УДК 681.3.06

А. В. Бессалов, Д. Б. Третьяков, О. В. Цыганкова

СВОЙСТВА ТОЧЕК МАЛЫХ ПОРЯДКОВ КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЕДВАРДСА

Дан анализ свойств точек порядков 2, 4, 8 кривой в обобщенной форме Эдвардса. Доказаны 3 теоремы об условиях существования точек 4-го и 8-го порядков кривой. На основе правил предельного перехода введена арифметика для групповых операций с особыми точками этих кривых, получены координаты для суммы произвольной и особых точек 2-го и 4-го порядков, имеющих бесконечную координату *x* или *y*. Дана новая классификация кривых в обобщенной форме Эдвардса на 3 непересекающиеся класса: полные кривые Эдвардса, кривые Эдвардса с квадратичным параметром и скрученные кривые Эдвардса. Доказано несуществование кривых в обобщенной форме Эдвардса порядка $2n$.

***Ключевые слова*:** кривая в обобщенной форме Эдвардса, скрученная кривая Эдвардса, полная кривая Эдвардса, параметр кривой, порядок точки, сложение точек, изоморфизм, квадратичное кручение, квадрат, неквадрат.

Введение

Эллиптические кривые в форме Эдвардса над простым полем перспективны для современных криптосистем. Как показано в работе [1], их производительность в среднем не менее чем в 1.5 раза превышает производительность кривых в форме Вейерштрасса. Арифметика этих кривых существенно упрощается в связи с наличием нейтрального элемента группы как неособой точки кривой (1,0).

Авторы работы [2] обобщили и расширили класс кривых Эдвардса [3] введением нового параметра a и снятием ограничения на неквадратичность параметра d кривой. Они назвали этот класс скрученными кривыми Эдвардса (Twisted Edwards Curves), а кривые, определенные в [3] – полными кривыми Эдвардса. Мы обнаружили, что кривые в форме Эдвардса разбиты в этой работе на пересекающиеся классы, в результате чего в статистических таблицах раздела 4 одни и те же кривые попадают в разные классы, что дает недостоверную статистику.

В данной работе мы даем анализ свойств точек порядков 2, 4 и 8 кривых в обобщенной форме Эдвардса, разбиваем их на классы и обосновываем несуществование таких кривых с порядком $2n$. В разделе 1 предлагается арифметика для групповых операций с особыми точками этих кривых, дан анализ точек малых порядков и формулы, связывающие их с другими точками кривой. Во 2-м разделе обсуждается некорректность классификации кривых и статистики их порядков в [2], предложена классификация кривых в обобщенной форме Эдвардса с разбиением на три непересекающиеся класса. Дан анализ свойств кривых всех 3-х классов и возможных значений порядков этих кривых. В 3-м разделе обосновано несуществование кривых в форме Эдвардса с кофактором 2 порядка кривой.

1. Свойства точек порядков 2, 4, 8 кривых в обобщенной форме Эдвардса

В работе [2] *скрученные кривые Эдвардса* (Twisted Edwards Curves) определены как обобщение кривых Эдвардса $x^2 + y^2 = 1 + dx^2y^2$ [1] путем ввода нового параметра a в уравнение

$$E_{E,a,d}: \quad ax^2 + y^2 = 1 + dx^2y^2, \quad a, d \in F_p^*, d \neq 1, a \neq d, p \neq 2.$$

Наряду с вводом параметра a авторы [2] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{\mathrm{ad}}{\mathrm{p}}\right) = \pm 1$. При $a = 1$ такая кривая получила в [2] название кривой Эдвардса, а если у нее d – неквадрат (то есть $\left(\frac{\mathrm{d}}{\mathrm{p}}\right) = -1$), то – полной кривой Эдвардса. Этот термин связан с полнотой закона сложения точек кривой [3]. В работе [4] мы предложили поменять местами x и y координаты в форме кривой Эдвардса с целью

сохранения горизонтальной симметрии обратных точек, принятой в теории эллиптических кривых. Опираясь на это свойство, определим кривую в обобщенной форме Эдвардса уравнением

$$E_{E,a,d}:\ x^2 + ay^2 = 1 + dx^2y^2, a, d \in F_p^*, d(d-a) \neq 0, d \neq 1, p \neq 2 \qquad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{(1-dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1+dx_1x_2y_1y_2)}\right). \qquad (2)$$

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

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1-dx_1^2y_1^2)}, \frac{2x_1y_1}{(1+dx_1^2y_1^2)}\right). \qquad (3)$$

Использование модифицированных законов (2), (3) позволяет сохранить горизонтальную симметрию (относительно оси x) обратных точек, принятую в криптографии. Определяя теперь обратную точку как $-P = (x_1, -y_1)$, получаем согласно (1) $(x_1, y_1) + (x_1, -y_1) = \boldsymbol{O}=(1,0)$. 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 и 2 или 4 точки 4-го порядка. Как следует из (1), на оси y могут лежать точки $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$ 4-го порядка, для которых $\pm 2\boldsymbol{F_0} = \boldsymbol{D_0} = (-1,\ 0)$. Эти точки существуют над полем F_p, если параметр a является квадратом.

Из уравнения (1) определим квадраты

$$x^2 = \frac{1 - ay^2}{1 - dy^2}, \qquad y^2 = \frac{1 - x^2}{a - dx^2},$$

порождающие в ряде случаев особые точки на бесконечности (знак "∞"мы ставим при делении на 0):

$$\boldsymbol{D_{1,2}} = \left(\pm\sqrt{\frac{a}{d}},\ \infty\right), \qquad \pm\boldsymbol{F_1} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \qquad (4)$$

Они возникают в случаях $\left(\frac{ad}{p}\right) = 1$ и $\left(\frac{d}{p}\right) = 1$, соответственно. По правилам обычного предельного перехода и закона удвоения (3) легко проверить, что $2\boldsymbol{D_{1,2}} = \mathbf{O}$, $\pm 2\boldsymbol{F_1} = \boldsymbol{D_0} = (-1,\ 0)$. Иными словами, при выполнении условий их существования особые точки $\boldsymbol{D_{1,2}}$ есть точки 2-го порядка, а особые точки $\pm\boldsymbol{F_1}$ – точки 4-го порядка. Нейтральный элемент группы **O** и точки 2-го, 4-го и 8-го порядков кривой в форме Эдвардса здесь и далее выделяются жирным шрифтом.

Кроме перечисленных, точки 4-го порядка могут существовать как неособые при ненулевых координатах x и y.

Теорема 1.1. *Точки 4-го порядка кривой* (1) *при* $x \neq 0$ *существуют тогда и только тогда, когда выполняются условия*:

$$\left(\frac{ad}{p}\right) = 1, \qquad p \equiv 3 mod 4.$$

Доказательство. *Необходимость.* Положим $2\boldsymbol{F_2} = 2(x_1, y_1) = \boldsymbol{D_1}$. Тогда согласно (2) и (4) запишем два уравнения

$$\frac{x_1^2 - ay_1^2}{(1 - dx_1^2y_1^2)} = \sqrt{\frac{a}{d}}, \qquad \frac{2x_1y_1}{(1 + dx_1^2y_1^2)} = \infty.$$

Отсюда $(1 + dx_1^2y_1^2) = 0, \Rightarrow x_1^2 + ay_1^2 = 0, \Rightarrow x_1^2 = -ay_1^2$. Из $x_1 \neq 0 \Rightarrow y_1 \neq 0$. Согласно первому из уравнений имеем:

$$\frac{2x_1^2}{1+\frac{d}{a}x_1^4} = \sqrt{\frac{a}{d}} \quad \Rightarrow \frac{d}{a}x_1^4 - 2\sqrt{\frac{d}{a}}x_1^2 + 1 = 0 \quad \Rightarrow \quad x_1^2 = \sqrt{\frac{a}{d}}, \quad y_1^2 = -\frac{1}{\sqrt{ad}}.$$

Итак, получаем точки с координатами:

$$\pm\boldsymbol{F_2} = \left(\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right), \pm\boldsymbol{F_3} = (-\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}). \quad (5)$$

Необходимыми условиями существования таких точек являются:

$$\text{(i)}: \quad \left(\frac{ad}{p}\right) = 1, \qquad \text{(ii)}: \quad p \equiv 3 mod 4. \quad (6)$$

Действительно, если β – примитивный элемент мультипликативной группы $F_p{}^*$, и β^2 – квадрат этой группы, то при условии (ii) в (6) $\beta^2\beta^{p-1} = \beta^{2+4k+2} = \beta^{4(k+1)}$. Значит, любой квадрат имеет квадратные корни и корни 4-й степени. Существование первых координат в (5) с учетом условия (i) в (6) доказано. Элемент (-1) есть неквадрат (квадратичный невычет) для данного случая [5]. Учитывая (6) и принимая значение $\left(\frac{-\sqrt{ad}}{p}\right) = 1$ (то есть, как квадрата, квадратичного вычета), при этом $\sqrt{ad}$ – неквадрат), получаем по 2 решения для вторых координат в точках (5). Так как квадраты ad и a/d имеют корни 4-й степени, такие точки в условиях (6) существуют. Необходимость условий (6) доказана.

Достаточность. Пусть выполняются условия (i) и (ii) в (6). Тогда существуют 4 точки $\pm\boldsymbol{F_{2,3}} = \pm\boldsymbol{F_{2,3}} = (\pm\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}})$, для которых согласно (3) получим $\pm 2\boldsymbol{F_{2,3}} = \boldsymbol{D_{1,2}}$. Так как удвоение точек $\boldsymbol{F_{2,3}}$ дает точки 2-го порядка, то определенные координатами (5) точки есть точки 4-го порядка. Это доказывает достаточность условий теоремы. Теорема доказана.

Точки $\pm\boldsymbol{F_{2,3}}$ можно рассматривать как точки деления на два точек 2-го порядка $\boldsymbol{D_{1,2}}/2$ [4].

За пределами теоремы 1.1 остались еще две точки 4-го порядка $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$ на оси y, если $\left(\frac{a}{p}\right) = 1$.

Например, для кривой $x^2 + 6y^2 = (1 + 3x^2y^2) \bmod 7$ (здесь $a = -1$ и $d = 3$ – неквадраты при $p = 7$) точки 4-го порядка имеют координаты $\boldsymbol{F_{2,3}} = (\pm 2, \pm 2)$. При удвоении согласно (3) получим $2\boldsymbol{F_2} = \left(\sqrt{\frac{a}{d}}, \infty\right) = \boldsymbol{D_1}$. Порядок N_E этой кривой, включающей точки $\mathbf{0}, \boldsymbol{D_{0,1,2}} \pm \boldsymbol{F_{2,3}}$, равен 8, группа точек нециклическая с типом $T = (2, 2^2)$.

Найдем условия существования точек 8-го порядка, порожденных делением на 2 точки $\boldsymbol{F_0}$.

Теорема 1.2. *Необходимыми условиями существования точек 8-го порядка кривой* (1) *являются*:

$$\text{i. При } \left(\frac{ad}{p}\right) = -1: \quad \left(\frac{a}{p}\right) = 1, \quad \left(\frac{1-\frac{d}{a}}{p}\right) = 1;$$

$$\text{ii. При } \left(\frac{ad}{p}\right) = 1: \quad \left(\frac{a}{p}\right) = 1, \quad \left(\frac{1-\frac{d}{a}}{p}\right) = 1 \text{ и } \left(\frac{1+\sqrt{1-\frac{d}{a}}}{p}\right) = 1.$$

Доказательство.

Пусть $\boldsymbol{S} = (x1, y1)$– точка 8-го порядка, тогда $2\boldsymbol{S_1} = \boldsymbol{F_0} = (0, 1/\sqrt{a})$ – точка 4-го порядка на оси y. Согласно (3) и координат $\boldsymbol{F_0}$ имеем

$$\frac{x_1^2 - ay_1^2}{(1 - dx_1^2y_1^2)} = 0, \qquad \frac{2x_1y_1}{(1 + dx_1^2y_1^2)} = \frac{1}{\sqrt{a}}.$$

Тогда $x_1^2 = ay_1^2$, $\Rightarrow$ $\frac{d}{a}x_1^4 - 2x_1^2 + 1 = 0$ $\Rightarrow x_{1,2}^2 = \frac{a}{d}\left(1 \pm \sqrt{1-\frac{d}{a}}\right)$.

Координаты точек S_k, $k = 1\ldots4$, или $k = 1\ldots8$ определяются из

$$\boldsymbol{S}_k = \left(\pm\left(\frac{a}{d}\left(1 \pm \sqrt{1-\frac{d}{a}}\right)\right)^{1/2}, \pm\left(\frac{1}{d}\left(1 \pm \sqrt{1-\frac{d}{a}}\right)\right)^{1/2}\right). \quad (7)$$

Так как справедливо

$$\left(1 + \sqrt{1-\frac{d}{a}}\right)\left(1 - \sqrt{1-\frac{d}{a}}\right) = \frac{d}{a}, \quad (8)$$

то при $\left(\frac{ad}{p}\right) = -1$ и $\left(\frac{1-\frac{d}{a}}{p}\right) = 1$, либо $\left(1 + \sqrt{1-\frac{d}{a}}\right)$ является квадратом, либо $\left(1 - \sqrt{1-\frac{d}{a}}\right)$.

Умножая неквадрат из этой альтернативы на неквадрат $\frac{a}{d}$, получим значение x_1^2 координаты одной из точек S_k. Извлекая из квадрата x_1^2 два корня, определяем значения координат $\pm x_1$ в (7). Учитывая условие $\left(\frac{a}{p}\right) = 1$ и разделив эти значения на $\sqrt{a}$, получим координаты $\pm y_1$точки 8-го порядка. Число точек 8-го порядка для данного случая равно 4. Первое из необходимых условий теоремы доказано.

При $\left(\frac{ad}{p}\right) = 1$ оба значения в скобках (8) есть квадраты или неквадраты. Так как сомножитель $\frac{a}{d}$ квадрата x_1^2 является квадратом, то вместе с условием $\left(\frac{1-\frac{d}{a}}{p}\right) = 1$ должно выполняться $\left(\frac{1+\sqrt{1-\frac{d}{a}}}{p}\right) = 1$, (и, соответственно, $\left(\frac{1-\sqrt{1-\frac{d}{a}}}{p}\right) = 1$). Тогда с учетом $\left(\frac{a}{p}\right) = 1$ получаем обе координаты 8-ми точек 8-го порядка (7). Увеличение вдвое числа точек связано с нециклической структурой точек четного порядка для этого случая. Итак, 8 точек 8-го порядка в условиях теоремы существуют. Теорема доказана.

Теорема 1.2 не исчерпывает всех возможных точек 8-го порядка, так как при $\left(\frac{ad}{p}\right) = 1$ возникают особые точки 4-го порядка (4), для которых деление на 2 может также породить точки 8-го порядка.

В приведенном выше примере кривой с$a = -1$и $d = 3$ при $p = 7$ оба параметра – неквадраты и нарушаются условия $\left(\frac{a}{p}\right) = 1$ и $\left(\frac{a-d}{p}\right) = -1$. Хотя порядок кривой равен 8, точек 8-го порядка она не содержит, так как группа точек нециклическая.

Теорема 1.3. *Необходимым и достаточным условием существования точек 8-го порядка полной кривой* Эдвардса $E_{E,1,d}$ *является* $\left(\frac{1-d}{p}\right) = 1$.

Доказательство.

Необходимость. Имеют место условия (i) теоремы 1.2 при $a = 1$. Из нее следует необходимое условие $\left(\frac{1-d}{p}\right) = 1$ существования точек 8-го порядка.

Достаточность. Пусть выполняется условие $\left(\frac{1-d}{p}\right) = 1$. В соответствии с (8) либо $\left(1 + \sqrt{1-d}\right)$, либо $\left(1 - \sqrt{1-d}\right)$ являются неквадратом, и, следовательно, его произведение с неквадратом d^{-1} дает квадрат. Значит, существует ровно 4 точки с координатами (7) 8-го порядка. Других точек 8-го порядка в этих условиях не существует. Теорема доказана.

Ранее в работе [6] одним из авторов настоящей работы было получено условие существования точек 8-го порядка для полной кривой Эдвардса.

При поиске кривых в форме Эдвардса с минимальным четным кофактором 4 порядка кривой следует исключать кривые, для которых выполняются условия теорем 1.2 или 1.3.

При условии существования особых точек (4) вместе с точками $\boldsymbol{D_0},\ \pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$, принимая правила предельного перехода в (2), можно найти координаты сумм:

$$(x_1, y_1) + (-1, 0) = (-x_1, -y_1),$$
$$(x_1, y_1) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}} \cdot x_1^{-1},\ \frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$
$$(x_1, y_1) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}} \cdot x_1^{-1}, -\frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$
$$(x_1, y_1) + \left(\infty, \frac{1}{\sqrt{d}}\right) = \left(-\frac{1}{\sqrt{d}} \cdot y_1^{-1},\ \frac{1}{\sqrt{d}} \cdot x_1^{-1}\right),$$
$$(x_1, y_1) + \left(\infty, -\frac{1}{\sqrt{d}}\right) = \left(\frac{1}{\sqrt{d}} \cdot y_1^{-1}, -\frac{1}{\sqrt{d}} \cdot x_1^{-1}\right).$$

Все найденные суммы удовлетворяют уравнению (1) при подстановке, то есть являются точками кривой. Сумма $(x_1, y_1) + D_0 = P^* = (-x_1, -y_1)$ меняет знаки координат точки P, тогда как сложение с особыми точками 2-го порядка инвертирует их с весами, сложение же с особыми точками 4-го порядка инвертирует с весами и меняет координаты местами.

Подчеркнем, что использование правил предельного перехода сохраняет операцию сложения любых пар точек, включая особые точки. Это позволяет говорить об изоморфизме кривых в различной форме, в частности, форме Монтгомери и Эдвардса.

2. Изоморфизм и пары кручения кривых в форме Монтгомери и форме Эдвардса

В пионерской работе [2] впервые введено понятие скрученной кривой Эдвардса. В ней, как нам представляется, имеются некорректные утверждения и результаты, которые мы выносим на обсуждение. Основные теоремы в работе [2] опираются на бирациональную эквивалентность между кривыми (1) и кривыми в форме Монтгомери, заданными уравнением:

$$\mathrm{E_{M,A,B}}:\ Bv^2 = u^3 + \mathrm{A}u^2 + u,\ A = 2\frac{a+d}{a-d},\ B = \frac{4}{a-d},\ a = \frac{A+2}{B}, d = \frac{A-2}{B}, \mathrm{A}^2 \neq 4. \quad (9)$$

Она основана на замене координат с помощью рациональных функций:

$$y = \frac{u}{v},\ x = \frac{u-1}{u+1} \Rightarrow u = \frac{1+x}{1-x},\quad v = \frac{u}{x}. \quad (10)$$

В работе [2] доказывается теорема 3.2: *любая скрученная кривая Эдвардса* (1) *бирационально эквивалентна кривой* (9) *в форме Монтгомери*.

Так как нам придется обращаться к паре квадратичного кручения (quadratic twist в [2]), мы также проведем отображение точек (9) в точки кривой (1) .

Разделим (9) на v^2 и с учетом (10) получим:

$$\frac{4}{(a-d)}\frac{1}{y^2} = u + u^{-1} + 2\frac{a+d}{a-d},\quad \Rightarrow \frac{2}{(a-d)}\frac{1}{y^2} = \frac{1+x^2}{1-x^2} + \frac{a+d}{a-d}.$$

Отсюда

$$\frac{2(1-x^2)}{y^2} = (1+x^2)(a-d) + (1-x^2)(a+d),$$

и, наконец, получаем изоморфную кривой (9) кривую в форме (1):

$$E_{M,A,B} \sim E_{E,a,d}:\ (1-x^2) = y^2(a-dx^2)$$

Нетрудно с помощью (10) осуществить и обратное преобразование. Имеет место взаимно однозначное отображение точек $(u_1, v_1) \leftrightarrow (x_1, y_1)$. Если для любой пары точек принять операцию сложения (2) с включением особых точек (см. раздел 1), то можно утверждать, что кривые $E_{M,A,B}$ и $E_{E,a,d}$ изоморфны. Этот изоморфизм сохраняет порядки всех точек.

Перейдем теперь к парам квадратичного кручения. Пусть $\left(\frac{c}{p}\right) = -1$, тогда кривая кручения для кривой (9) в форме Монтгомери имеет вид:

$$E^t_{M,A,B} \sim E_{M,A\,cB}:\ \ cBv^2 = u^3 + \mathrm{A}u^2 + u,\ A = 2\frac{a+d}{a-d},\ B = \frac{4}{a-d}$$

Изоморфная ей кривая в обобщенной форме Эдвардса (1), как можно видеть из выполненных выше преобразований, записывается как:

$$E^{t}_{E,a,d} \sim E_{E,ca,cd}: (1 - x^2) = cy^2(a - dx^2) = y^2(ca - cdx^2)\,. \qquad (11)$$

Иначе говоря, для построения пары квадратичного кручения к кривой в форме (1) необходимо перейти к новым параметрам кривой (11) в форме Эдвардса $a' = ca,\ d' = cd$, то есть квадраты обращаются в неквадраты и наоборот.

Чтобы классифицировать кривые в обобщенной форме Эдвардса с разбиением на непересекающиеся классы, рассмотрим всевозможные сочетания для пар параметров a и d кривой (1).

П.1. $\left(\frac{ad}{p}\right) = -1.$

П.1.1. $\left(\frac{a}{p}\right) = 1,\ \left(\frac{d}{p}\right) = -1.$

Согласно (1) и (2) в этом случае на кривой (1) имеется единственная точка $\boldsymbol{D_0} = (-1, 0)$ 2-го порядка и 2 точки 4-го порядка $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$. В соответствии с (10) им отвечают точки кривой Монтгомери (9) $D_{\mathrm{M}0} = (0, 0)$ и $\pm F_{\mathrm{M}0} = (1, \pm\sqrt{a})$. Этот случай определен в работе [1]. Здесь заменой $(x, y) \to (X, Y/\sqrt{a})$получаем изоморфную кривой (1) полную кривую Эдвардса $X^2 + Y^2 = 1 + d'X^2Y^2\,, d' = d/a \Rightarrow \left(\frac{d'}{p}\right) = -1.$ Итак, для этого случая имеет место изоморфизм $E_{E,a,d} \sim E_{E,1,d/a}$.

П.1.2. $\left(\frac{a}{p}\right) = -1,\ \left(\frac{d}{p}\right) = 1.$

Здесь также нет особенностей, так как параметры a и d просто меняются местами. С помощью замены $(x, y) \to (\frac{1}{X}\,, Y)$ получим изоморфную кривую $X^2 + dY^2 = 1 + aX^2Y^2$. Ее квадратичное кручение образуется смещением параметров $d' = cd,\ a' = ca,\ \left(\frac{c}{p}\right) = -1,$ при этом попадаем в условия П.1.1. Далее аналогично строим изоморфную кривую Эдвардса $\bar{x}^2 + \bar{y}^2 = 1 + \left(\frac{a}{d}\right)\bar{x}^2\bar{y}^2$. Таким образом, пара кривых $E^{t}_{E,1,d/a} \sim E_{E,1,a/d}$ образуют пару квадратичного кручения. Этот результат известен [1].

Итак, рассмотренные в П.1 условия для a и d порождают класс изоморфизмов полных кривых Эдвардса, и каждая кривая в условиях П.1.1 заменой $d \to d^{-1}$ отображается в кривую квадратичного кручения П.2.2 и обратно.

П.2. $\left(\frac{ad}{p}\right) = 1.$

Именно этот случай образует новые классы скрученных кривых Эдвардса и кривых Эдвардса с квадратичным параметром. Как мы показали, квадратичное кручение образуется смещением параметров $d' = cd,\ a' = ca$, где c – неквадрат. Поэтому кривые в П.2.1. и П.2.2. образуют пару квадратичного кручения, то есть $E^{t}_{E,a,d} \sim E_{E,ca,cd}$. Свойства одной из кривых пары кручения полезны для определения свойств другой.

П.2.1. $\left(\frac{a}{p}\right) = -1,\ \left(\frac{d}{p}\right) = -1.$

Согласно (9) имеем $(Bad)^2 = (A + 2)(A - 2)$ и, следовательно, дискриминант квадратного уравнения в правой части (9) $(A^2 - 4)$ является квадратом. Тогда кубическое уравнение $u^3 + Au^2 + u = 0$ имеет 3 корня в поле F_p: $\{0, -(\mathrm{A} \pm \sqrt{A^2 - 4})/2\}$, а кривая Монтгомери содержит 3 точки 2-го порядка: $D_{\mathrm{M}0} = (0, 0), D_{\mathrm{M}1,2} = (-\frac{\mathrm{A} \pm \sqrt{A^2 - 4}}{2}, 0)$, с координатами $v_{0,1,2} = 0$. Преобразованием координат (10) точка $D_{\mathrm{M}0}$ кривой (9) переходит в точку $\boldsymbol{D_0} = (-1, 0)$ кривой (1), а две другие точки $D_{\mathrm{M}1,2}$ отображаются в 2 точки 2-го порядка $\boldsymbol{D_{1,2}} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$

с делением на 0 y-координаты $y = u/v$. Так как при $x = 0$ из (1) следует $ay^2 = 1$, решения для y-координаты нет и точки 4-го порядка на оси y для этого случая не существуют. Согласно (6), точки 4-го порядка кривая (1) имеет при выполнении условий $\left(\frac{ad}{p}\right) = 1$ и p≡ 3mod4. Итак, данный случай характерен наличием 3-х точек 2-го порядка (из них две точки – особые) и наличием точек 4-го порядка лишь при$p \equiv 3mod4$. Заметим, что в данном случае изоморфизм на основе замены $(x, y) \to (X, Y/\sqrt{a})$ (см. П.1.1) построить нельзя из-за несуществования элемента $\sqrt{a}$. В то же время для кривой квадратичного кручения (П.2.2) такой изоморфизм существует.

П.2.2.$\left(\frac{a}{p}\right) = 1,\ \left(\frac{d}{p}\right) = 1.$

Как и в предыдущем случае, при $v = 0$ дискриминант уравнения (9) $(A^2 - 4) = (Bad)^2$ является квадратом и имеются 3 точки 2-го порядка с теми же координатами, что и в П.2.1. Две из них преобразованием (10) переходят в особые точки 2-го порядка $\boldsymbol{D_{1,2}} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ кривой Эдвардса с квадратичным параметром. В отличие от П.2.1, здесь всегда имеются точки 4-го порядка, в частности, точки $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$ на оси y кривой (1). Кроме того, кривая Монтгомери (9) содержит 2 точки 4-го порядка с координатой $u_1 = -1$, которые отображением (10) порождают особые точки кривой Эдвардса (1). Действительно, из уравнения касательной к кривой (3) в точке 4-го порядка $P_{\text{M}} = (u_1, v_1)$, проходящей через точку (0,0) 2-го порядка, имеем:

$$\frac{dv}{du}\Big|_{\text{u=u}_1} = \frac{3u_1^2 + 2Au_1 + 1}{2Bv_1} = \frac{v_1}{u_1}.$$

Тогда с учетом (9) получим $u_1^2 = 1 \Rightarrow u_1 = \pm 1$. Одна из пар точек 4-го порядка имеет координаты $\pm F_M = \left(-1,\ \pm\sqrt{\frac{A-2}{B}}\right)$. Как следует из (10), эти 2 точки кривой Монтгомери с координатой $u_1 = -1$ преобразуются в особые точки 4-го порядка $\pm\boldsymbol{F_1} = \left(\infty,\ \pm\frac{1}{\sqrt{d}}\right)$ кривой (1). В итоге в рассматриваемом случае получаем 4 особые точки (на бесконечности): по 2 точки 2-го и 4-го порядков. Для данного случая преобразование координат $(x, y) \to \left(\frac{X}{\sqrt{a}}, Y\right)$ дает изоморфную кривой (1) кривую Эдвардса с квадратичным параметром $X^2 + Y^2 = 1 + d'X^2Y^2$, где $d' = \frac{d}{a} \Rightarrow \left(\frac{d'}{p}\right) = 1$ и имеет место класс изоморфизмов $E_{E,a,d} \sim E_{E,1,d/a}$. Кривые этого пункта мы относим к кривым Эдвардса с квадратичным параметром.

Как мы отмечали, для всех кривых П.2 при обращении параметров $\left(\frac{a}{d}\right) \to \left(\frac{d}{a}\right)$ имеет место изоморфизм $E_{E,a,d} \sim E_{E,d,a}$. Это следует из квадратичности $\left(\frac{ad}{p}\right) = 1$.

На основе свойств кривых П.1 и П.2 мы разбиваем все кривые в форме Эдвардса на 3 непересекающиеся класса изоморфизмов:

- *полные кривые Эдвардса* (с условиями П.1: $\left(\frac{ad}{p}\right) = -1$;
- *скрученные кривые Эдвардса* (с условиями П.2.1:$\left(\frac{a}{p}\right) = -1.\ \left(\frac{d}{p}\right) = -1$;
- *кривые Эдвардса с квадратичным параметром* (с условиями П.2.2:$\left(\frac{a}{p}\right) = 1.\left(\frac{d}{p}\right) = 1.$);

Далее мы опираемся на нашу терминологию.

В работе [3] доказано (теорема 3.3), что закон сложения для кривых Эдвардса является полным, т.е при любых входах знаменатели в (2) $1 + dx_1x_2y_1y_2 \neq 0,\ 1 - dx_1x_2y_1y_2 \neq 0,$ если параметр d есть квадратичный невычет: $\left(\frac{d}{p}\right) = -1$. Очевидно, что для кривых Эдвардса

с квадратичным параметром нарушается полнота закона сложения, так как для них $\left(\frac{d}{p}\right) = 1$. Для скрученных кривых Эдвардса с $\left(\frac{d}{p}\right) = -1$ также существуют точки четного порядка, для которых возможны особенности с $1 \pm dx_1x_2y_1y_2 = 0$. Например, для приведенных в разделе 1 сумм точек, включающих особые точки 2-го и 4-го порядков, можем принять $x_2 = \sqrt{\frac{a}{d}} \cdot x_1^{-1}$, $y_2 = \frac{1}{\sqrt{ad}} \cdot y_1^{-1}$,тогда$1 - dx_1x_2y_1y_2 = 0$. В то же время для точек нечетного порядка полнота закона сложения точек выполняется.

Для криптографических приложений следует искать кривые Эдвардса порядка $N_E = 4n$ с минимальным кофактором 4 при нечетном n, из которых отбираются кривые с простым n. Среди полных кривых Эдвардса (условия П.1) практически половина имеют порядок $4n$ (n – нечетное). Они являются циклическими, и их порядки пробегают все кратные 4-м числа в границах Хассе. Кривые Эдвардса с квадратичным параметром d (П.2.2.) являются нециклическими с тремя точками 2-го порядка и четырьмя точками 4-го порядка. Отсюда следует, что они содержат нециклическую подгруппу, изоморфную $Z/2 \times Z/4$ порядка 8, а порядок этих кривых имеет минимальный кофактор 8. Поэтому кривые порядка $N_E = 4n$ наряду с полными кривыми Эдвардса можно искать лишь среди скрученных кривых в условиях П.2.1.

При $p \equiv 1mod4$ получим $N_E + N_E^t = 2(p+1) = 2(4k+1+1) \equiv 0\mathrm{mod}4$, т.е. с учетом $N_E \equiv 0\mathrm{mod}8$ для скрученной кривой Эдвардса порядок $N_E^t \equiv 0\mathrm{mod}4$. Ясно, что в этом случае она имеет 3 точки 2-го порядка и не имеет точек 4-го порядка. Это подтверждается условием (6) теоремы 1.1. Конечно, при этом нет изоморфизма скрученной кривой Эдвардса с кривой $E_{E,1,d}$, имеющей точки 4-го порядка (теорема 3.5 [2]). Итак, скрученные кривые Эдвардса с минимальным кофактором порядка $N_E = 4n$ существуют лишь для половины возможных значений модуля$p \equiv 1\mathrm{mod}4$.

3. Несуществование кривых в обобщенной форме Эдвардса порядка *2n*

Кривая Монтгомери, заданная уравнением (9), имеет точки 4-го порядка всегда, кроме случая П.2.1 для класса скрученных кривых при $p \equiv 1\mathrm{mod}4$. Однако и в этом случае ее порядок $N_E = 4n$ из-за наличия 3-х точек 2-го порядка. Кривая в форме Монтгомери может иметь одну точку 2-го порядка и не иметь точек 4-го порядка, тогда ее порядок равен $N_E = 2n$. Можно ли построить изоморфную ей кривую обобщенной форме Эдвардса?

Найдем параметры обобщенной кривой (9) при одной точке второго порядка и отсутствии точек 4-го порядка. Введем в форму (9) Монтгомери новый параметр C кривой и запишем более общее уравнение:

$$E_{M,A,B,C}: \quad Bv^2 = u^3 + \mathrm{A}u^2 + Cu, \quad A = 2\frac{a+d}{a-d},\ B = \frac{4}{a-d}. \tag{12}$$

Необходимыми и достаточными условиями единственности точки 2-го порядка $D_{\mathrm{M}0} = (0,0)$ и отсутствия точек 4-го порядка являются [7]:

$$\text{(i)} \quad \left(\frac{A^2-4C}{p}\right) = -1, \qquad \text{(ii)} \quad \left(\frac{C}{p}\right) = -1, \tag{13}$$

Первое условие связано с неквадратичностью дискриминанта квадратного уравнения в (12), а второе – с решением $u_1^2 = \mathrm{C}$ для координаты точки 4-го порядка. При выполнении (13) порядок кривой (12) равен $2n$. Существует ли в этом случае изоморфизм этой кривой с кривой в обобщенной форме Эдвардса?

Уравнение (12) можно переписать как:

$$Bv^2 = \sqrt{\mathrm{C}}\left(\left(\sqrt{\mathrm{C}}\right)^{-1}u^3 + Au^2 + \sqrt{\mathrm{C}}\,u\right),$$

или

$$B\frac{v^2}{u^2} = \sqrt{\mathrm{C}}\left(\left(\sqrt{\mathrm{C}}\right)^{-1}u + \sqrt{\mathrm{C}}\,u^{-1}\right) + A.$$

Принимая теперь вместо (10) $\left(\sqrt{\mathrm{C}}\right)^{-1}u = U = \frac{1+x}{1-x}$, получим

$$B\frac{v^2}{CU^2} = 2\sqrt{\mathrm{C}}\left(\frac{1+x^2}{1-x^2}\right) + A.$$

С учетом этого равенства можно теперь принять взамен (9) и (10)

$$A = 2\sqrt{\mathrm{C}}\,\frac{a+d}{a-d}, \qquad y = \frac{v}{\sqrt{\mathrm{C}}\,U}.$$

Аналогично преобразованиям в разделе 2 можно получить уравнение

$$(1 - x^2) = \sqrt{\mathrm{C}}\,y^2(a - dx^2).$$

Это уравнение отличается от кривой в обобщенной форме Эдвардса (1) лишь сомножителем $\sqrt{\mathrm{C}}$ в правой части. Очевидно, что с учетом условия (13i) оно не имеет решений в поле F_p, кроме одной точки $\mathrm{O} = (1, 0)$. К примеру, возводя в квадрат обе части уравнения, получим в левой части квадрат, а в правой – неквадрат. Итак, в условиях (13) не существует изоморфизм между кривой в форме Монтгомери (12) и кривой (1) в обобщенной форме Эдвардса.

Заключение

Кривые с минимальным четным кофактором 4 порядка $4n$ составляют половину всех полных кривых Эдвардса и весь класс скрученных кривых Эдвардса при $p \equiv 1 \bmod 4$. Для криптосистем из них отбираются кривые с простым n.

Литература

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

2. BernsteinDaniel J. , BirknerPeter, JoyeMarc, LangeTanja, 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, PP. 1-17.

3. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

4. 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.103-109.

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

6. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

7. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. Кибернетика и системныйанализ, т.51, №2, 2015. С.3-12.

Надійшла 10.05.2016 р. Рецензент: д.т.н., проф. Барабаш О.В.