, \\ H &= C - D, & I &= (X_1 + Y_1)(X_2 + Y_2) - C - D, \\ X_3 &= (E + B)H, & Y_3 &= (E - B)I, & Z_3 &= AHI. \end{aligned}$$

Сложность вычисления составляет $9\check{M} + \check{S} + \check{d} + 7\check{A}$. Сложность удвоения в инвертированных координатах Эдвардса составит $3\check{M} + 4\check{S} + \check{d} + 6\check{A}$. Таким образом, в инвертированных координатах Эдвардса сложность вычислений меньше, чем в координатах Эдвардса. В большинстве случаев эти координаты и расширенные системы координат на квартиках Якоби для вычисления кратных точек на эллиптических кривых над конечными полями являются наиболее эффективными.

В работе [27] приведены новые формулы для сложения точек в инвертированных координатах Эдвардса со сложностью $11\check{M}$.

В работе [5] приведен анализ методов вычисления кратных точек kP с использованием двух оснований системы счисления для записи k и с использованием координат Эдвардса, инвертированных координат Эдвардса, либо некоторых видов расширенных систем координат на квартиках Якоби. Показано, что применение двух оснований системы счисления в этом случае либо совсем не дает выигрыша, либо выигрыш очень незначителен. В указанных системах координат следует использовать одно основание системы счисления.

Можно также (см. [6]) рассматривать кривые вида

$$a'x^2 + y^2 = 1 + d'x^2y^2, \quad (24)$$

где a', d' — различные ненулевые элементы поля. Эти кривые называются скрученными кривыми Эдвардса. Такие кривые изоморфны кривым вида (15); изоморфизм задается отображением $(x, y) \rightarrow (x\sqrt{a'}, y)$. Сложность вычисления суммы точек на (24) составляет $10\check{M} + \check{S} + \check{a}' + \check{d}' + 7\check{A}$. Такие кривые можно использовать для вычисления кратных точек в некоторых специальных случаях. В работе [29] показано, в частности, что на кривой

$$-x^2 + y^2 = 1 + dx^2y^2$$

сложение точек может быть выполнено за $8\check{M} + \check{d}$ операций.

7. Использование двух оснований систем счисления для вычисления кратных точек на эллиптических кривых

Использование двух оснований систем счисления для вычисления кратных точек на эллиптических кривых впервые было предложено в работах [14, 15]. Мы будем рассматривать представление натурального числа k в виде

$$k = \sum_{i=1}^m s_i 2^{b_i} 3^{t_i}, \quad s_i = \pm 1, \quad b_i, t_i \geq 0. \quad (25)$$

Такое представление мы будем называть DBSN-представлением.

Теорема 2. *Для каждого натурального числа k существует представление (25) с $m = O(\log k / \log \log k)$.*

Данная теорема доказана в [16] с помощью оценок линейных форм от логарифмов алгебраических чисел (см. [41]) и не является конструктивной. Это означает, что у нас нет быстрого алгоритма построения представления (25) с наименьшим значением m или с каким-либо m , удовлетворяющим теореме 2. Заметим, что с помощью указанного в теореме представления мы можем вычислить кратную точку на кривой kP за $O(\log k / \log \log k)$ арифметических операций, т.е. с сублинейной сложностью (меньшей, чем линейная).

Для практических приложений мы будем использовать так называемое DBC-представление вида

$$k = \sum_{i=1}^m s_i 2^{b_i} 3^{t_i}, \quad s_i = \pm 1, \quad b_i \leq b_{i+1}, t_i \leq t_{i+1}. \quad (26)$$

Такое представление нетрудно получить с помощью следующего несложного алгоритма. Для заданного k мы фиксируем границы $b_{\max}, t_{\max}$, $2^{b_{\max}} 3^{t_{\max}} > k$. При очередной итерации мы находим ближайшее к k число вида $2^b 3^t$, $b \leq b_{\max}$, $t \leq t_{\max}$, вычисляем и сохраняем знак разности $k - 2^b 3^t$ и затем переприсваиваем $k := |k - 2^b 3^t|$, $b_{\max} := b$, $t_{\max} := t$. Заметим, что в этом алгоритме важно, что основаниями системы счисления являются именно 2 и 3, поскольку как только очередное приближение примет вид 3^t , дальнейшие слагаемые в строящейся сумме (26) могут быть только степенями 3. В этом случае мы можем в записи текущего k в троичной системе счисления заменить коэффициенты 2 на $3 - 1$, т.е. использовать представление вида $\sum_j \pm 3^j$.

Замечание. Нахождение ближайшего к k числа вида $2^b 3^t$ проводится достаточно быстро, если использовать предварительно вычисленную и упорядоченную таблицу чисел такого вида (или их логарифмов).

Несколько иной метод построения представления (26) предложен в работе [17]. Суть метода описывается следующим образом. Строится граф. В исходную его вершину помещаем число k в виде $k = 2^{v_2(k)} 3^{v_3(k)} k_1$. Затем выпускаем из нее два ребра, на концах которых помещаем аналогичные представления для $k_1 - 1$ и $k_1 + 1$. Продолжаем этот процесс с получившимися концевыми вершинами. На очередном шаге мы убираем все повторяющиеся концевые вершины (кроме одной) и также убираем все концевые вершины, кроме B минимальных. В результате, дойдя до 1, мы получим искомого представление (возможно, даже не одно). Результаты экспериментов показывают, что оптимальным является значение $B = 4$. Эвристическая оценка средней длины получаемых представлений при $B = 1$ составляет примерно $\log_2 k / 4.6419$. При $B = 4$ экспериментальная оценка близка к $\log_2 k / 4.9$, хотя доказать это пока не удастся даже с помощью эвристических аргументов.

Замечание. В [17] приведен график, который показывает зависимость от B средней длины строящихся представлений для чисел различной битовой длины (от 256 до 512 битов). Из него следует, что увеличение B от 4 до 128 влияет на эту среднюю длину очень слабо.

С использованием DBC-представления (26) мы получаем следующий алгоритм вычисления кратной точки kP на кривой.

Алгоритм вычисления $Q = kP$.

1 шаг. $Q := s_1 P$.

2 шаг. Для $i = 1, \dots, m - 1$ выполнить следующие операции:

$u := b_i - b_{i+1}, \quad v := t_i - t_{i+1},$

$Q := 3^v Q, \quad Q := 2^u Q, \quad Q := Q + s_{i+1} P.$

3 шаг. Вычислить и выдать $Q := Q 2^{b_m} 3^{t_m}$.

Конец описания алгоритма.

В работе [15] для вычисления кратной точки kP на кривой с использованием DBC-представлений рекомендуется использовать якобиевы координаты (см. [2]). При этом для утроения точки $P = (X_1, Y_1, Z_1)$ предложены формулы

$$M = 3X_1^2 + aZ_1^4, \quad E = 12X_1Y_1^2 - M^2, \quad T = 8Y_1^4,$$

$$X_3 = 8Y_1^2(T - ME) + X_1E^2,$$

$$Y_3 = Y_1(4(ME - T)(2T - ME) - E^3), \quad Z_3 = Z_1E.$$

Сложность составляет $9\check{M} + 7\check{S}$. В работе [15] на основе численных экспериментов показано, что предложенный метод быстрее методов NAF, 4-NAF и методов [30, 31]. Нетривиальные теоретические оценки сложности метода здесь получить пока не удастся, поскольку нет нетривиальных оценок длины представления (26), подобных теореме 2. Скорее всего, длина такого представления будет существенно больше, чем оптимальная длина представления теоремы 2.

В работе [20] предложено использовать представления вида

$$k = \sum_{i=1}^m d_i 2^{b_i} 3^{t_i}, \quad b_i \leq b_{i+1}, \quad t_i \leq t_{i+1}, \quad (27)$$

где d_i принадлежат некоторому фиксированному множеству S , содержащему 1. Алгоритм построения представления (27) аналогичен алгоритму построения (26). Алгоритм вычисления $Q = kP$ очевидным образом модифицируется на 2 шаге: $Q := Q + d_{i+1}P$. Заметим, что в представлении (27) мы можем использовать и другие основания систем счисления, а не только 2 и 3; нужно только соответствующим образом выбирать множество S . Данный метод на практике является более быстрым, чем предыдущий, однако и здесь сравнение возможно только путем экспериментов. Кроме того, в [5] указано, что в работе [20] используются не оптимальные формулы сложения точек и виды уравнений кривых.

Дальнейшая разработка способов использования двух оснований систем счисления для вычисления кратных точек на эллиптических кривых над конечными полями проведена в работе [21]. Здесь рассматривается ситуация, в которой необходимо эффективно вычислять кратные точки вида $nP + mQ$. Для этого необходимо уметь вычислять подходящие представления для пар натуральных чисел m, n . Один из возможных видов такого представления — совместная разреженная форма, JSF — рассматривался ранее в работе [40]. В [21] предлагается рассматривать представления

$$n = \sum_{i=1}^l c_i 2^{a_i} 3^{b_i}, \quad m = \sum_{i=1}^l d_i 2^{a_i} 3^{b_i}, \quad (28)$$

где $c_i, d_i \in \{0, \pm 1\}$. Такое представление называется JDBNS-представлением. Сокращенно мы будем записывать (28) в виде

$$\left| \begin{matrix} n \\ m \end{matrix} \right| = \sum_{i=1}^l \left| \begin{matrix} c_i \\ d_i \end{matrix} \right| 2^{a_i} 3^{b_i}.$$

Плотностью JDBNS-представления называется отношение l к максимуму двоичных длин n, m . Для эффективного вычисления кратных точек вида $nP + mQ$ также предлагается рассматривать JDBC-представления вида (28), в которых $a_l \geq a_{l-1} \geq \dots \geq a_1$, $b_l \geq b_{l-1} \geq \dots \geq b_1$. Алгоритм нахождения JDBC-представлений достаточно очевиден. Для его описания через $v_p(x, y)$, $p = 2, 3$, мы будем обозначать $\min(v_2(x)v_2(y)), \min(v_3(x)v_3(y))$ соответственно. Также рассмотрим функцию $\text{gain}(x, y)$, которая вычисляет тройку чисел: наибольший из множителей $2^{v_2(x-c, y-d)} 3^{v_3(x-c, y-d)}$, $c, d \in \{0, \pm 1\}$, и саму пару c, d . Обозначим через $\mathcal{S}$ множество пар натуральных чисел (x, y) , у которых $v_2(x, y) = v_3(x, y) = 0$.

Алгоритм нахождения JDBC-представлений состоит в следующем. Для построения JDBC-представления пары чисел n, m мы делим их на $2^{v_2(m, n)} 3^{v_3(m, n)}$ и получаем пару чисел $(x, y) \in \mathcal{S}$. Далее вычисляем $\text{gain}(x, y)$ и заменяем (x, y) на $((x - c)/2^{v_2(x-c, y-d)} 3^{v_3(x-c, y-d)}, (y - d)/2^{v_2(x-c, y-d)} 3^{v_3(x-c, y-d)})$. Затем продолжаем итерации. Корректность этого метода построения JDBC-представления очевидна, а его характеристики исследованы в [21].

Теорема 3. *Средняя плотность вычисляемых описанным алгоритмом JDBC-представлений содержится в интервале $[0.3942, 0.3945]$. Средние значения наибольших степеней 2 и 3 в соответствующих представлениях приблизительно равны $0.55 \log_2 n$ и $0.28 \log_2 n$.*

Как следует из теоремы, по сравнению с JSF в JDBC-представлениях в среднем на 21 процент меньше слагаемых, что позволяет существенно ускорить вычисление кратных точек вида $nP + mQ$.

В работе [19] предложена также гибридная бинарно-тернарная совместная форма HBTJF. Алгоритм ее построения подобен алгоритму построения JDBC. В результате его работы получается представление вида

$$n = \sum_{i=1}^l c_i 2^{a_i} 3^{b_i}, \quad m = \sum_{i=1}^l d_i 2^{a_i} 3^{b_i}, \quad (29)$$

где $c_i, d_i \in \{0, \pm 1\}$. На практике JDBC-представление для вычисления $nP + mQ$ более эффективно, так как требует меньшего числа предварительных вычислений.

В работе [35] изучается представление чисел с использованием нескольких оснований систем счисления, называемое mbNAF. Такое представ-

ление имеет вид

$$k = \sum_{i=1}^m s_i \prod_{j=1}^J a_j^{c_i(j)}, \quad (30)$$

где a_i — простые числа из множества оснований $\mathcal{A}$, a_1 — главное основание. Здесь величины s_i принадлежат некоторому фиксированному множеству ненулевых целых чисел D , $c_i(j)$ — невозрастающие показатели, $c_1(j) \geq c_2(j) \geq \dots \geq c_m(j) \geq 0$, $j = 2, \dots, J$, $c_i(1)$ — невозрастающие показатели для главного основания, $c_i(1) \geq c_{i+1}(1) + 2$, $1 \leq i \leq m-1$. С использованием (30) вычисление кратной точки проводится по формуле

$$\begin{aligned} kP = \\ = \prod_{j=1}^J a_j^{d_m(j)} \left(\prod_{j=1}^J a_j^{d_{m-1}(j)} \left(\dots \left(\prod_{j=1}^J a_j^{d_1(j)} (s_1 P) + s_2 P \right) + \dots + s_{m-1} P \right) + s_m P \right). \end{aligned}$$

Аналогично, с введением длины окна w можно определить представление wmbNAF.

Алгоритм построения mbNAF является естественным обобщением алгоритмов построения DBC-представлений, описанных выше. Из исходного k мы выносим все возможные степени $a_1 \dots, a_J$, затем из получившегося числа вычитаем подходящий элемент $s \in D$, чтобы результат делился на некоторые из $a_1 \dots, a_J$, и продолжаем процесс. Аналогично строится и представление wmbNAF. Можно (см. [35]) указать средние величины для количества сложений, удвоений и утроений точек на кривой при использовании mbNAF и wmbNAF, когда $\mathcal{A} = \{2, 3\}$. Аналогичные оценки получены и при $\mathcal{A} = \{2, 3, 5\}$.

В [35] также рассматриваются другие виды представлений, так называемые дробные wmbNAF и рафинированные wmbNAF. Описанные в этой работе результаты экспериментов показывают эффективность рассмотренных представлений, особенно в сочетании с использованием расширенных систем координат на кватриках Якоби.

В работах [37, 38] рассматриваются возможности использования нескольких оснований систем счисления для вычисления кратных точек на эллиптических кривых над конечными полями. В частности, предложены некоторые модификации алгоритма Яо [43] с использованием чисел Фибоначчи и представлений вида $k = \sum_{i=1}^m s_i 2^i$ с достаточно большими значениями коэффициентов s_i .

8. Использование на некоторых специальных кривых двух оснований систем счисления, одно из которых является квадратичной иррациональностью

В работе [4] исследуются методы вычисления кратных точек с использованием двух оснований систем счисления на кривых Коблица E_a над $GF(2^l)$, l – простое,

$$y^2 + xy = x^3 + ax^2 + 1, \quad a = 0 \text{ или } a = 1, \quad (31)$$

и на суперсингулярных кривых E_b над $GF(3^m)$

$$y^2 = x^3 - x + b, \quad b = \pm 1. \quad (32)$$

На кривых Коблица E_a отображение Фробениуса $(x, y) \rightarrow (x^2, y^2)$, удовлетворяющее квадратному уравнению $X^2 - (-1)^{1-a}X + 2 = 0$, соответствует мнимой квадратичной иррациональности $\tau = ((-1)^{1-a} + \sqrt{-7})/2$, лежащей в евклидовом кольце $\mathbb{Z}[\tau]$. Это позволяет быстро вычислять представления натуральных чисел в виде

$$n = \sum_{i=0}^{k-1} (-1)^{e[i]} A^{s[i]} \tau^{t[i]}, \quad e[i] = 0, 1, \quad (33)$$

где $A = 3$ или $A = \bar{\tau}$, и использовать такие представления для вычисления кратных точек nP . Умножение $\tau \cdot P$ есть действие отображения Фробениуса на точку P , что соответствует двум возведениям в квадрат в основном поле. С использованием представления (33), в котором $s[i+1] \geq s[i]$ и $t[i+1] > t[i]$ при $s[i+1] = s[i]$ для всех i , получаем следующий алгоритм вычисления nP .

Алгоритм вычисления $Q = nP$.

1 шаг. $Q := O$, $i := k - 1$, $s[-1] := 0$.

2 шаг. Пока $i \geq 0$, выполнять шаги 3-7.

3 шаг. Найти наименьшее $j \leq i$, для которого $s[j] = s[i]$.

4 шаг. $R := (-1)^{e[i]} P$.

5 шаг. Пока $i > j$, выполнять

$$R := \tau^{t[i]-t[i-1]} R + (-1)^{e[i-1]} P, \quad i := i - 1.$$

6 шаг. $Q := Q + \tau^{t[i]} R$.

7 шаг. $Q := A^{s[i]-s[i-1]} Q$.

8 шаг. Выдать Q .

Конец описания алгоритма.

Корректность алгоритма проверяется непосредственно. Как доказано в [4], в среднем $k \leq (1 + o(1)) \log n / \log \log n$, $n \rightarrow \infty$, что позволяет вычислять кратные точки на кривой Коблица в среднем за $O(\log n / \log \log n)$ операций на кривой, т. е. с сублинейной сложностью. В [4] также приведены результаты численных экспериментов, показывающие преимущество предлагаемого метода перед методами, использующими τ -NAF представления для n и τ -NAF представления ширины w .

Для суперсингулярных кривых (32) следует использовать представление $n = \sum_{i=0}^{k-1} 2^{s[i]} 3^{t[i]}$, поскольку утроение точки на такой кривой делается быстро: $3P = (x^9 - b, -y^9)$. Здесь также в среднем k не превосходит $(1 + o(1)) \log n / \log \log n$, $n \rightarrow \infty$.

В работе [21] также предложены способы ускорения вычисления кратных точек на кривых Коблица.

9. Эффективный метод вычисления кратных точек на эллиптических кривых одного класса

Здесь мы опишем новый способ вычисления кратных точек на эллиптических кривых одного класса и получим оценку его сложности, которая лучше оценок сложности известных в настоящее время методов.

Рассмотрим эллиптическую кривую

$$Y^2 = X^3 - \frac{1}{4}X \quad (34)$$

над $GF(p)$, p — простое, $p > 3$, $p \equiv 1 \pmod{4}$. Эта кривая не является суперсингулярной и обладает эффективно вычислимым эндоморфизмом ϕ , $\phi(X, Y) = (-X, iY)$, где i — элемент четвертого порядка в $GF(p)$ (см. [2, 24]).

Пусть $P \in E(GF(p))$ — точка простого порядка $N \neq p$ и $E[N] \not\subset E(GF(p))$. Тогда ϕ действует на $\langle P \rangle_N$ как умножение на λ , где $\lambda \in \mathbb{Z}$, $\lambda^2 \equiv -1 \pmod{N}$, $0 < \lambda < N$.

При вычислении кратной точки kP , согласно результатам работ [2, 24], мы эффективно находим представление

$$k \equiv k_1 + k_2 \lambda \pmod{N}, \quad 0 \leq k_1, |k_2| \leq \sqrt{N/2}. \quad (35)$$

Затем вычисляем

$$kP = k_1P + k_2Q, \quad Q = \phi(P) = \lambda P. \quad (36)$$

Это вычисление мы будем проводить, используя обобщенные координаты на квартике Якоби и JDBC-представление для пары k_1, k_2 . Согласно приведенным выше формулам, квартика Якоби будет иметь вид

$$y^2 = x^4 + 1, \quad (37)$$

и отображение ψ из (34) в (37) задается формулами

$$\begin{aligned} x &= X/Y, \\ y &= \frac{(2X - a)X^2}{Y^2} - 1. \end{aligned}$$

Переходя на кривую (37), мы вычисляем точку

$$T = \psi(kP) = k_1\psi(P) + k_2\psi(Q),$$

используя JDBC-представление (28) в виде

$$\begin{vmatrix} k_1 \\ k_2 \end{vmatrix} = \sum_{i=1}^l \begin{vmatrix} c_i \\ d_i \end{vmatrix} 2^{a_i} 3^{b_i},$$

и затем находим искомую точку $kP = \psi^{-1}(T)$. По теореме 3 величина l в среднем не превосходит при больших N

$$0.3945 \cdot \log_2(N/2)^{1/2} = 0.1973 \cdot \log_2 N.$$

При этом максимальная степень 2 в среднем примерно равна

$$0.55 \log_2(N/2)^{1/2} = 0.275 \log_2 N,$$

а максимальная степень 3 в среднем примерно равна

$$0.28 \log_2(N/2)^{1/2} = 0.14 \log_2 N.$$

Поэтому для вычисления T указанным методом нам потребуется в среднем $l = 0.1973 \log_2 N + O(1)$ сложений различных точек плюс $0.275 \log_2 N + O(1)$ удвоений плюс $0.14 \log_2 N + O(1)$ утроений. Пользуясь приведенными выше формулами для сложений, удвоений и утроений на квартиках Якоби и оценками их сложности, получаем, что сложность вычисления кратной точки kP в среднем не превосходит

$$\begin{aligned} &O(\log N) + 0.1973 \cdot \log_2 N (7\check{M} + 3\check{S}) + 0.275 \log_2 N (2\check{M} + 5\check{S}) + \\ &+ 0.14 \log_2 N (5\check{M} + 10\check{S}) + 2\check{I} + 4\check{M} + 2\check{S} = \\ &= O(\log N) + 2.632 \cdot \log_2 N \cdot \check{M} + 3.367 \cdot \log_2 N \cdot \check{S} + 2\check{I} + 4\check{M} + 2\check{S}, \quad (38) \end{aligned}$$

где $\check{I}$ — сложность одной инверсии в основном поле. Величина $2\check{I} + 4\check{M} + 2\check{S}$ появляется за счет перехода к квартике Якоби (37) и обратно к кривой (34).

Мы доказали следующую теорему.

Теорема 4. Пусть E — эллиптическая кривая (34), $P \in E(GF(p))$ — точка простого порядка $N \neq p$ и $E[N] \not\subset E(GF(p))$. Тогда можно вычислить кратную точку kP со сложностью, в среднем не превосходящей $O(\log N) + (2.632 \cdot \log_2 N + 4) \cdot \check{M} + (3.367 \cdot \log_2 N + 2) \cdot \check{S} + 2\check{I}$.

ЗАМЕЧАНИЕ. Можно проводить вычисления только на кривой (37), не пользуясь формой Вейерштрасса (34). Тогда вообще не надо будет делать инверсии, и сложность вычислений составит $O(\log N) + 2.632 \cdot \log_2 N \cdot \check{M} + 3.367 \cdot \log_2 N \cdot \check{S}$.

Сравним полученные результаты с оценками сложности из работы [7], в которой даны наиболее обширные и детальные результаты сравнения различных методов вычисления кратных точек. Как и в [7], мы предположим, что $\check{S} = 0.8\check{M}$, $\check{I} = 8\check{M}$, и рассмотрим 160-значные модули, т.е. положим $\log_2 N = 160$. Тогда наилучшая оценка работы [7] составит $1285.9\check{M}$. Оценка теоремы 4 без учета $O(\log N)$ составит примерно $(441.12 + 540.72 \cdot 0.8)\check{M} \approx 873.7\check{M}$. Мы видим, что наилучший метод [7] по сложности примерно в $1285.9/873.7 \approx 1.47$ (т.е. в полтора раза) хуже предложенного нами метода. Если не использовать форму Вейерштрасса, а работать только с квартикой Якоби, то инверсий не будет, и оценка сложности нашего метода примет вид $421.12\check{M} + 538.72\check{S} = 852.1\check{M}$, а отношение оценок сложностей равно $1285.9/852.1 \approx 1.51$.

Список литературы

1. Василенко О.В. Теоретико-числовые алгоритмы в криптографии. 2-е изд. — МЦНМО, М., 2006, 334 с.
2. Василенко О.В. Новые методы вычисления кратной точки на эллиптической кривой над конечным полем. — Труды по дискретной математике. Т. 11, вып. 2. — М.: ФИЗМАТЛИТ, 2008, с. 5–30.
3. Avanzi R., Cohen H., Doche C., Frey G., Nguyen K., Lange T., Vercauteren F. Handbook of elliptic and hyperelliptic curve cryptography. — Chapman and Hall/CRC, 2005, 808 pp.
4. Avanzi R., Dimitrov V., Doche C., Sica F. Extending scalar multiplication using double bases. — ASIACRYPT'2006, Lect. Notes Comput. Sci., 2006, v. 4284, p. 130–144.

5. Bernstein D., Birkner P., Lange T., Peters C. Optimizing double-base elliptic curve single-scalar multiplication. — INDOCRYPT'07, Lect. Notes Comput. Sci., 2007, v. 4859, p. 167–182.
6. Bernstein D., Birkner P., Lange T., Peters C. Twisted Edwards curves. — AFRICACRYPT'08, Lect. Notes Comput. Sci., 2008, v. 5023, p. 389–405.
7. Bernstein D., Lange T. Analysis and optimization of elliptic-curve single-scalar multiplication. — Cryptology ePrint Archive, Report 2007/455.
8. Bernstein D., Lange T. Faster addition and doubling on elliptic curves. — ASIACRYPT'07, Lect. Notes Comput. Sci., 2008, v. 4833, p. 29–50.
9. Bernstein D., Lange T. Inverted Edwards coordinates. — AAEECC-17, Lect. Notes Comput. Sci., 2007, v. 4851, p. 20–27.
10. Billet O., Joye M. The Jacobi model of an elliptic curve and side-channel analysis. — Lect. Notes Comput. Sci., 2003, v. 2643, p. 34–42.
11. Blake I., Seroussi G., Smart N. Elliptic curves in cryptography. — Cambridge: Cambridge Univ. Press, 1999, 204 pp.
12. Blake I., Seroussi G., Smart N. Advances in elliptic curve cryptography. — Cambridge: Cambridge Univ. Press, 2005, 296 pp.
13. Ciet M., Joye M., Lauter K., Montgomery P. L. Trading inversions for multiplications in elliptic curve cryptography. — Cryptology ePrint Archive, Report 2003/257.
14. Dimitrov V., Imbert L., Mishra P. Fast elliptic curve point multiplication using double-base chains. — Cryptology ePrint Archive, Report 2005/069.
15. Dimitrov V., Imbert L., Mishra P. Efficient and secure elliptic curve point multiplication using double-base chains. — ASIACRYPT'2005, Lect. Notes Comput. Sci., 2005, v. 3788, p. 59–78.
16. Dimitrov V., Julien G., Miller W. An algorithm for modular exponentiation. — Inf. Process. Lett., 1998, v. 66, № 3, p. 155–159.
17. Doche C., Habsieger L. A tree-based approach for computing double-base chains. — ACISP'2008, Lect. Notes Comput. Sci., 2008, v. 5107, p. 433–446.
18. Doche C., Icart T., Kohel D. Efficient scalar multiplication by isogeny decomposition. — PKC'2006, Lect. Notes Comput. Sci., 2006, v. 3958, p. 191–206.
19. Doche C., Imbert L. The double-base number system in elliptic curve cryptography. — Preprint, 2008.
20. Doche C., Imbert L. Extended double-base number system with applications to elliptic curve cryptography. — INDOCRYPT'2006, Lect. Notes Comput. Sci., 2006, v. 4329, p. 335–348.

21. *Doche C., Kohel D., Sica F.* Double-base number system for multi-scalar multiplications. — EUROCRYPT'2009, Lect. Notes Comput. Sci., 2009, v. 5479, p. 502–519.
22. *Duquesne S.* Improving the arithmetic of elliptic curves in the Jacobi model. — Inf. Process. Lett., 2007, v. 104, p. 101–105.
23. *Edwards H.* A normal form for elliptic curves. — Bull. Amer. Math. Soc., 2007, v. 44, № 3, p. 393–422.
24. *Gallant R. P., Lambert R. J., Vanstone S. A.* Faster point multiplication on elliptic curves with efficient endomorphisms. — CRYPTO'2001, Lect. Notes Comput. Sci., 2001, v. 2139, p. 190–200.
25. *Hesse O.* Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. — J. reine ang. Math., 1844, № 28, p. 68–96.
26. *Hisil H., Carter G., Dawson E.* New formulae for efficient elliptic curve arithmetic. — INDOCRYPT'2007, Lect. Notes Comput. Sci., 2007, v. 4859, p. 138–151.
27. *Hisil H., Wong K.-H., Carter G., Dawson E.* Faster group operations on elliptic curves. — Cryptology ePrint Archive, Report 2007/441.
28. *Hisil H., Wong K.-H., Carter G., Dawson E.* Jacobi quartic curves revisited. — Cryptology ePrint Archive, Report 2009/312.
29. *Hisil H., Wong K.-H., Carter G., Dawson E.* Twisted Edwards curves revisited. — Cryptology ePrint Archive, Report 2008/522.
30. *Izu T., Möller B., Takagi T.* Improved elliptic curve multiplication methods resistant against side channel attacks. — INDOCRYPT'2002, Lect. Notes Comp. Science, 2002, v. 2551, p. 269–313.
31. *Izu T., Takagi T.* Fast elliptic curve multiplications resistant against side channel attacks. — IEICE Trans. Fund., 2005, v. 88, p. 161–171.
32. *Joye M., Quisquater J.-J.* Hessian elliptic curves and side-channel attacks. — CHES'2001, Lect. Notes Comput. Sci., 2001, v. 2162, p. 402–410.
33. *Lange T.* A note on López-Dahab coordinates. — Cryptology ePrint Archive, Report 2006/323.
34. *Liardet P., Smart N.* Preventing SPA/DPA in ECC systems using the Jacobi form. — In: CHES'2001, Lect. Notes Comput. Sci., 2001, v. 2162, p. 391–401.
35. *Longa P., Gebotys C.* Fast multibase methods and other several optimizations for elliptic curve scalar multiplication. — PKC'2009, Lect. Notes Comput. Sci., 2009, v. 5443, p. 443–462.
36. *López J., Dahab R.* Improved algorithms for elliptic curve arithmetic in $GF(2^n)$. — Tech.Rep. IC-98-39, Relatorio Tecnico, October 1998.

- 37. *Meloni N., Hasan M.* Elliptic curve point scalar multiplication combining Yao's algorithm and double bases. — Univ. Waterloo, preprint, 2009.
- 38. *Meloni N., Hasan M.* Exponentiation using a large-digit representation and ECC applications. — Univ. Waterloo, preprint, 2009.
- 39. *Smart N.* The Hessian form of an elliptic curve. — CHES'2001, Lect. Notes Comput. Sci., 2001, v. 2162, p. 118–125.
- 40. *Solinas J.* Low-weight binary representations for pairs of integers. — Combin. and Optim. Res. Rep., CORR 2001-41, Univ. Waterloo, 2001.
- 41. *Tijdeman R.* On the maximal distance between integers composed of small primes. — *Compositio Math.*, 1974, v. 28, p. 159–162.
- 42. *Vasilenko O.* Number-theoretic algorithms in cryptography. — Transl. Math. Monogr., v. 232, AMS, 2007.
- 43. *Yao A.* On the evaluation of powers. — *SIAM J. Comput.*, 1976, v. 5, № 1, p. 100–103.