УДК 681.3.06

КРИПТОСТОЙКИЕ СКРУЧЕННЫЕ КРИВЫЕ ЭДВАРДСА С МИНИМАЛЬНОЙ СЛОЖНОСТЬЮ ГРУППОВЫХ ОПЕРАЦІЙ

А.В. БЕССАЛОВ, К.А. ОЛЕШКО, Д.Н. ПОРЕЧНАЯ, О.В. ЦЫГАНКОВА, О.Н. ЧЕРНЫЙ

Дан анализ оценок сложности групповых операций для скрученных кривых Эдвардса. Предложен метод минимизации вычислений путем выбора минимального значения параметра кривой. Приведены таблицы общесистемных параметров 25 криптостойких рекордно быстрых кривых со значениями модулей поля длиной 192, 224, 256, 384 и 521 бит.

Ключевые слова: скрученные кривые Эдвардса, полные кривые Эдвардса, порядок кривой, порядок точки, квадратичный вычет, квадратичный невычет, сложность операций.

ВВЕДЕНИЕ

Термин «скрученные кривые Эдвардса» был введен авторами работы [2]. В работе [6] мы дали критический анализ противоречий, некорректных определений и статистики распределений числа кривых разных классов в работе [2] и предложили новую классификацию кривых в обобщенной форме Эдвардса, одним из классов которых мы и рассматриваем скрученные кривые Эдвардса. Важным свойством этих кривых является то, что при $p = 1 mod 4$ все они имеют порядок $4n$ (n – нечетное) с минимальным четным кофактором 4. Циклическая подгруппа этих кривых простого порядка n обладает всеми преимуществами полных кривых Эдвардса [1], что открывает пути для их криптографических приложений и стандартизации.

Для полных кривых Эдвардса над простым полем задача поиска криптостойких кривых и их табуляция впервые была решена нами в работе [4]. В данной работе мы решаем ту же задачу для нециклических скрученных кривых Эдвардса. В разделе 1 приведен анализ сложности групповых операций на них и полных кривых Эдвардса в проективных координатах. Далее в разделе 2 мы предлагаем метод минимизации сложности операций путем использования минимального значения параметра a кривой. В разделе 3 описан метод и инструменты поиска быстрых криптостойких скрученных кривых Эдвардса с табуляцией результатов расчетов общесистемных параметров 25 кривых в диапазоне стандартных значений модуля поля.

1. СЛОЖНОСТЬ ГРУППОВЫХ ОПЕРАЦИЙ НА СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА

В работе [6] мы предложили новую классификацию кривых в обобщенной форме Эдвардса с уравнением

$$E_{a,d}: \begin{matrix} x^2 + ay^2 = 1 + dx^2 y^2, \\ a, dF_p^*, d \neq 1, \ \ a \neq d, \ p \neq 2. \end{matrix} \qquad (1)$$

В зависимости от свойств квадратичности параметров a и d в [6] определены 3 непересекающиеся класса кривой (1): полные кривые Эдвардса ($\left(\frac{ad}{p}\right) = -1$), скрученные кривые Эдвардса ($\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$) и квадратичные кривые Эдвардса ($\left(\frac{a}{p}\right) = 1 \left(\frac{d}{p}\right) = 1$). В данном разделе мы приведем оценки сложности групповых операций для первых двух классов, интересных для криптографических задач. Модифицированный универсальный закон сложения точек кривой (1) имеет вид [5]

$$(x_1, y_1) + (x_2, y_2) = \\ = \left(\frac{x_1 x_2 - a y_1 y_2}{1 - d x_1 x_2 y_1 y_2}, \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2} \right). \qquad (2)$$

При совпадении двух точек получим из (2) закон удвоения точек

$$2(x_1, y_1) = \left(\frac{x_1^2 - a y_1^2}{1 - d x_1^2 y_1^2}, \frac{2 x_1 y_1}{1 + d x_1^2 y_1^2} \right). \qquad (3)$$

Использование модифицированных законов (2), (3) позволяет сохранить общепринятую горизонтальную симметрию (относительно оси x) обратных точек. Нейтральный элемент группы здесь равен $\boldsymbol{O} = (1,0)$. Определяя теперь обратную точку как $-P = -(x_1, y_1) = (x_1, -y_1)$, получим согласно (1) $(x_1, y_1) + (x_1, -y_1) = (1,0) = \boldsymbol{O}$. Кроме нейтрального элемента $\boldsymbol{O}$ на оси x также всегда лежит точка $D_0 = (-1,0)$ второго порядка, для которой в соответствии с (3) $2D_0 = (1,0) = \boldsymbol{O}$. В зависимости от свойств параметров a и d можно получить еще 2 особые точки второго порядка, а также 0, 2, 4, 6, или 8

точек 4-го порядка. Как следует из (1), на оси *y* могут лежать точки $\pm F_0 = \left(0, \pm 1/\sqrt{a}\right)$ 4-го порядка, для которых $\pm 2F_0 = D_0 = \left(-1, 0\right)$. Эти точки существуют над полем $\mathbf{F}_p$, если параметр *a* является квадратичным вычетом.

1.1.Сложение точек

Для полных кривых Эдвардса этот анализ приведен в работе [1]. Так как в уравнении кривой (1) появился новый параметр a, требуется оценить, насколько он увеличивает вычислительные затраты. Введем третью координату Z как общий знаменатель в (2). Пусть $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, тогда однородное уравнение кривой (1) в проективных координатах имеет вид

$$\left(X^2 + aY^2\right)Z^2 = Z^4 + dX^2Y^2,$$

$$X = xZ, \quad Y = yZ.$$

Сумма двух точек теперь записывается как $\left(X_1 : Y_1 : Z_1\right) + \left(X_2 : Y_2 : Z_2\right) = \left(X_3 : Y_3 : Z_3\right)$. С учетом подстановок выразим координаты суммарной точки согласно (2):

$$x_3 = \frac{X_3}{Z_3} = \frac{Z_1Z_2\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right)\left(X_1X_2 - aY_1Y_2\right)}{\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right)\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)}$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{Z_1Z_2\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)\left(X_1Y_2 + X_2Y_1\right)}{\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right)\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)}$$

Обозначим:

$$A = Z_1Z_2; B = A^2; \; C = X_1X_2; D = aY_1Y_2;$$

$$E = dCD; F = B - E; G = B + E.$$

Тогда:

$$X_3 = A \cdot G \cdot \left(D - C\right),$$

$$Y_3 = A \cdot F\left(\left(X_1 + Y_1\right) \cdot \left(X_2 + Y_2\right) - C - D\right),$$

$$Z_3 = F \cdot G.$$

Подсчет числа элементарных операций здесь дает 10 умножений M, одно возведение в квадрат S и 2 умножения *U* на параметры *a* и d кривой. Итак, находим сложность вычисления суммы различных точек, выраженную через число умножений и возведений в квадрат в поле $V_E = 10M + 1S + 2U$ [2].

1.2.Удвоение точек

Используя уравнение кривой (1), закон удвоения (3) запишем в форме, не зависящей от параметра d

$$2\left(x_1, y_1\right) = \left(\frac{x_1^2 - y_1^2}{2 - x_1^2 - y_1^2}, \frac{2x_1y_1}{x_1^2 + y_1^2}, \right).$$

Тогда координаты точки удвоения согласно (3):

$$x_3 = \frac{X_3}{Z_3} = \frac{\left(\left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)}{\left(2 - \left(\frac{X_1}{Z_1}\right)^2 - \left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)} =$$

$$= \frac{\left(X_1^2 - Y_1^2\right)\left(X_1^2 + Y_1^2\right)}{\left(2Z_1^2 - X_1^2 - Y_1^2\right)\left(X_1^2 + Y_1^2\right)},$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{2\frac{X_1}{Z_1}\frac{Y_1}{Z_1}\left(2 - \left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)}{\left(2 - \left(\frac{X_1}{Z_1}\right)^2 - a\left(\frac{Y_1}{Z_1}\right)^2\right)\left(\left(\frac{X_1}{Z_1}\right)^2 + a\left(\frac{Y_1}{Z_1}\right)^2\right)} =$$

$$= \frac{2X_1Y_1\left(X_1^2 + Y_1^2\right)}{\left(2Z_1^2 - X_1^2 - aY_1^2\right)\left(X_1^2 + aY_1^2\right)}$$

Обозначим

$$A = X_1^2, B = aY_1^2, C = Z_1^2, D = \left(A + B\right),$$

$$E = \left(A - B\right), F = 2C - A - B,$$

$$G = \left(X_1 + Y_1\right)^2, \quad H = G - D.$$

Тогда:

$$X_3 = DE,$$

$$Y_3 = 2XYF,$$

$$Z_3 = DF.$$

Подсчет числа возведений в квадрат и умножений в поле дает суммарную сложность удвоения $T_E = 3M + 4S + 1U\left[2\right]$.

Значения сложности групповых операций в проективных координатах для полных кривых Эдвардса [1] и скрученных кривых Эдвардса приведены в таблице 1.

Таблица 1

Класс кривых	Сложность групповой операции	
	Сложение точек	Удвоение точек
Полные кривые Эдвардса	$10\mathrm{M} + 1S + 1U$	$3M + 4S$
Скрученные кривые Эдвардса	$10\mathrm{M} + 1S + 2U$	$3M + 4S + 1U$

Наименьших вычислительных затрат, как следует из таблицы, требуют операции на полных кривых Эдвардса. Особенно они выигрывают при удвоении, которое обходится без операции умножения $1U$. По сравнению с кривыми в форме Вейерштрасса полные

кривые Эдвардса дают выигрыш в скорости экспоненцирования точки в 1.5 – 1.6 раза [7].

2. МЕТОД ДОСТИЖЕНИЯ МИНИМАЛЬНОЙ СЛОЖНОСТИ ГРУППОВЫХ ОПЕРАЦИЙ НА СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА

Как следует из таблицы 1, ввод дополнительного параметра *a* в уравнение скрученной кривой (1) увеличивает вычислительные затраты сложения точек на одну операцию $1U$ и удвоения точек на $1U$ в сравнении с полной кривой Эдвардса. В этом подразделе мы предлагаем простой способ, как можно избавиться от этих дополнительных затрат и достичь максимальной производительности экспоненцирования точки на скрученной кривой Эдвардса.

В работе $[6]$ показано, что квадратичное кручение скрученной кривой Эдвардса дает квадратичную кривую Эдвардса и обратно: $E^t_{a,d}\ E_{ca,cd}$ (здесь $\left(\frac{c}{p}\right)=-1,\left(\frac{ad}{p}\right)=1$). Кроме того, внутри классов скрученных и квадратичных кривых Эдвардса имеет место изоморфизм кривых $E_{a,d}E_{d,a}$.

Свойства изоморфизма и квадратичного кручения можно обосновать также, используя *j*-инвариант кривой в обобщенной форме Эдвардса [2,3]

$$j(a,d)=\frac{16\left(a^2+d^2+14ad\right)^3}{ad\left(a-d\right)^4},$$

$$ad\left(a-d\right)\neq 0. \qquad (4)$$

Как известно [3,8], изоморфные кривые (с порядком $N_E=p+1-t$) и кривые квадратичного кручения (с порядком $N^t_E=p+1+t$) имеют один и тот же *j*-инвариант. Из (4) сразу следуют свойства симметрии *j*-инварианта относительно переменных ca,cd и их инверсий:

$$j(a,d)=j(d,a), \qquad (5)$$

$$j(a,d)=j(ca,cd), \qquad (6)$$

$$j(a,d)=j\left(a^{-1},,d^{-1}\right), \qquad (7)$$

$$j(a,d)=j(1,d/a)=j(1,a/d). \qquad (8)$$

Внутри класса скрученных кривых Эдвардса нет пар квадратичного кручения, но для каждой кривой имеется изоморфная кривая со свойством (5) или $E_{a,d}E_{d,a}$, причем $\left(\frac{a}{p}\right)=-1,\left(\frac{d}{p}\right)=-1.$

Идея состоит в том, что при поиске подходящей для криптографии скрученной кривой Эдвардса нет смысла в переборе различных значений параметров a и d. Можно зафиксировать один из этих параметров (например, параметр a) и варьировать другим в области его допустимых значений. Если задать этот фиксированный параметр на минимальном числовом уровне $a=$, таком что $\left(\frac{a}{p}\right)=-1,$ то можно сэкономить полевую операцию $1U$ (умножение на параметр кривой) при сложении точек, а также и удвоении точки кривой. Например, если $=2,$ тогда одно сложение (тождественное умножению на 2) можно считать «бесплатной» операцией. При этом достигается минимальная сложность групповой операции, равная сложности операции для полной кривой Эдвардса. Это же справедливо для всех малых.

Нам требуется доказать, что при фиксации параметра $a=,$ перебор всех допустимых параметров d дает все возможные значения *j*-инварианта и, соответственно, порядков скрученной кривой.

Утверждение 1. *При фиксированном значении параметра* $a=$ *кривой* (1) ее *j-инвариант* $j(,d)$ *принимает* $(p-1)/4$ *возможных значений при* $p=1mod4$ *и* $(p-3)/4$ *возможных значений при* $p=3mod4$ *при всех* $\left(\frac{d}{p}\right)=-1,d\neq .$

Доказательство. Рассмотрим квадратичные кривые Эдвардса с параметрами $\left(\frac{a}{p}\right)=1,\left(\frac{d}{p}\right)=1.$ Для любой такой кривой существует изоморфизм $E_{a,d}\ E_{1,d/a}\ E_{1,a/d}.$ Обозначим $=\frac{d}{a}.$ Из всех $\frac{(p-1)}{2}$ квадратов мультипликативной группы параметр $\neq 1$ принимает ровно $\frac{(p-3)}{2}$ допустимых значений. При $p=1mod4$ для каждого, кроме квадрата $=-1,$ существует пара изоморфных кривых $E_{1,}$. Случай $=-1=^{-1}$ вырождает пару изоморфных кривых в одну кривую. Тогда *j*-инвариант (8) кривой $E_{1,}$ принимает ровно $\frac{(p-1)}{4}$ значений. При $p=3mod4$ имеется ровно $\frac{(p-1)}{2}$ квадратов и $\frac{(p-3)}{2}$ допустимых значений. В этом случае элемент (-1) является квадратичным невычетом и су-

ществует ровно $\frac{(p-3)}{4}$ пар изоморфных кривых и такое же число *j*-инвариантов.

Парой кручения каждой квадратичной кривой Эдвардса является скрученная кривая в форме (1) при

$$\left(\frac{a}{p}\right)=\left(\frac{d}{p}\right)=-1, \text{ т.е. } E^{t}_{a,d}E_{ca,cd},\ \left(\frac{c}{p}\right)=-1.$$

Следовательно, число изоморфных пар скрученных кривых, равное числу *j*-инвариантов с теми же значениями, что и для квадратичных кривых Эдвардса, также равно $\frac{(p-1)}{4}$ при $p=1mod4$ и $\frac{(p-3)}{4}$ при $p=3mod4.$ Осталось доказать, что все изоморфные пары скрученных кривых Эдвардса могут быть получены при одном фиксированном значении параметра $a=$.

Воспользуемся свойствами (5), (6), и умножим параметры второго *j*-инварианта на $c=\frac{a}{d}$,

$$j(a,d)=j(d,a)=j\left(a,\frac{a^2}{d}\right). \qquad (9)$$

Отсюда следует, что любая пара изоморфных скрученных кривых Эдвардса определяется единственным параметром $a=$ и множеством всех пар квадратичных невычетов d и $d^{-1},d\neq$. Объемы множеств таких пар, как и число изоморфизмов скрученных кривых Эдвардса, остается таким же, как и для квадратичных кривых Эдвардса. Утверждение доказано.

Как ранее отмечалось, все скрученные кривые Эдвардса имеют порядок 4*n* при $p=1mod4$, поэтому нам интересен для криптографии лишь этот случай. Минимальное числовое значение квадратичного невычета $=2$ существует лишь при $p=\pm3mod8$ [8]. Следующее желаемое значение квадратичного невычета $=3$ требует выполнения $p=\pm5mod12$ [9]. В таблице 2 приведены для примера простые числа $p=1mod4$, для которых $=2$ и $=3$ (соответствующие столбцы помечены знаком +).

Таблица 2

p	3	7	29	7	1	3	1	3	9	7
α=2	+		+	+		+	+			
α=3		+			+				+	

Хотя эта выборка из первой сотни простых чисел с заданными свойствами не репрезентативна, можно сделать предположение, что около 80% простых чисел $p=1mod4$ являются модулями полей, содержащих квадратичные невычеты 2 или 3. В других случаях всегда можно найти минимальное значение параметра $a=$, что позволяет пренебречь сложностью операции $1U$ в оценках сложности групповых операций сложения и удвоения точек.

Пример 1. Пусть $p=29$ и $a==2$. Согласно формулы (4) можно сначала найти *j*-инвариант единственной квадратичной кривой Эдвардса $j(1,-1)=17$ и соответствующей скрученной кривой Эдвардса $j(2,-2)=17$. Далее в соответствии с утверждением 1 и формул (9) находим 6 *j*-инвариантов для изоморфных пар скрученных кривых Эдвардса

$$j(2,3)=j(2,11)=18,\ j(2,8)=j(2,15)=12,$$
$$j(2,10)=j(2,12)=16,$$
$$j(2,14)=j(2,21)=18,\ j(2,18)=j(2,26)=23,$$
$$j(2,19)=j(2,17)=18.$$

Все скрученные кривые Эдвардса с одинаковым *j*-инвариантом имеют одинаковый порядок. Но число допустимых порядков в нашем примере почти вдвое меньше числа различных вычисленных *j*-инвариантов. Действительно, все скрученные кривые при $p=1mod4$ имеют минимальный кофактор 4 порядка кривой. В границах Хассе [$p\pm2\sqrt{p}$] имеются лишь 3 значения таких порядков $N_E\in\{20,\ 28,\ 36\}$. В данном примере получены такие результаты:

$$N_E=20 \quad \text{при} \quad j(2,-2)=17,$$
$$N_E=28 \quad \text{при} \quad j(2,d)\in\{16,18\},$$
$$N_E=36 \quad \text{при} \quad j(2,d)\in\{12,23\}.$$

Подчеркнем, что кривые с одинаковым *j*-инвариантом не обязательно изоморфны, но всегда имеют одинаковый порядок. В то же время одинаковый порядок могут иметь кривые с разными значениями *j*-инвариантов и, разумеется, неизоморфные кривые.

Итак, задавая в скрученной кривой Эдвардса минимальное не квадратичное значение параметра $a=$, можно достичь максимальной производительности вычисления групповых операций и экспоненцирования точек, равной производительности вычислений на полной кривой Эдвардса с параметром $a=1$.

3. РЕЗУЛЬТАТЫ ВЫЧИСЛЕНИЙ ОБЩЕСИСТЕМНЫХ ПАРАМЕТРОВ КРИПТОСТОЙКИХ СКРУЧЕННЫХ КРИВЫХ ЭДВАРДСА С МИНИМАЛЬНОЙ СЛОЖНОСТЬЮ

В данном разделе мы рассматриваем простые поля с модулями длиной 192, 224, 256, 384 и 521 бит, которые рекомендуются стандартом FIPS–186–4-2013, и приводим перечень параметров скрученных кривых Эдвардса почти простого порядка $N_E = 4n$ (n – простое) над каждым из полей. Результаты расчетов общесистемных параметров кривых в шестнадцатеричной системе чисел сведены в таблицы 3 – 7. Здесь модули длины L обозначены как p_L. Модули полей $p1 mod 4$ выбирались как простые числа с малым двоичным весом Хэмминга 3..5. Для каждой кривой приведены значения p, порядки $n = N_E / 4$ генератора G криптосистемы и его координаты (x_G, y_G), а также значения параметров $a\,u\,d$.

Надо заметить, что параметр $a = 2$ является квадратичным невычетом лишь при $p = \pm 3 mod 8$. Это значит, что двоичное представление числа p заканчивается тремя младшими разрядами $101 = 5_{10}$ или $011 = 3_{10}$, а все более старшие разряды дают $0 mod 8$. В нашем алгоритме случайного поиска простых чисел с малым весом лишь одно значение $p = 2^{255} + 2^{38} + 2^2 + 1$ в таблице 5 отвечает этому условию (здесь $a = 2$), поэтому практически все кривые имеют минимальный параметр $a = 3$.

Проверка чисел p и n на простоту производилась с помощью тестов Миллера-Рабина и Лукаса-Лемера, реализованных в языках программирования C#, Java и в системе Wolfram Mathematica.

Вычисление символов Лежандра для нахождения подходящих параметров a и d производилось с помощью библиотечных функций языка Java и системы Wolfram Mathematica.

Порядки эллиптических кривых рассчитывались по алгоритму SEA (Schoof- Elkies -Atkin), реализованном в библиотеке PARI/GP.

Точки-генераторы были найдены удвоением случайной точки, удовлетворяющей уравнению (1), с использованием системы Wolfram Mathematica и языка Java. Удвоения достаточно, так как на нециклической скрученной кривой порядка $4n$ максимальный порядок точки равен $2n$.

В каждой из приведенных ниже таблиц содержатся параметры 5 скрученных кривых Эдвардса с минимальным значением параметра $a = 2,3$ или 5. Далее параметр d подбирался как наименьшее из значений, при котором порядок кривой $4n$ становился почти простым. Порядок кривых по длине сравним с длиной поля.

Таблица 3

Скрученные кривые Эдвардса почти простого порядка над полем с модулем p_{192}

p = $2^{191} + 2^{16} + 2^{12} + 1$ p = 8000000000000000000000000000000000000000000011001 n = 2000000000000000000000004447D62B952200D604D2BEB9 a = 3 d = DD xG = 79FD21DC7BF961D56CDD092798C3016F11C2034F154A94B5 yG = 17B25C0DADFD379FF3D7CD1EAEFD83328B945410BE11D5DB
p = $2^{191} + 2^{45} + 2^{41} + 1$ p = 8000000000000000000000000000000000220000000001 n = 1FFFFFFFFFFFFFFFFFFFFFEAA490B04DCC3760DB69D80B a = 5 d = B7 xG = 41D4C37EE995324B600442F0DCE31A0EA61C08C92D80110B yG = 3EC06FDFB33AFA858E30D898F9C18606CA62E79F6175FD80
p = $2^{191} + 2^{46} + 2^{36} + 1$ p= 8000000000000000000000000000000000401000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFC219C1BBD9EF98692F7D3077 a = 3 d = 4D xG = 50707DB9B16BF11C894E2A2F25A2887A6AB3A5921E9AACDE yG = 1BEF37EF93DBA0D7203F96BD14FCDA0E6B1CF118866982B2

$p = 2^{191} + 2^{49} + 2^{27} + 1$ p = 800000000000000000000000000000000200000800000001 n = 1FFFFFFFFFFFFFFFFFFFFFFD4622687DA3DDCBF47806983 a = D d = AC xG = 3BFDC9D07301A8A3A9BEC18540B0EEDC0F7C3CD21F652EFE yG = 3C48E70B7F04C446A8CC208696DA2592A56FB29C79888D52
$p = 2^{191} + 2^{158} + 1$ p = 800000004000000000000000000000000000000000000001 n = 200000001000000000000004DE2B37DC449E40E33C414B9 a = 5 d = 800000003FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC0F xG = 209295DA12CEDAE57617AF4911C57DDCE7043EB18687E13C yG = 3847775699DF8A7F431D8DA8FE993A28A6D4F108B6502917

Таблица 4

Скрученные кривые Эдвардса почти простого порядка над полем с модулем p_{224}

$p= 2^{223} + 2^{24} + 2^{20} + 1$ p = 800000000000000000000000000000000000000000000000000001100001 n = 200000000000000000000000003F330C2860F36EC9E831F641A2B9 a = 3 d = 93 xG = 6C7CC9C10F4259CBEB0D1973AF0E4FC64AE442A301A90DFEEB5BC081 yG = 2D4F15BA1A686CAEDB9D43F9525BF78683DAA39B82301FCA8A7874BE
$p = 2^{223} + 2^{38} + 2^{36} + 1$ p = 800000000000000000000000000000000000000000000005000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFFBCE784913191A6362578E1CD28C9 a = 3 d = 215 xG = 60536D73F2A4EF1F54C1048734301E01306FF7F331719201335D5A55 yG = DDBFD9D1AFD09CD322F639F524CC60F9A7A727139F56BBF8D127940
$p = 2^{223} + 2^{61} + 2^{41} + 1$ p = 800000000000000000000000000000000000000000020000020000000001 n = 200000000000000000000000002165B89B7402F30BF010CB396EA9 a = 5 d = 3D xG = 59507C9FEF622459507C9FEF622459507C9FEF623AAD7109DDBA6AF7 yG = 1366A5B9781878270245AAA111E53CDC079B0322CB4A8C805309452A
$p = 2^{223} + 2^{72} + 2^{20} + 1$ p = 800000000000000000000000000000000000000100000000000100001 n = 1FFFFFFFFFFFFFFFFFFFFFFFFE0DAC7710567C631D4CA120783E9 a = 3 d = 15C xG = 5C611714E8FD05D966F07BD978DF524642C21CF3BDBB6BA1FE037DD8 yG = 3499A41BF2C767BD41A045CDB7285F9E4907598421C0B78D29D5A7E0
$p = 2^{223} + 2^{66} + 2^{14} + 1$

p = 8000000000000000000000000000000000000000400000000000004001
n = 20000000000000000000000000014E4DE701954CB43404E060EAC01
a = 3
d = 26
xG = 2A795ABA13A5D9DC2BEB32468049F7E8E287393711EA0A66DCBFF040
yG = 532C172BF052220CDE0B63A2F421DB65E8A676B96D7FA0307DDC0E53

Таблица 5

Скрученные кривые Эдвардса почти простого порядка над полем с модулем p_{256}

p = $2^{255} + 2^{46} + 2^{42} + 1$
p = 8000000000000000000000000000000000000000000000000000440000000001
n = 20000000000000000000000000330A60EA43DF5957AC18C44AB8122EB7
a = 3
d = 1AF
xG = 25091FBF427205B62204FD7FE48236752C1FE497EF2DB3197938BA36D9A27554
yG = 52A7749533218F16BB1F32137CE731DC0F26149CE2E1CF1378B74E066B952532

p = $2^{255} + 2^{41} + 1$
p = 8000000000000000000000000000000000000000000000000000020000000001
n = 20000000000000000000000002498CDC14EB2676199F9EFB8C86EA9D1
a = 3
d = BC
xG = 1306A0056F9B6F44758D8146286E140B8D2A4C7179CCB2B515E9EAE4A679F81
yG = 33CD1A3853C6059B39DE2485F320CC00D97E1BB77D5C79025BF01D1F3C0D8868

p = $2^{255} + 2^{66} + 2^{60} + 1$
p = 8000000000000000000000000000000000000000000000000004100000000000001
n = 20000000000000000000000000002BC056BB954BD3CF60CD27D370FF3265
a = 3
d = 6C
xG = 7E5D3187BA7FF18EF3066E57C722DCE95279A01945D6B4C2E918B56C32FF35D1
yG = 3AC8B7A5A64DA05FF1F28870506E451F103DA6EE32FAB89D3D903E073660572E

p = $2^{255} + 2^{38} + 2^{2} + 1$
p = 8000000000000000000000000000000000000000000000000000000004000000005
n = 20000000000000000000000000031F23720CCCC83EF9F44858B6E952E4F
a = 2
d = 1CC
xG = 25091FBF427205B62204FD7FE48236752C1FE497EF2DB3197938BA36D9A27554
yG = 52A7749533218F16BB1F32137CE731DC0F26149CE2E1CF1378B74E066B95253

p = $2^{255} + 2^{70} + 2^{66} + 1$
p = 8000000000000000000000000000000000000000000000000044000000000000001
n = 20000000000000000000000002B81184994F3F0880BB2B78314AFD2E9
a = 3
d = 13A
xG = 1C32148FB9F80F78D2E84879553296DA0858C29EFEAD3EDCCBFC55E8FEE15C85
yG = 2D4ED6C59052B9113E76AEDACBC668F3BB0EE5819C5B5221A311118DECAAE65E

Таблица 6

Скрученные кривые Эдвардса почти простого порядка над полем с модулем p_{384}

p = $2^{383} + 2^{155} + 1$
p = 8000000000000000000000000000000000000000000000000000000000000000000000000000000800000000000000000000000000000000000000001
n = 1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE935B9B743CFBDC890CDB6FC507DB7744384DF7B5FAF81D1
a = 3

d = EC
xG =
5B83FE601E531F45B83FE601E531F45B83FE601E531F45B83FE601E537AC9B6A004550477AC9B6A004550477AC9B69FF
yG =
5FF608B37764C7FE1719D75DA24646D8869E60637F0C477A548C46BDECB0270BF2C840E083654F63367D737325053472

n =
1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD2E846F4DD24CB4DC3014E1B9B39C56950B3F5FF1870523
a = 3
d = 10A
xG =
2301C9793214FC6152B4CEED1379498ACA6F87089186C2301C97932151F631C2E01020FDA9C3F995C9A81DB118C9FA39
yG =
79AFEE927FA08107917851B6F7DD952DC852C052D6A2DDE0E0E1AF9EA781CDC8AF1ED4E9B024BFA5FAB992443F80C745

$p = 2^{383} + 2^{233} + 1$
p=
800000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000000001
n =
20000000000000000000000000000000000007FFFFFFFFFCEA783C2F07E63118A47FDB07FBAD3E742437E35EA11EA81
a = 3
d = 15A
xG =
45FB6177745030C78D712C115E5354E6F6AB496E668C3DB6A55EB1EF2F9418052C6FF89BF253B3813F48B5134EFD5220
yG =
35525C097B1F9D1DB5ABB1695B62EF88E79DDCE007ACD8F167E7022A2EC379AF0A7C184F8C09934F230A30522FA27EE3

n =
20000000000000000000000000000000000007FFFFFFFFFC4E3F96E2B485B72DB4DC623D7ECECFE59A562991D60A279
a = 3
d = 7B0
xG =
5EE2C5033D54291ACD632030F57D0AD23E537766CAEF2EC8E7117FA4D247D71E488F0FAA45B5A1E8FEA7E6617BFA140E
yG =
39949C9783884C7491E5D3F0D33704A278A6D4DF52C56C9B83FDC59BCF9282A42BFB06B377CF4E00933842AD9B65511

n =
20000000000000000000000000000000000007FFFFFFFFFFFB43327D7C94B4BEA93CCCFCA103CF64D6A40B8F00E9016B
a = 3
d = 33B
xG =
56499011F2275F6A3E9421923C69AA0F8C47A25BD16EF68635243D6B1867A732DC11CA8C8CEFF30132EFDF33C9B2B969
yG
=46D521F9D3A98FF01C4D5676A6CBB88A78AB84F2502A0A30E9A51A64A26D60FD47F8B02E0B5F1713783CFC878DAF6108

Таблица 7

Скрученные кривые Эдвардса почти простого порядка над полем с модулем p_{521}

$p = 2^{520} + 2^{66} + 2^{65} + 1$
p =
1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000006000
0000000000001
n =
40000000000000000000000000000000000000000000000000000000000001E5EE0522024E5E359E578FDD4AAE5B3388CCE2795EC03189792778B80EDB1251
a = 3
d = 2A8
xG =
BA5B99F7375F86F6D700E0DCD8E750E64FE9EA4F44B5C4CF022B45EDD2B81962129B6AED970FCAF0754EA418054E5AAB55FD9911C
3BBAA99DB75F86F6D700E0DCD
yG =
91E0646D69810E9FC606F87EA7BFA7140B1446EEA937536CDDC166C301BB0ECE279DA15838913154E7BEDE69C7AC43D2756A279005
625F52F9D145A41E77E31D4B

$p = 2^{520} + 2^{80} + 2^{39} + 1$
p =
1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010000000000800000001
n =
3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD4F3EBC07
4E5DCC909AAE45C02D90E60764C007
6526D0C9B9F66517F45515A05
a = 3
d = 87
xG =
6287A808BC52FD146441B870582B459B15414
9EC3E444F88F3950A07DF4AC946781D7517D8628
7A808BC52FD146441B870582B459B154
1AC73E64D0C0D347D72A7
yG =
6A20EC64258785F16B2A400BF0C6D2E90C80
80AE25A96F465029EE2A148A0EF2BF0DF9E087F1
E02487738C927BAF4B0C50A9349BA68
FAF1D3B24BB6E0D8E991B1

$p = 2^{520} + 2^{110} + 2^4 + 1$
p =
10000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000400000000000000
0000000000011
n =
3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFBE822ED9EC
C69628BD3C3257DB51B5FC7477094B
E7A8266F720BFB22D9AA02123
a = 5
d = D2
xG =
DE935EF49AF7A4D7BD26BDE935EF49AF7A4
D7BD26BDE935EF49AF7A4D7BD26BDE935EF49A
F7A4D7BD26BDE935EF49AF7A4D7B
D5E62C0F3160798B03CC581E62C1C
yG =
7CD02BB98782E14860C91A53E907B7C4FDA
A1C6898375790CB3FDED238FD9A069B8C53B67A
C5DC0C8B782D74624A69D91450D20C
C9DCA8B76DB97994008CB492F1

$p = 2^{520} + 2^{348} + 2^{278} + 1$
p =
10000000000000000000000000000000000000000
00010000000000000000400000000000000000000
00000000000000000000000000000000000
0000000000001
n =
40000000000000000000000000000000000000000
00040000000000000000FFFFDCB98F10F9CF70F01
865640CBDD9D354DDFB78BBD8EE3F20DD416BE
23E0E1D08D
a = 5
d = 53
xG =
D8F7F6D0EEC7BFB687763DFDB43BB1EFED
A1DD8F7F7A9E6BE90A54F35F4888E598AE7E472
CC573F239662B9F91CB315CFC8E598AE7E472CC5
73F239662B9F91CB2
yG =
FDB9481BBAFC22AD99D0C546F5B6C680901
3308A794235AEE551A74142CBE4695FD23708A6C
27631A6AF3DF61BB4F83C481614132F713D0B860
EAB37B7F74748D2

$p = 2^{520} + 2^{73} + 1$
p =
10000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000000000200000
0000000000001
n =
3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFD34B63B11FF
960C064B6AEA3B6851C23CCDC50B6
E6921941026DF9E4883D1C157
a = 7
d =
10000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000001FFFF
FFFFFFFFE786B
xG =
4CFD4C477A7FABB556313753CD284B6B2315
E866A9C3A38F399E19FCEC6BA0796367AFBD7B6
AAE33967252EA110AF880CB1038A2E
699072C8FACACCF0F919B3C67
yG =
74E83FF02F90FB98F028FC1D0BD94A0093E94
E6250BA9DDEE68F1DE65242E496D90B9CEAE817
717DFB7EC4E9E2D7A0004FDBB99B2
79AA75BF2E785DB9A5D415EBA

ЗАКЛЮЧЕНИЕ

В заключение отметим, что предлагаемые для стандартизации и имплементации скрученные кривые Эдвардса имеют рекордную скорость экспоненцирования точки. Большинство из рассчитанных кривых наряду с минимальным значением параметра $a = 3$ имеют всего двух- или трехразрядное шестнадцатеричное значение второго параметра d, что практически позволяет пренебречь сложностью операций $1U$ и $2U$ для скрученных кривых в таблице 1. Оценки сложности сложения точек $V_E = 10M + 1S + 2U$ и удвоения точки $T_E = 3M + 4S + 1U$ достигают в нашем случае нижних границ $V_E = 10M + 1S = \frac{32}{3}M$, $T_E = 3M + 4S = \frac{17}{3}M$, если принять $S = \frac{2}{3}M$ [1]. Кроме того, в отличие от предыдущей работы [4] с параметрами полной кривой

Эдвардса, здесь найдены кривые для модулей поля p_{521} с наивысшим стандартным уровнем стойкости.

Литература

[1] *Bernstein D.J., Lange T.* Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology – ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29 – 50.

[2] Bernstein Daniel J.,Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008. P. 1 – 17.

[3] *Morain F.* Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009.

[4] *Бессалов А.В., Дихтенко А.А.* Криптостойкие кривые Эдвардса над простыми полями**.** Прикладная радиоэлектроника, 2013, Том 12, №2. – С. 285-291.

[5] *Бессалов А.В., Цыганкова О.В.* Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Проблемы передачи информации. – Том 51, вып 4, 2015. – С.92 – 98.

[6] *Бессалов А.В., Цыганкова О.В.* Классификация кривых в форме Эдвардса над простым полем . Прикладная радиоэлектроника: научно-техн. журнал. – 2015. – Том 14. – №4. – С.197 – 203.

[7] *Бессалов А.В., Цыганкова О.В.* Производительность групповых операций на скрученной кривой Эдвардса над простым полем. Радиотехника, №181, 2015. – С.58 – 63.

[8] *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

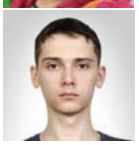
[9] *Дэвенпорт Г.* Высшая арифметика: введение в теорию чисел // Пер. с англ. под редакцией Ю.В.Линника. – М: «Наука», 1965. – 176с.

Бессалов Анатолий Владимирович, д-р. техн. наук, профессор, профессор физико-технического института НТУУ «КПИ им. Игоря Сикорского».

Олешко Константин Андреевич, магистрант физико-технического института НТУУ «КПИ им. Игоря Сикорского».

Поречная Дарья Никитична, магистрант физико-технического института НТУУ «КПИ им. Игоря Сикорского».

Цыганкова Оксана Валентиновна, аспирант физико-технического института НТУУ «КПИ им. Игоря Сикорского».



Черный Олег Николаевич, магистрант физико-технического института НТУУ «КПИ им. Игоря Сикорского».

УДК 681.3.06

Криптостійкі скручені криві Едвардса з мінімальною складністю групових операцій / А.В. Бессалов, К.А. Олешко, Д.Н. Поречна, О.В. Циганкова, О.М. Чорний // Прикладна радіоелектроніка: наук.-техн. журнал. – 2016. – Том 15, № 3. – С. 141 – 150.

Дано аналіз оцінок складності групових операцій для скручених кривих Едвардса. Запропоновано метод мінімізації обчислень за допомогою вибору мінімального значення параметра a кривої. Наведено таблиці загальносистемних параметрів 25 криптостійких рекордно швидких кривих зі значеннями модулів поля довжиною 192, 224, 256, 384 і 521 біт.

Ключові слова: скручені криві Едвардса, повні криві Едвардса, порядок кривої, порядок точки, квадратичний лишок, квадратичний нелишок, складність операцій.

Табл.: 07. Бібліогр.: 09 найм.

UDC 681.3.06

Secure twisted Edwards curves with minimal complexity of group operations / A.V Bessalov, K.A. Oleshko, D.M. Porechna, O.V. Tsygankova, O.M. Chornyi // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. – P. 141 – 150.

An analysis of evaluations of group operations complexity for twisted Edwards curves is given. A method of minimizing calculations by selecting the minimum value of the curve parameter (a) is suggested. Tables of system-wide settings of 25 record fast cryptographically secure curves in finite fields with modules of lengths 192, 224, 256, 384, and 521 bits are provided.

Keywords: twisted Edwards curves, complete Edwards curves, order of a curve, order of a point, quadratic residue, nonquadratic residue, complexity of operations.

Tab.: 07. Ref.: 09 items.