КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ОЦЕНКА

УДК 681.3.06

ПОСТРОЕНИЕ КРИВОЙ ЭДВАРДСА НА БАЗЕ ИЗОМОРФНОЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В КАНОНИЧЕСКОЙ ФОРМЕ

А.В. БЕССАЛОВ

Получены условия существования канонических кривых, изоморфных кривым в форме Эдвардса над простым полем. Найдена зависимость параметра d кривой Эдвардса от параметров канонической кривой. Приведено новое доказательство для точных формул расчета числа кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b.

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

ВВЕДЕНИЕ

Перспективным классом эллиптических кривых сегодня являются кривые в форме Эдвардса [1–6], рекордные по быстродействию и удобные для программирования. Двойная симметрия их в координатах поля характеристики $p > 2$ порождает четырехкратную избыточность по числу точек N_E. Так как $N_E \equiv 0(\mathrm{mod}4)$, циклические кривые Эдвардса всегда содержат одну точку 2-го порядка и две точки 4-го порядка. Кривых в канонической форме с таким свойством сравнительно немного, поэтому для построения изоморфных им кривых Эдвардса следует решить задачу поиска кривых в форме Вейерштрасса с двумя точками 4-го порядка. В работе [6] мы ввели зависимый от традиционных параметров (a, b) канонической кривой параметр c как единственный в поле F_p корень кубического уравнения. В ней получены системы линейных уравнений для неизвестных параметров a и c^2 с решениями, выраженными через квадратичные вычеты и невычеты. Для нахождения точного числа канонических кривых с ненулевыми параметрами, изоморфных форме Эдвардса, потребовалось сформулировать и доказать две леммы о числе решений уравнений, связывающих суммы вычетов и невычетов. Доказательства опираются на схему Гаусса распределения квадратичных вычетов. В итоге удалось найти формулы расчета точного числа кривых с заданными свойствами для любых $p \equiv 3\mathrm{mod}4$ и $p \equiv 1\mathrm{mod}4$.

В настоящей работе, опираясь на свойства кривых в канонической форме, автор нашел функциональную связь между параметром d кривой Эдвардса и параметрами изоморфной канонической кривой. Далее приводится новое более лаконичное доказательство утверждения, определяющего формулы расчета точного числа кривых Эдвардса, изоморфных кривым в форме Вейерштрасса с ненулевыми параметрами a и b. Кроме того, приведен алгоритм поиска изоморфных форме Эдвардса кривых, полезных для криптографии.

1. ОПРЕДЕЛЕНИЕ ФУНКЦИОНАЛЬНОЙ ЗАВИСИМОСТИ МЕЖДУ ПАРАМЕТРАМИ КРИВОЙ В ФОРМЕ ЭДВАРДСА И КАНОНИЧЕСКОЙ КРИВОЙ

Каноническая кривая над полем характеристики $p \neq 2, 3$ описывается известным уравнением [7]

$$\mathbf{E}_p : y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0,\ a,b \in F_p. \quad (1)$$

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

$$y^2 = (x - c)(x^2 + cx + a + c^2),$$

$$b = -c^3 - ac,\ c \in F_p. \quad (2)$$

Определим условия, накладываемые на параметры a и c, при которых имеется единственная точка 2-го порядка и 2 точки 4-го порядка. Второй задачей в этом разделе будет нахождение зависимости между параметрами a и c канонической формы эллиптической кривой и параметром d кривой $x^2 + y^2 = 1 + dx^2y^2$ в форме Эдвардса.

Примем $u = x - c$, тогда уравнение (3) представляется в форме Монтгомери [2,3]

$$y^2 = u(u^2 + 3cu + a + 3c^2). \quad (3)$$

Парабола в правой части (4) не имеет корней в поле F_p, если дискриминант квадратного уравнения является квадратичным невычетом, т.е.

$$9c^2 - 4(a + 3c^2) = -(3c^2 + 4a) \neq A^2. \quad (4)$$

Это условие гарантирует существование единственной точки 2-го порядка кривой (3), определяемой для (3) как $D = (0,0)$. Условие $A^2 \neq 0$, входящее в (4), исключает появление кратных корней кубического уравнения и, тем самым, сингулярные кривые [7].

Пусть $P = (u_1, y_1)$ – точка 4-го порядка кривой (3). Ее удвоение $2P = D$ дает координаты точки $D = (0, 0)$. При удвоении мы строим касательную к кривой в точке P, которая проходит через точку (0,0). Таким образом из (3)

$$\left.\frac{dy}{du}\right|_{u=u_1}=\frac{3u_1^2+6cu_1+3c^2+a}{2y_1}=\frac{y_1}{u_1}$$

Отсюда

$$2y_1^2=3u_1^3+6cu_1^2+(3c^2+a)u_1. \qquad (5)$$

С другой стороны, в этой же точке согласно (3) имеем

$$2y_1^2=2u_1^3+6cu_1^2+2(3c^2+a)u_1. \qquad (6)$$

Из системы уравнений (5), (6) получим квадраты для координат точки P 4-го порядка

$$u_1^2=3c^2+a,\quad y_1^2=2u_1^3+3cu_1^2. \qquad (7)$$

Из последнего выражения можно теперь получить

$$3c=\frac{y_1^2}{u_1^3}\left(1-2\frac{u_1^3}{y_1^2}\right)u_1=2\frac{1+d}{1-d}u_1 \qquad (8)$$

где

$$d=1-4\frac{u_1^3}{y_1^2}. \qquad (9)$$

Формулы (7), (9) позволяют выразить параметр d через параметры a и c канонической формы кривой

$$d=\frac{3c-2u_1}{3c+2u_1},\qquad u_1=(-1)^{\alpha}\sqrt{3c^2+a},\qquad \alpha\in\{0,1\}. \qquad (10)$$

Здесь с помощью двоичного α выбирается одно из решений квадратного уравнения u_1, которое принадлежит кривой (3) и дает ровно две точки 4-го порядка. Второе решение не может лежать на кривой: это порождает четыре точки 4-го порядка, что нарушает структуру группы [7].

Из (4) и (7) следует, что необходимыми условиями существования одной точки 2-го и двух точек 4-го порядков являются следующие соотношения, выраженные через символы Лежандра как

$$a)\ \left(\frac{-(3c^2+4a)}{p}\right)=-1,\quad b)\ \left(\frac{(3c^2+a)}{p}\right)=1. \qquad (11)$$

С учетом (7) и (8) и деления на u_1^3 уравнение (3) теперь может быть приведено к виду

$$\frac{1}{1-d}v^2=u^3+2\frac{1+d}{1-d}u^2+u. \qquad (12)$$

Эта форма кривой с помощью сравнительно несложной замены переменных $(u.v)\to(x,y)$ [2,3] приводится к кривой в форме Эдвардса

$$x^2+y^2=1+d\,x^2y^2,\ d\neq 0,\ 1,\ \left(\frac{d}{p}\right)=-1. \qquad (13)$$

Класс изоморфных кривых Эдвардса

$$X^2+Y^2=e^2(1+d^*X^2Y^2),\ d^*=e^{-4}d, \qquad (14)$$

определяется линейной заменой переменных $x\to e^{-1}X$, $y\to e^{-1}Y$. Такая трансформация расширяет множество всех кривых в $(p-1)/2$ раз, но практически бесполезна (более того, добавление нового параметра e усложняет групповые операции).

Как нетрудно видеть из (12), заменой $d\to d^{-1}$ получаем кривую кручения с порядком $N_E^t=p+1+t$, симметричным порядку $N_E=p+1-t$ исходной кривой относительно середины $p+1$. Заметим, что для кривых Эдвардса порядок кривой $N_E=0\bmod 4$, поэтому след уравнения Фробениуса t может быть равен 0 лишь для значений модуля $p=3\bmod 4$. В этом случае элемент поля (-1) является квадратичным невычетом, и при значении $d=d^{-1}=-1$ пара кривых кручения вырождается в одну суперсингулярную кривую с порядком $N_E=p+1$. Это следует также из уравнения (12), которое при $d=-1$ принимает вид $y^2=u^3+u$ [7]. В форме (1) это кривая с коэффициентом $b=0$.

В криптографических приложениях не используются уязвимые к MOV-атаке кривые с нулевыми параметрами a или b. Возникает вопрос о числе кривых Эдвардса, изоморфных каноническим кривым с ненулевыми коэффициентами a и b. Эта задача получила точное решение в работе [6] на основе свойств параметров a и c канонических кривых, при этом нам пришлось сформулировать и доказать две леммы в теории квадратичных вычетов и теорему. В следующем разделе мы более лаконично докажем полученные в [6] результаты, опираясь в основном на свойства кривой в форме Эдвардса.

2. НОВОЕ ДОКАЗАТЕЛЬСТВО ДЛЯ РАСЧЕТА ТОЧНОГО ЧИСЛА КРИВЫХ ЭДВАРДСА, ИЗОМОРФНЫХ КРИВЫМ В КАНОНИЧЕСКОЙ ФОРМЕ С НЕНУЛЕВЫМИ ПАРАМЕТРАМИ *A* И *B*

Утверждение. Число кривых Эдвардса (14), изоморфных кривым (1) в канонической форме с параметрами $a\neq 0$ и $b\neq 0$ над полем F_p с двумя точками 4-го порядка определяется формулами:

I. При $p\equiv 3\bmod 4$

(α) $M_\alpha=(p-1)(p-7)/4$, если $\left(\frac{3}{p}\right)=1$;

(β) $M_\beta=(p-1)\,)(p-3)/4$, если $\left(\frac{3}{p}\right)=-1$;

II. При $p\equiv 1\bmod 4$

(γ) $M_\gamma=(p-1)^2/4$.

Доказательство.

1. Пусть $p\equiv 3\bmod 4$, тогда (-1) – квадратичный невычет [7], т.е. $\left(\frac{-1}{p}\right)=-1$ и для $(11a)$ невычет заменяем квадратичным вычетом

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

Аргументы символов Лежандра (11) являются линейными функциями параметров a и c^2. Следовательно, имеем невырожденную систему двух линейных уравнений над полем F_p

$$3c^2+4a=A^2,$$
$$3c^2+a=B^2,$$

с решениями:

$$a = 3^{-1}(A^2 - B^2),\ c^2 = 9^{-1}(4B^2 - A^2). \qquad (15)$$

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, т. к. из $c = 0 \Rightarrow b = -c^3 - ac = 0$). Из (11) следует, что $A^2 \neq 0$ и $B^2 \neq 0$.

Так как параметр d в форме кривой Эдвардса (13) пробегает все квадратичные невычеты поля F_p, их число равно $(p-1)/2$. Из этого числа исключим значение $d = -1$, которое порождает коэффициенты $c = b = 0$ (см. формулы (1) и (10)). Остается $(p-3)/2$ квадратичных невычетов d.

Пусть $\left(\frac{3}{p}\right) = 1$. Из (15) следует, что при $a = 0$ $A^2 = B^2$ и $c^2 = 3^{-1}A^2$, т.е. существует решение для с и, соответственно, для параметра d, равного согласно (10)

$$d = \frac{3c \mp 2c\sqrt{3}}{3c \pm 2c\sqrt{3}} = \frac{\sqrt{3} \mp 2}{\sqrt{3} \pm 2}. \qquad (16)$$

Нетрудно видеть, что оба решения (16) являются невычетами. Например, умножив числитель и знаменатель на знаменатель, получим в знаменателе квадрат, а в числителе разность квадратов $3 - 4 = -1$, т.е. невычет при $p \equiv 3 \bmod 4$. Следовательно, из $(p-3)/2$ значений невычетов d, исключающих значение $b = 0$, следует удалить еще 2 значения (16), порождающих коэффициент $a = 0$. При этом остается $(p-7)/2$ допустимых значений невычетов d. Для каждой кривой Эдвардса в форме (13) существует $(p-1)/2$ изоморфных кривых (14) с соответствующим числом квадратов e^2. Общее число кривых Эдвардса с оговоренными свойствами равно $M_\alpha = (p-1)(p-7)/4$. Утверждение (α) доказано.

Пусть теперь $\left(\frac{3}{p}\right) = -1$. В этом случае $a \neq 0$, т. к. при $A^2 = B^2$ уравнение $c^2 = 3^{-1}A^2$ (см.(15)) не имеет решения. Тогда имеем $(p-3)/2$ допустимых значений невычетов d, которые вместе с $(p-1)/2$ значениями квадратов e^2 для изоморфных кривых дает $M_\beta = (p-1))(p-3)/4$ кривых. Утверждение (β) доказано.

2. Пусть теперь $p \equiv 1 \bmod 4$, тогда (-1) – квадратичный вычет, т.е. $\left(\frac{-1}{p}\right) = 1$. [7]. Тогда для (11*a*), принимая А невычетом в системе уравнений

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

$$3c^2 + a = B^2,$$

можно найти ее единственное решение

$$\Rightarrow a = 3^{-1}(A - B^2),\ c^2 = 9^{-1}(4B^2 - A). \qquad (17)$$

Здесь, как видим, нулевые решения для a и c^2 невозможны. Итак, мы имеем $(p-1)/2$ допустимых значений невычетов d, которые вместе с $(p-1)/2$ значениями квадратов e^2 для кривых в форме (14) дает $M_\gamma = (p-1)^2/4$ кривых. Утверждение (γ) доказано.

Можно заметить, что приведенное здесь доказательство формул, определяющих точное число кривых Эдвардса с оговоренными свойствами, существенно проще предыдущего доказательства [6].

Рассчитанные по формулам (α), (β), (γ) мощности семейств кривых, изоморфных кривым Эдвардса при значениях $p = 7, 11, 13, \ldots, 47$ приведены в табл. 1.

Таблица 1

p	7	11	13	17	19	23	29	31	37	41	43	47
M	6	10	36	64	72	88	196	210	324	400	420	529

Пример. Требуется построить кривую Эдвардса на базе изоморфной канонической кривой с двумя точками 4-го порядка над полем F_7. Примем $A^2 = 2$, $B^2 = 1$, тогда согласно (15) $c^2 = 1$ – квадрат в поле, $a = 5$ и $b = \pm c(c^2 + a) = \pm 1$. Получили пару кривых кручения $y^2 = x^3 + 5x \pm 1$ с порядками $N_E = 12$ и $N_E{}^t = 4$. Первая кривая с параметром $c = 1$ в форме Монтгомери (3) имеет вид $y^2 = u(u^2 + 3u + 1)$. Ее точка второго порядка $D = (0,0)$, а координаты точек 4-го порядка первой кривой в соответствии с (7) равны

$$u_1{}^2 = 3c^2 + a = 1 \Rightarrow u_1 = -1,$$
$$y_1{}^2 = 2u_1{}^3 + 3cu_1{}^2 = 1 \Rightarrow y_1 = \pm 1.$$

Здесь решение $u_1 = 1$, не лежащее на кривой (3), отбрасывается. Переход к кривой Эдвардса (13) осуществляется вычислением d согласно (10)

$$d = \frac{3+2}{3-2} = 5.$$

Кривая $x^2 + y^2 = (1 + 5x^2y^2) \bmod 7$ имеет порядок 12. Соответствующая кривая кручения с параметром $d^{-1} = 3$ имеет порядок 4. Кривая с параметром $d = -1$ отбрасывается. Других кривых в форме (13) при $p = 7$ не существует. Для каждой из этих двух кривых можно получить по 3 изоморфных кривых (14) с коэффициентами $e^2 = 1, 4, 2$. Вообще над полем F_7 существует, как следует из таблицы 1, 6 кривых Эдвардса, изоморфных каноническим кривым с ненулевыми параметрами a и b и двумя точками 4-го порядка. Здесь каждая пара кривых кручения содержит по 3 изоморфных пар.

Формулы (15), (17) конструктивны, т. к. 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 (11) и формул (15), (17) 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) или пары (А, B^2) и согласно (15) или (17) 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 (2).

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) или (A, B^2) (возвращаемся в п.1).

В предложенном виде алгоритм достаточно быстро приводит к кривой с двумя точками 4-го порядка. Далее, как описано в данной работе, 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. – P. 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, том 11, № 2, 2012. – С. 225–227.

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

[6] *Бессалов А.В., Дихтенко А.А., Цыганкова О.В.* Плотность канонических эллиптических кривых со свойством изоморфизма к форме Эдвардса. Известия ЮФУ. Технические науки", вып. №4, 2014. – С. 146–153.

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

Поступила в редколлегию 6.06.2014

Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор кафедри ММЗИ ФТИ НТУУ «КПИ». Научные интересы: криптография, теория корректирующего кодирования.

УДК621.391.7:336.71

Побудова кривої Едвардса на базі ізоморфної еліптичної кривої у канонічній формі / А.В. Бессалов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 286–289.

Отримано умови існування канонічних кривих, які ізоморфні кривим у формі Едвардса над простим полем. Знайдено залежність параметра *d* кривої Едвардса від параметрів канонічної кривої. Наведено новий доказ для точних формул розрахунку кількості кривих Едвардса, які є ізоморфними канонічним кривим з ненульовими параметрами *a* і *b*.

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

Табл.: 01. Бібліогр.: 07 найм.

UDC 621.391.7:336.71

Construction of Edwards curve on the basis of an isomorphic elliptic curve in an canonical form / A.V. Bessalov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 286–289.

Living conditions of canonical curves, isomorphic to curves in the Edwards form over a simple field, are established. The dependence of Edward curve parameters *d* on parameters of a canonical curve is found. A new proof for exact calculation formulae of Edwards curves number, isomorphic to canonical curves with nonzero parametres *a* and *b* is provided.

Keywords: canonical elliptic curve, Edwards curve, torsion curve, curve parametres, isomorphism, quadratic residue, non-quadratic residue.

Tab.: 01. Ref.: 07 items.