УДК 681.3.06

Бессалов А.В., Дихтенко А.А., Цыганкова О.В.

Мощность множества эллиптических кривых, изоморфных кривым Эдвардса над простым полем

Предложен алгоритм построения канонической эллиптической кривой с двумя точками четвертого порядка, изоморфной кривой Эдвардса над простым полем. Найдена средняя оценка числа таких кривых с ненулевыми значениями параметров a и b кривой. Доказано, что для больших полей доля таких кривых близка к 1/4.

Ключевые слова: каноническая эллиптическая кривая, кривая Эдвардса, кривая кручения, параметры кривой, изоморфизм, квадратичный вычет, квадратичный невычет.

Запропонований алгоритм побудови канонічної еліптичної кривої з двома точками четвертого порядку, що ізоморфна кривій Едвардса над простим полем. Знайдена середня оцінка числа таких кривих з ненульовими значеннями параметрів a та b кривої. Доведено, що для великих полів частка таких криивих близька до1/4.

Ключові слова: канонічна еліптична крива, крива Едвардса, крива кручіння, параметри кривої, ізоморфізм, квадратичний лишок, квадратичний нелишок.

An algorithm is proposed to obtain a canonical elliptic curve with two points of order four which is isomorphic to an Edwards curve over the prime field. Average estimation is calculated for a number of such curves with non-zero values of the curve parameters a and b. It is proved that for large-characteristic fields a rate of such curves is close to1/4.

Key words: canonical elliptic curve, Edwards curve, curve twist, curve parameters, isomorphism, quadratic residue, quadratic non-residue

Введение. Привлекающие в последние годы внимание криптографов кривые Эдвардса [1-5] обладают двойной симметрией в координатах поля характеристики $p>2$ и, как следствие, четырехкратной избыточностью по числу точек N_E. Так как $N_E \equiv 0 \bmod 4$, циклические кривые Эдвардса всегда содержат ровно 2 точки 4-го порядка и одну точку 2-го порядка. Канонических кривых с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса возникает задача поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. В настоящей работе предложен оригинальный подход, основанный на замене традиционных параметров (a,b) канонической кривой парой параметров (a,c), где c – единственный в поле F_p корень кубического уравнения. Кривая с требуемыми свойствами отбирается при выполнении двух условий на квадратичные вычеты выражений, линейно связывающих параметры кривой.

1. Условия, порождающие 2 точки 4-го порядка канонической кривой

Каноническая кривая над полем характеристики $p \neq 2,3$ описывается известным уравнением [6]

$$E_p: \quad y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0,\ a,b \in F_p \tag{1}$$

Далее нам потребуется операция удвоения точки $P = (x_1, y_1)$, которая дает координаты точки $2P = (x_3, y_3)$, равные:

$$\begin{cases} x_3 = \nu^2 - 2x_1 \\ y_3 = -y_1 - \nu(x_3 - x_1) \end{cases} \qquad \nu = \frac{3x_1^{\,2} + a}{2y_1} \tag{2}$$

Пусть c – единственный в поле F_p корень кубического уравнения $x^3 + ax + b = 0$, тогда вместо (1) можно записать

$$y^2 = (x - c)(x^2 + cx + a + c^2), \qquad b = -c^3 - ac,\ c \in F_p \tag{3}$$

Парабола в правой части (3) не имеет корней в поле F_p, если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

$$c^2 - 4(a + c^2) = -(3c^2 + 4a) \neq A^2 \tag{4}$$

Это условие гарантирует существование единственной точки 2-го порядка кривой (2), определяемой как $D = (c, 0)$.

Пусть $P = (x_1, y_1)$ – точка 4-го порядка. Ее удвоение в соответствии с (2) дает координаты точки $D = (c, 0)$:

$$\begin{cases} x_3 = \left(\dfrac{3x_1^{\,2} + a}{2y_1}\right)^2 - 2x_1 = c \\ y_3 = -y_1 - \left(\dfrac{3x_1^{\,2} + a}{2y_1}\right)(c - x_1) = 0 \end{cases} \tag{5}$$

Из этой системы после сокращения сомножителя $(3x_1^{\,2} + a)$ получим квадратное уравнение для координаты x_1 точки 4-го порядка:

$$x_1^{\,2} - 2cx_1 - (2c^2 + a) = 0$$

Корни этого уравнения находятся из

$$x_1 = c \pm \sqrt{\delta} = c \pm \sqrt{3c^2 + a}, \qquad \delta = 3c^2 + a \tag{6}$$

Из двух решений в (6) выбирается значение x_1, лежащее на кривой E_p. Из (5) можно также получить формулу для вычисления координаты y_1 точки 4-го порядка:

$$y_1{}^2 = \delta\left(\pm 2\sqrt{\delta} + 3c\right) \tag{7}$$

Из (6) следует, что точка 4-го порядка существует, если дискриминант квадратного уравнения δ является квадратом в поле, т.е.

$$\delta = 3c^2 + a = B^2 \tag{8}$$

Условия существования точек 2-го и 4-го порядков (4) и (8) можно выразить через символы Лежандра как

$$\text{a)}\ \left(\frac{-\left(3c^2+4a\right)}{p}\right) = -1, \qquad \text{b)}\ \left(\frac{\delta}{p}\right) = \left(\frac{3c^2+a}{p}\right) = 1. \tag{9}$$

Пример. Требуется найти кривую с двумя точками 4-го порядка над полем F_7. Примем $c=1$ и вычислим аргументы функций (9) для всех ненулевых значений a (таблица 1). Так как $p \equiv 3 \bmod 4$, (-1) – квадратичный невычет в поле [6], поэтому $\left(3c^2+4a\right)$ должен быть вычетом, как и δ.

Таблица 1

a	1	2	3	4	5	6
$\left(3c^2+4a\right)$	0	4	1	5	**2**	6
$\delta = \left(3c^2+a\right)$	4	5	6	0	**1**	2

Из таблицы видим, что условия (9) для совместных вычетов совпадают лишь при одном значении $a=5$, при этом согласно (3) $b=-c^3-ac=1$. Тогда имеем кривую $y^2=x^3+5x+1$ порядка $N_E=12$ (след Фробениуса $t=-4$). Ее единственная точка второго порядка $D=(1,0)$, а координаты точки 4-го порядка в соответствии с (6), (7) равны: $x_1 = c \pm \sqrt{\delta} = 1 \pm 1, \quad \Rightarrow x_1 = 0,$

$$y_1{}^2 = \delta\left(\pm 2\sqrt{\delta} + 3c\right) = 1, \quad \Rightarrow y_1 = \pm 1.$$

Здесь решения, не лежащие на кривой, отбрасываются.

Для найденной кривой легко построить кривую кручения $y^2 = x^3 + 3x + 6$ порядка $N_E = 4$ и параметром $t = 4$ (см.[6]). Здесь корень кубика смещается $(c = 3)$, но свойства (9) выполняются и имеются лишь 2 точки 4-го порядка.

Вообще над полем F_7 существует 6 кривых с ненулевыми параметрами a и b и двумя точками 4-го порядка. Их параметры c, a и b вместе с порядками N_E кривых приведены в таблице 2. Здесь слева даны параметры трех изоморфных кривых порядка 12 с корнями $c = 1, 2, 4$, а справа – их кривые кручения порядка 4 с корнями $c = 3, 6, 5$ (они, разумеется, также изоморфны).

Таблица 2

Параметры кривой E_p				Параметры кривой кручения $E_p^{\,t}$			
c	a	b	N_E	c	a	b	N_E
1	5	1	12	3	3	6	4
2	6	1	12	6	5	6	4
4	3	1	12	5	6	6	4

Можно заметить, все $(p-1)$ ненулевых значений корня c могут дать, по крайней мере, $\frac{(p-1)}{2}$ значений параметра a, так как в (9) решение определяется квадратом c^2. Поэтому число решений можно вдвое сократить, переходя (при необходимости) к кривой кручения [6].

Возникает закономерный вопрос: какова доля кривых, для которых существует изоморфизм с кривыми Эдвардса при любых значениях порядка поля p?

2. Расчет числа канонических кривых, изоморфных кривым Эдвардса

Утверждение. Число канонических кривых (1) с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. $M_1 = \frac{(p-1)(p-5)}{4}$ при $p \equiv 3 \bmod 4$ и $M_2 = \frac{(p-1)^2}{4}$ при $p \equiv 1 \bmod 4$.

Доказательство.

1. Пусть $p \equiv 3 \bmod 4$, тогда (-1) – квадратичный невычет [6], т.е. $\left(\frac{-1}{p}\right) = -1$, и для (9а) невычет заменяем квадратичным вычетом

$$\left(\frac{-1}{p}\right)\left(\frac{(3c^2+4a)}{p}\right) = \left(\frac{-1}{p}\right) \qquad \Rightarrow \qquad \left(\frac{(3c^2+4a)}{p}\right) = 1$$

Аргументы символов Лежандра (9) являются линейными функциями параметров a и c^2, следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p с соответствующим решением:

$$\begin{cases} 3c^2+4a = A^2 \\ 3c^2+a = B^2 \end{cases} \Rightarrow \begin{cases} a = 3^{-1}(A^2-B^2) \\ c^2 = 9^{-1}(4B^2-A^2) \end{cases} \tag{10}$$

Для кривых с параметрами $a \neq 0$ и $b \neq 0$ квадратичные вычеты $A^2 \neq B^2$ и, кроме того, $4B^2 \neq A^2$(нулевые вычеты c^2 отбрасываются, так как из $c = 0 \Rightarrow b = 0$, и согласно (3) $b = -c^3 - ac$,). Из (9) следует, что $A^2 \neq 0$, но не исключается $B^2 = 0$. Однако из (10) при $B^2 = 0$ получим $c^2 = -(A/3)^2$, т.е. правая часть этого равенства есть квадратичный невычет и решения нет. Итак, следует учитывать лишь ненулевые квадратичные вычеты A^2 и B^2. Всего можно составить $(p-1)(p-3)/4$ пар различных ненулевых квадратичных вычетов. Из этого числа необходимо вычесть $(p-1)/2$ пар, для которых $4B^2 = A^2$, и получить $(p-1)(p-5)/4$ допустимых пар квадратичних вычетов и, соответственно, такое же число решений (10) для параметров a и c^2. В среднем при больших p половина решений объема $(p-1)(p-5)/8$ с невычетами для параметра c^2 отбраковываются, остальные дают по две кривых с корнями кубики $\pm c$. Таким образом, число кривых или число решений для параметров $(a, \pm c)$ или $(a, \pm b)$ в среднем оценивается величиной $M_1 = (p-1)(p-5)/4$.

2. Пусть теперь $p \equiv 1 \bmod 4$, тогда (-1)– квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$ [6]. Тогда для (9а) можно получить квадратичный вычет, умножив аргумент функции Лежандра на квадратичный невычет n и найти единственное решение системы

$$\begin{cases} (3c^2+4a)n = A^2 \\ 3c^2+a = B^2 \end{cases} \Rightarrow \begin{cases} a = (3n)^{-1}(A^2-nB^2) \\ c^2 = 9^{-1}(4nB^2-A^2) \end{cases} \tag{11}$$

Если принять $B^2 = 0$, в формуле для c^2 мы вновь получим невычет в правой части, поэтому и в данном случае учитываем лишь ненулевые квадраты

A^2 и B^2. Но здесь уже всегда $A^2 \neq nB^2$, так как n – невычет, поэтому параметр $a \neq 0$ для любых ненулевых пар A^2 и B^2. Очевидно, что число таких пар квадратичных вычетов равно $(p-1)^2/4$. Условие $c^2 \neq 0$ в (11) выполняется всегда, так как для всех ненулевых квадратов A^2 и B^2 имеем $n(2B)^2 \neq A^2$, и в левой части неравенства – квадратичный невычет. Аналогичные предыдущему случаю рассуждения приводят к оценке среднего числа отобранных пар $(a, \pm b)$, равной $M_2 = (p-1)^2/4$. Эта оценка определяет среднее число эллиптических кривых с двумя точками 4-го порядка. Доказательство завершено.

Замечание. За формулировку и доказательство утверждения берет на себя ответственность первый автор статьи.

Так как общее число всех кривых с ненулевыми параметрами a и b равно $(p-1)^2$, относительная доля кривых, изоморфных кривым Эдвардса, при достаточно больших p оценивается в среднем величиной $\frac{p-5}{4(p-1)}$ (при $p \equiv 3 \bmod 4$) или $\frac{1}{4}$ (при $p \equiv 1 \bmod 4$). Для больших полей асимптотически обе оценки дают четверть всех эллиптических кривых.

Формулы (10), (11) конструктивны, так как позволяют рассчитывать параметры a и $\pm c$ кривой (и, соответственно, $\pm b$) при заданных значениях пар квадратичных вычетов (A^2, B^2). На основе условий (9) и формул (10), (11) можно предложить следующий алгоритм построения канонических кривых с двумя точками 4-го порядка:

1. В поле F_p задаем произвольное значение пары квадратичных вычетов (A^2, B^2) и согласно (10) или (11) рассчитываем параметры a и c^2. Если вычисленное значение c^2 – невычет, меняем параметр B^2 и повторяем расчеты.
2. Если вычисленное c^2 – квадратичный вычет, находим 2 кривые с параметрами $(a, \pm c)$ и $(a, \pm b)$. Значение параметра b рассчитываем в соответствии с (3).
3. Находим координаты точки 4-го порядка (для построения изоморфной кривой Эдвардса).

4. Вычисляем порядок одной из кривых и, в случае неприемлемого порядка, рассчитываем порядок кривой кручения. Если решение не найдено, переходим к другой паре значений (A^2, B^2) (возвращаемся в п.1).

Разумеется, можно модифицировать данный алгоритм, фиксируя, например, параметр c^2, после чего требовать выполнения условий (9). Однако в предложенном виде алгоритм быстрее приводит к кривой с двумя точками 4-го порядка. Далее, как описано в [3], строится изоморфная кривая в форме Эдвардса.

Литература

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.
3. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.
4. Бессалов А.В., Гурьянов А.И., Дихтенко А.А. Кривые Эдвардса почти простого порядка над расширениями малых простых полей. Прикладная радиоэлектроника №2, 2012. С.225-227.
5. Бессалов А.В., Дихтенко А.А., Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника том 12 №2, 2013. С.107-113.
6. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.