СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06

А.В. БЕССАЛОВ, д-р техн. наук, А.А. ДИХТЕНКО, О.В. ЦЫГАНКОВА

АЛГОРИТМ ВЫБОРА КАНОНИЧЕСКОЙ КРИВОЙ, ИЗОМОРФНОЙ КРИВОЙ ЭВАРДСА НАД ПРОСТЫМ ПОЛЕМ

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 две точки четвертого порядка и одну точку второго 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 четвертого 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.

Условия, порождающие две точки четвертого порядка канонической кривой

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

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

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

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

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

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

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

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

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

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

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

Из этой системы после сокращения сомножителя $\left(3{x_1}^2 + a\right)$ получим квадратное уравнение для координаты x_1 точки четвертого порядка:

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

Корни этого уравнения находятся из

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

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 четвертого порядка:

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

Из (6) следует, что точка четвертого порядка существует, если величина δ – четверть дискриминанта квадратного уравнения, является квадратом в поле, т.е.

$$\delta = 3c^2 + a = B^2 \qquad (8)$$

Условия существования точек второго и четвертого порядков (4) и (8) можно выразить через символы Лежандра как

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

Пример. Требуется найти кривую с двумя точками четвертого порядка над полем F_7. Примем $c = 1$ и вычислим аргументы функций (9) для всех ненулевых значений a (табл. 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 четвертого порядка в соответствии с (6), (7):

$$x_1 = c \pm \sqrt{\delta} = 1 \pm 1, \qquad \Rightarrow x_1 = 0,$$
$${y_1}^2 = \delta\left(\pm 2\sqrt{\delta} + 3c\right) = 1, \qquad \Rightarrow y_1 = \pm 1.$$

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 две точки четвертого порядка.

Над полем F_7 существует шесть кривых с ненулевыми параметрами a и b и двумя точками четвертого порядка. Их параметры c, a и b вместе с порядками N_E кривых приведены в табл. 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 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*?

Оценка числа канонических кривых, изоморфных кривым Эдвардса

Утверждение. Средняя **о**ценка числа канонических кривых (1) с параметрами $a \neq 0$ и $b \neq 0$ над полем F_p с двумя точками четвертого порядка определяется как $M_1 = \frac{(p-1)(p-5)}{4}$ 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

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

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:

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

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 $c = 0 \Rightarrow b = 0$, так как 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 $c^2 = -\left(\frac{A}{3}\right)^2$, т.е. правая часть этого равенства есть квадратичный невычет и

решения нет. Итак, следует учитывать лишь ненулевые вычеты A^2 и B^2. Всего можно составить $\frac{(p-1)(p-3)}{4}$ пар различных ненулевых квадратичных вычетов. Из этого числа необходимо вычесть $\frac{(p-1)}{2}$ пар, для которых $4B^2 = A^2$ и получить $\frac{(p-1)(p-5)}{4}$ допустимых пар квадратичных вычетов и, соответственно, такое же число решений (10). В среднем при больших p половина решений объема $\frac{(p-1)(p-5)}{8}$ с невычетами для параметра c^2 отбраковываются, остальные дают по две кривые с корнями $\pm c$. Тогда число решений, для параметров $(a, \pm c)$ или $(a, \pm b)$ в среднем оценивается величиной $M_1 = \frac{(p-1)(p-5)}{4}$.

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

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

Если принять $B^2 = 0$ в формуле для c^2, вновь получим невычет в правой часть, 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 $\frac{(p-1)^2}{4}$. Условие $c^2 = 0$ в (11) выполняется всегда, т.к. для всех ненулевых квадратов A^2 и B^2 имеем $n(2B)^2 \neq A^2$, и в левой части – квадратичный невычет. Аналогичные предыдущему случаю рассуждения приводят к оценке среднего числа отобранных пар $(a, \pm b)$ равной $M_2 = \frac{(p-1)^2}{4}$. Эта оценка определяет среднее число эллиптических кривых с двумя точками четвертого 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, 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 $\left(A^2, B^2\right)$. На основе условий (9) и формул (10), (11) можно предложить следующий алгоритм построения канонических кривых с двумя точками четвертого порядка:

1. В поле F_p задаем произвольное значение пары квадратичных вычетов $\left(A^2, B^2\right)$ 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 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 четвертого 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 $\left(A^2, B^2\right)$ (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 четвертого порядка. Далее, как описано в [3], строится изоморфная кривая в форме Эдвардса.

Список литературы: 1. *Edwards, H.M.* A normal form for elliptic curves // Bulletin of the American Mathematical Society. – Volume 44, Number 3, July 2007. – PP. 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. – 2011. – Вып. 167. – 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. – 2012. – №2. – С.225-227. 5. *Бессалов, А.В., Дихтенко, А.А.* Криптостойкие кривые Эдвардса над простыми полями // Прикладная радиоэлектроника. – 2013. – Т.12, №2. – С.107-113. 6. *Бессалов, А.В., Телиженко, А.Б.* Криптосистемы на эллиптических кривых : учеб. пособие. – К. : ІВЦ «Політехніка», 2004. – 224с.

Национальный технический университет Украины «КПИ»
Донецкий национальный университет

Поступила в редколлегию 05.11.2013