УДК 681.3.06

Бессалов А.В.

Число изоморфизмов и пар кручения кривых Эдвардса над простым полем

Рассмотрена трансформация канонической формы эллиптической кривой в изоморфную форму Эдвардса. Дан анализ условий существования точек 8-го порядка. Получены оценки для числа изоморфизмов и пар кручения кривых в форме Эдвардса.

Розглянуто перетворення канонічної форми еліптичної кривої в ізоморфну форму Едвардса. Дано аналіз існування точок 8-го порядку. Отримано оцінки кількості ізоморфізмів і пар кручення кривих у формі Едвардса.

Transformation of a canonical form of an elliptic curve in isomorphic Edwards's-form is considered. The analysis of existing conditions of points of 8th order is given. Estimations for number of isomorphisms and torsion-pairs in the Edwards-form are received.

Введение

Среди изобилия различных форм представления эллиптических кривых [5] в последние годы появилась новая форма (точнее, давно забытая старая), предложенная в работе Эдвардса [1] и обладающая рядом замечательных свойств. Эти свойства сразу были замечены и исследованы криптографами. Одной из первых публикаций в развитие этого направления следует отметить работу [2] (за ней последовала серия работ этих авторов). Оказалось, что наряду со свойствами полноты и универсальности закона сложения, заменой точки на бесконечности аффинной точкой (нуль группы), кривые Эдвардса среди известных являются наиболее производительными: в проективных координатах групповая операция выполняется минимальным числом 10M + 1S + 2D операций в поле (M - умножение, S – возведение в квадрат, D – умножение на параметр кривой).

В настоящей работе более подробно излагается преобразование канонической кривой в форму Эдвардса (в работе [2] изоморфизм сразу строится из формы Монтгомери), проанализированы условия существования точек 8-го порядка, даны простые оценки для расчета числа изоморфизмов и пар кривых кручения, рассмотрены примеры. Изоморфные кривые могут

найти различные приложения, например, при формировании псевдослучайных последовательностей, обновлении параметров в протоколах и пр.

1. Трансформация канонической эллиптической кривой в форму Монтгомери

Каноническая форма эллиптической кривой над простым полем F_p ($p \neq 2, 3$) имеет вид

$$\mathbf{E}: \quad \tilde{y}^2 = \tilde{x}^3 + a\tilde{x} + b, \qquad a, b \in F_p \ , \tag{1}$$

Если кривая имеет единственную точку 2-го порядка $\widetilde{D} = (c_0, 0)$ и две точки 4-го порядка $\pm\tilde{P} = (\tilde{x}_1, \tilde{y}_1)$, таких, что $2\tilde{P} = \widetilde{D}$, то она может быть преобразована в форму Эдвардса

$$\mathbf{E_{ED}}: \quad X^2 + Y^2 = 1 + d\,X^2Y^2, \quad d(1-d) \neq 0, \ d \neq A^2, d \in F_p{}^* . \tag{2}$$

Формулы преобразования координат существенно упрощаются, если вместо (1) в качестве промежуточной кривой использовать кривую в форме Монтгомери

$$\mathbf{E_M}: \quad v^2 = u^3 + eu^2 + gu, \qquad e, g \in F_p \ , e = 3c_0 \ , \ g = 3c_0{}^2 + a, \tag{3}$$

изоморфную кривой (1) при $\tilde{x} = u + c_0$, $\tilde{y} = v$, причем точка 2-го порядка единственна при дискриминанте квадратного уравнения $\Delta = -(3c_0{}^2 + 4a) \neq A^2 \ mod p$. Именно эта кривая использовалась в [2] в качестве базовой кривой вместо (1).

Изоморфизм между (1) и (3) переводит точку 2-го порядка $\widetilde{D} = (c_0, 0)$ в точку $D_\mathrm{M} = (0, 0)$ в координатах (u, v). По условию кривая содержит 2 точки 4-го порядка $\pm D_\mathrm{M} = (u_1 \ , \ \pm v_1)$. Выразим параметры e, g кривой (3) через координаты $u_1 \neq 0 \ , v_1 \neq 0$. Производная кривой в этой точке равна

$$\frac{dv}{du}\,|u = u_1| = \frac{3u_1^2 + 2eu_1 + g}{2v_1} = \frac{v_1}{u_1}, \ u_1 \neq 0 \ , v_1 \neq 0.$$

Из этого равенства с учетом (3) следует

$$g = u_1^2 \ , \quad e = \frac{v_1^2}{u_1^3}\left(1 - 2\frac{u_1^3}{v_1^2}\right)u_1 = 2\frac{1+d}{1-d}\,u_1, \tag{4}$$

где

$$d = 1 - 4\frac{u_1^3}{v_1^2}, \qquad v_1^2 = 2u_1^3 + eg. \tag{5}$$

Делением на u_1^3 с учетом (4) и (5) уравнение (3) теперь может быть представлено парой кривых кручения:

$\mathbf{E_M}$: $$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u, \tag{6}$$

$\mathbf{E_M}^t$: $$\frac{d}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u, \tag{7}$$

Поскольку d – квадратичный невычет в $F_p{}^*$, решения (6) и (7) взаимоисключающи (кроме точки (0,0)), а порядки $N_E = p + 1 \pm t$ симметричны относительно $p + 1$. Из (6), (7) очевидно, что переход к кривой кручения осуществляется простой заменой $d \to d^{-1}$.

Ограничения для параметра d. Так как $u_1 \neq 0, d \neq 1$. Если допустить, что $d = 0$, то в уравнении (3) появляются кратные корни кубики, т.е. нарушается несингулярность кривой. Требование единственности точки второго порядка эквивалентно тому, что дискриминант правой части уравнения (6) или (7) после выделения корня $u = 0$ должен быть невычетом

$$\Delta = 4\left(\left(\frac{1+d}{1-d}\right)^2 - 1\right) = \frac{16d}{(1-d)^2} \neq A^2.$$

Отсюда следует, что $d \neq A^2$ – квадратичный невычет в поле F_p.

2. Трансформация кривой Монтгомери в форму Эдвардса. Закон сложения точек

Прямое и обратное преобразование координат $(u, v) \Leftrightarrow (X, Y)$ задается рациональными функциями

$$X = 2\frac{u}{v}, \qquad Y = \frac{u-1}{u+1}, \tag{8}$$

$$u = \frac{1+Y}{1-Y}, \qquad v = 2\frac{1+Y}{1-Y}X^{-1}. \tag{9}$$

Умножение (6) на $(1 - d)/u^2$ дает

$$\left(\frac{v}{u}\right)^2 = (1-d)(u + u^{-1}) + 2(1+d).$$

С учетом (8) и (9) получим

$$\frac{2}{X^2} = (1 + d) + (1 - d)\frac{1+Y^2}{1-Y^2}.$$

Отсюда уже нетрудно получить уравнение кривой Эдвардса (2)

$$\mathbf{E_{ED}}: \qquad X^2 + Y^2 = 1 + d\,X^2Y^2.$$

Эта кривая изоморфна (или бирационально эквивалентна) кривой Монтгомери (6). Заменой $d \to d^{-1}$ легко перейти к кривой кручения, изоморфной кривой Монтгомери (7). Заметим, что если $d = -1 = d^{-1}$, кривая кручения совпадает с базовой кривой (параметр $t = 0$, $N_E = p + 1$). Так как d – невычет, то этот случай имеет место при модуле $p \equiv 3 \bmod 4$.

Линейное смещение координат точек $x = cX,\ y = cY$ дает изоморфную кривую

$$x^2 + y^2 = c^2\left(1 + \tilde{d}\,x^2y^2\right), \qquad \tilde{d} = c^{-4}d,\ \ \tilde{d}(1 - \tilde{d}c^4) \neq 0,\ \ \tilde{d} \neq A^2. \qquad (10)$$

Закон сложения двух точек этой кривой имеет вид [2]

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{c(1+\tilde{d}x_1x_2y_1y_2)},\ \frac{y_1y_2 - x_1x_2}{c(1-\tilde{d}x_1x_2y_1y_2)}\right). \qquad (11)$$

При ограничениях на параметр $\tilde{d}$, определенных в (10), формула сложения является *полной* в том смысле, что не существует исключительных точек, в которых знаменатели в (11) обращаются в 0 (т.е. $\tilde{d}x_1x_2y_1y_2 \neq \pm 1$). Доказательство этого приведено в [2] (теорема 3.3). Другое отличительное свойство формулы (11) – ее *унифицированность*: она справедлива как для сложения различных точек, так и для удвоения точки, причем составляющими суммы могут быть любые точки, включая точку **O** (нуль группы) и обратную точку. Последнее свойство – несомненное преимущество арифметики кривых Эдвардса перед эллиптическими кривыми **E**, существенно упрощающее программирование операций с точками в группе $\mathbf{E_{ED}}$.

Нулем абелевой группы точек кривой в форме Эдвардса является точка с аффинными координатами $(0, c) = \mathbf{O}$ (в отличие от точки на бесконечности эллиптической кривой E, не имеющей аффинных координат). Подстановка координат этой точки в (11) дает координаты другой точки. Точка, обратная точке $P = (x_1, y_1)$, определяется как $-P = (-x_1, y_1)$**.** Пары обратных точек симметричны относительно оси y (а не относительно оси x, как для кривой E). Сумма $P + (-P) = \mathbf{O}$**,** что легко проверяется законом сложения (11).

3. Точки малых порядков 2^k, k = 1..3

Любая кривая Эдвардса содержит ровно 1 точку 2-го порядка $D = (0, -c)$ и 2 точки 4-го порядка $\pm P = (\pm c, 0)$. Эти точки вместе с точкой O = (0, c) являются исключительными точками, лежащими на осях x, y (т.е. других точек на осях не существует). Для точек 4-го порядка выполняется равенство $2P = D$, что легко проверяется подстановкой координат в (11). Интересными являются следующие свойства: 1). Сумма двух *симметричных* относительно y-координаты точек $(x_1, y_1) + (x_1, -y_1) = (0, -1) = D$, т.е. дает точку 2-го порядка; 2). Сумма (разность) двух *взаимных* точек $(x_1, y_1) \pm (y_1, x_1) = (\pm 1, 0) = \pm P$, т.е. дает точку 4-го порядка. Кроме того, половина всех кривых содержит 4 точки 8-го порядка. Они лежат на прямых $y = \pm x$. Их координаты $(\pm x_0, \pm x_0) = Q_i$, i = 1..4, являются решениями возникающего из (10) биквадратного уравнения $\tilde{d}x^4 - 2c^{-2}x^2 + 1 = 0$. Действительно, удвоение любой из этих точек дает

$$2Q_i = \left(\frac{\pm 2x_0^2}{c\left(1+dx_0^4\right)}, 0\right) = (\pm c, 0) = \pm P,$$

т.е. получаем точки 4-го порядка. В отношении точек 8-го порядка сформулируем и докажем следующие утверждения.

Утверждение 1. Пусть $p \equiv 1 \bmod 4$. Тогда одна из кривых пары кручения, для которой $(1 - c^4\tilde{d}) = A^2$, имеет точки 8-го порядка (и, поэтому, $N_E \equiv 0 \bmod 8$), а другая кривая – не имеет ($N_E \equiv 4 \bmod 8$).

Доказательство. Положим $y = \pm x$ в (10), тогда уравнение $\tilde{d}x^4 - 2c^{-2}x^2 + 1 = 0$ имеет решения в поле F_p, если дискриминант уравнения $\Delta = 4(c^{-4} - \tilde{d}) = B^2$ – квадратичный вычет в поле. С учетом (10) это равнозначно тому, что $(1 - d)$ – квадратичный вычет. В этом случае биквадратное уравнение имеет два решения $\pm x_0$ в поле F_p, которые дают координаты $(\pm x_0, \pm x_0)$ точек 8-го порядка (следовательно, порядок кривой $N_E \equiv 0 \bmod 8$). Перейдем к кривой кручения обращением $d \to d^{-1}$. Тогда элемент поля

$$1 - d^{-1} = (-1)\frac{1-d}{d} \qquad (12)$$

при $p \equiv 1 mod 4$ является невычетом, так как (–1) – вычет в поле [4], а d – невычет. Для кривой кручения, таким образом, биквадратное уравнение решений не имеет, точки 8-го порядка отсутствуют и порядок кривой кратен 4.

Утверждение 2. Пусть $p \equiv 3 \bmod 4$. Тогда при $(1 - c^4\tilde{d}) = A^2$ обе кривые пары кручения имеют точки 8-го порядка ($N_E \equiv 0 \bmod 8$), а при $(1 - c^4\tilde{d}) \neq A^2$ – не имеют ($N_E \equiv 4 \bmod 8$).

Отличие доказательства этого утверждения от предыдущего в том, что в равенстве (12) при переходе к кривой кручения (-1) – невычет в поле при

$p \equiv 3 \bmod 4$[4]. Поэтому в зависимости от значения $(1 - d)$ (со свойством вычет - невычет) обе кривые пары кручения либо имеют точки 8-го порядка, либо нет.

Для последнего случая особым является значение невычета $d = -1$. При этом $d^{-1} = d$, пара кручения вырождается в одну суперсингулярную кривую с порядком $N_E = p + 1$ и параметром $t = 0$. Это следует также из свойств изоморфной для этого примера кривой Монтгомери $v^2 = (u^3 + u) \bmod p$ при $p \equiv 3 \bmod 4$[4].

На основе утверждений 1 и 2 можно прийти к выводу, что приблизительно половина кривых имеет точки 8-го порядка (и, возможно, более высоких степеней 2), а половина – нет. Для криптоприложений, как известно, следует выбирать кривые с минимальным кофактором простого числа, т.е. избегать кривых с точками 8-го порядка. Для этого, как следует из анализа выше, целесообразно ввести дополнительное ограничение на параметр кривой d: элемент $(1 - d)$ рекомендуется выбирать как невычет в мультипликативной группе поля F_p.

Кроме 4-х точек на осях x и y и, возможно, точек 8-го порядка на прямых $y = \pm x$, остальные точки кривой Эдвардса собираются в семейства по 8 точек $(\pm x_i, \pm y_i)$, $(\pm y_i, \pm x_i)$, расположенных на концентрических окружностях с центром в начале координат. Любая из этих точек определяет все семейство. Сумма любой пары точек этого семейства дает одну из точек O, D или $\pm P$. Вместе с тем порядки точек всегда совпадают только для обратных точек.

Пример 1. Каноническая эллиптическая кривая $y^2 = (x^3 + 2x + 5) \bmod 13$ имеет порядок $N_E = 12$ и единственный корень $c_0 = 8$ кубики. Изоморфная ей кривая Монтгомери согласно (3) имеет вид $v^2 = u^3 - 2u^2 - u$. С помощью (4), (5) находим ее точки 4-го порядка $\pm P = (8, \pm 5)$ и параметр $d = 8$. Итак, изоморфная канонической кривой E кривая Эдвардса имеет форму $x^2 + y^2 = (1 + 8x^2y^2) mod 13$ и порядок $N_E = 12$. Ее точки представлены на рис.1а. На рис.1б даны точки кривой кручения с параметром $d` = d^{-1} = 5$ и порядком $N_E = 16$. Эти изображения с двойной симметрией напоминают калейдоскоп.

(а) (б)

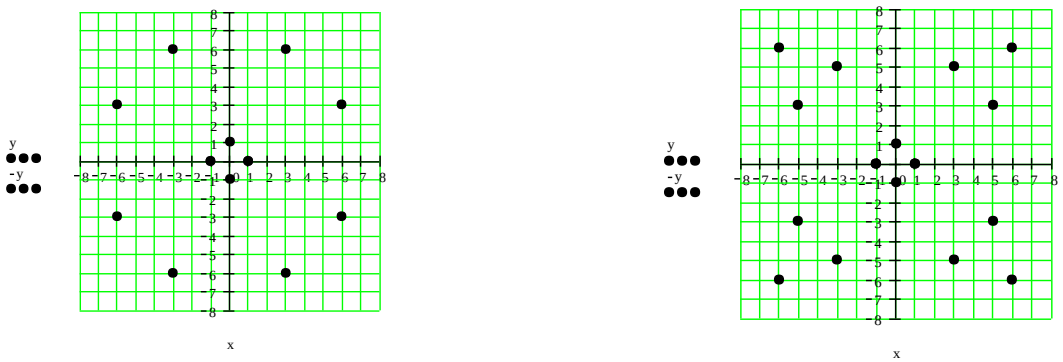

Рис.1

Первая кривая содержит 2 точки 3-го порядка. Из равенства 2Q = – Q, формулы сложения (11) и уравнения кривой (10) получим равенство, связывающее координаты x_Q, y_Q точки 3-го порядка

$$\frac{2x_Q y_Q}{1+dx_Q^2 y_Q^2} = -x_Q \Rightarrow \; y_Q^2 + x_Q^2 + 2y_Q = 0, \Rightarrow \; y_Q = -1 \pm \sqrt{1-x_Q^2}.$$

Для нашего примера точку 3-го порядка легко найти: при $x_Q = 3$, $y_Q = -1 \pm 2$, таких точек не существует; при $x_Q = 6$, $y_Q = -1 \pm 4$, тогда точка Q = (6, 3) – одна из точек 3-го порядка (вторая точка (−Q)). Точки $\pm R = \pm Q + D = (\pm 6, -3)$ имеют порядок 6, и, следовательно, точки с координатами $x_i = \pm 3$ – порядок 12. Любая из них генерирует всю группу.

Кривая кручения (рис.1б) имеет точки 8-го порядка $(\pm 6, \pm 6)$. В соответствии с утверждением 1 для ее параметра $d` = d^{-1} = 5$ выполняется свойство $(1 - d`) = 9 mod 13$ – вычет в поле F_{13}.

4. Число кривых Эдвардса, пар кручения и изоморфизмов

В некоторых криптографических задачах, использующих изоморфизмы, требуется знать мощность множества изоморфных преобразований или ее оценки. Для кривых в форме Эдвардса эта задача решается просто.

При c = 1 число различных кривых равно числу невычетов d поля $\mu = \frac{p-1}{2}$, а общее число различных кривых при всех значениях c^2 равно M = μ^2. Соответственно, для каждой кривой с фиксированным d при всех c^2 имеется ровно μ изоморфных кривых. Число пар кривых кручения при $p \equiv 1 \bmod 4$ равно $\mu/2$, а при $p \equiv 3 \bmod 4$ $-(\mu - 1)/2$. В последнем случае число пар уменьшается на 1, так как при $d = -1$ пара вырождается в одну кривую.

Пример 2. Расширим пример 1 и получим все кривые Эдвардса над полем F_{13}. В таблицу 1 сведены параметры a и b для $(p - 1)/2 = 6$ канонических кривых E с единственной точкой 2-го порядка, параметры d изоморфных им кривых Эдвардса, параметры t и N_E этих кривых. Середина таблицы является осью симметрии для пар кручения с параметрами $\pm t$ и взаимообратными значениями d.

Таблица 1

a	2	1	2	7	4	7
b	1	2	5	1	3	5
d	2	6	8	5	11	7
t	6	2	2	– 2	– 2	– 6
N_E	8	12	12	16	16	20

Каждая из приведенных в таблице кривых Эдвардса может быть преобразована в $\mu = 6$ изоморфных кривых умножением уравнения (10) на различные значения c^2. В итоге имеем $\mu^2 = 36$ кривых, что составляет ¼ всех эллиптических кривых с $a, b \neq 0$ (их число для поля $F_{13} - 12^2$).

Заключение

Несмотря на уменьшение вчетверо пространства всех кривых и наличие минимального сомножителя 4 у порядка кривой кривые Эдвардса можно считать перспективным направлением эллиптической криптографии. В первую очередь их отличает наивысшая среди известных производительность выполнения групповой операции в проективных координатах [2], универсальность и полнота закона сложения. В существующих стандартах есть канонические кривые с кофактором 4, которые могут быть преобразованы в форму Эдвардса и с успехом использоваться в криптопротоколах.

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. Bernstein Daniel J., Lange Tanja, Farashahi R.R. Binary Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2008, PP.1..23.

4. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

5. Daniel J. Bernstein, Tanja Lange, Explicit-formulas database (2007). hyperelliptic.org/EFD.

Опубликовано: Радиотехника, №167, 2011. С.203-208.