УДК 621.391.15 : 519.7

А.В.Бессалов, О.В.Цыганкова

ЧИСЛО КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА С МИНИМАЛЬНЫМ ЧЕТНЫМ КОФАКТОРОМ ПОРЯДКА КРИВОЙ

Дан анализ свойств точек порядков 2, 4, 8 кривой в обобщенной форме Эдвардса. Введена арифметика для групповых операций с особыми точками этих кривых. Предложена классификация кривых в форме Эдвардса на 3 непересекающихся класса. Получены формулы для числа кривых разных классов порядка $4n$. Дан критический анализ результатов работ других авторов.

Ключевые слова: кривая в обобщенной форме Эдвардса, скрученная кривая Эдвардса, параметры кривой, порядок точки, сложение точек, изоморфизм, квадратичное кручение, квадратичный вычет, квадратичный невычет .

§1.Введение

Эллиптические кривые в форме Эдвардса [1] над простым полем, без сомнения, перспективны в современной криптографии. Как мы показали в работе [2], скорость выполнения групповых операций для них в среднем не менее чем в 1.5 раза выше, чем для кривых в форме Вейерштрасса. При троичном NAF(k) представлении числа k точки kP выигрыш в скорости вычислений достигает 1.6 раза. Арифметика этих кривых проще в связи с наличием нейтрального элемента группы как неособой точки кривой (1,0). Исключая изоморфные кривые, в кривых Эдвардса достаточно использовать один параметр d вместо обычных двух параметров a и b кривой форме Вейерштрасса.

Авторы работы [3] обобщили и расширили класс кривых Эдвардса [4] 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 [4] – полными кривыми Эдвардса. В работе [3] был дан анализ некоторых свойств этих кривых, сделана попытка дать классификацию кривых в форме Эдвардса и привести статистику распределения порядков кривых, относящихся к разным классам этих кривых при небольших значениях модуля p = 1009 и p = 1019. Мы обнаружили, что кривые в обобщенной 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. Это 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 получаем формулы для числа таких кривых с порядком $4n$. В **§2** вводится арифметика для групповых операций с особыми точками этих кривых, дан анализ точек малых порядков и формулы, связывающие их с другими точками кривой. В **§3** обсуждается некорректность ряла утверждений, классификации кривых и статистики их порядков в [3], предложена классификация кривых в обобщенной форме Эдвардса с разбиением на три непересекающиеся класса в зависимости от квадратичности параметров a и d кривой. Дан анализ свойств кривых всех 3-х классов и возможных значений порядков этих кривых. В **§4** получены точные формулы для числа кривых различных классов с минимальным кофактором 4 порядка кривой и дан критический анализ результатов, приведенных в [3].

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

В работе [3] *скрученные кривые Эдвардса* (twisted Edwards curves) определены как обобщение кривых Эдвардса $x^2 + y^2 = 1 + dx^2y^2$ [4] введением нового параметра a в уравнение

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

Наряду с вводом параметра a авторы [3] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{ad}{p}\right) = \pm 1$. При $a = 1$ такая кривая получила в [3] название *кривой Эдвардса*, а если у нее d – квадратичный невычет (т.е. $\left(\frac{d}{p}\right) = -1$), то – *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [4]. В работе [5] 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

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

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

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

Использование модифицированных законов (2), (3) позволяет сохранить общепринятую горизонтальную симметрию (относительно оси x) обратных точек. Определяя теперь обратную точку как $-P = (x_1, -y_1)$, получим согласно (1) $(x_1, y_1) + (x_1, -y_1) = (1, 0) = \mathbf{O}$. Кроме нейтрального элемента **O** на оси x также всегда лежит точка $\boldsymbol{D_0} = (-1, 0)$ второго порядка, для которой в соответствии с (3) $2\boldsymbol{D_0} = (1, 0) = \mathbf{O}$. 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 (квадратичным вычетом).

Из уравнения (1) определим квадраты:

$$x^2 = \frac{1 - a y^2}{1 - d y^2}, \qquad y^2 = \frac{1 - x^2}{a - d x^2},$$

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 не особые при ненулевых координатах x и y.

Т е о р е м а 1. *Точки 4-го порядка скрученной кривой в форме* (1) *при* $x \neq 0$ *существуют тогда и только тогда, когда выполняются условия*:

$$\text{(i)} \quad \left(\frac{a}{p}\right) = -1, \ \left(\frac{d}{p}\right) = -1\,, \quad \text{(ii)} \qquad p \equiv 3 mod 4.$$

Д о к а з а т е л ь с т в о. Необходимость. Особых точек $\pm\boldsymbol{F_1} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ из (4) кривая не содержит, так как не существует $\sqrt{d}$. Нет также точек при $x = 0$. Положим $2\boldsymbol{F_2} = 2(x_1, y_1) = \boldsymbol{D_1}$. Тогда согласно (3) и (4) запишем два уравнения

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

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

$$\frac{2x_1^2}{1+\frac{d}{a}x_1^4} = \sqrt{\frac{a}{d}} \quad \Rightarrow\ dx_1^4 - 2\sqrt{ad}\,x_1^2 + a = 0 \quad \Rightarrow \quad x_1^2 = \sqrt{\frac{a}{d}},\ \ y_1^2 = -\frac{1}{\sqrt{ad}}\ .$$

Итак, получаем 4 точки с координатами:

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

Необходимыми условиями существования таких точек являются условия (i) и (ii) теоремы. Действительно, при $\left(\frac{a}{p}\right) = -1$ равенство $x_1^2 = -ay_1^2$ справедливо лишь при $p \equiv 3 mod 4$, так как в этом случае элемент (-1) есть квадратичный невычет [6], тогда $(-a)$ – квадратичный вычет. Кроме того, если β – примитивный элемент мультипликативной группы F_p^*, и β^2 – квадрат этой группы, то при условии (ii) имеем $\beta^2\beta^{p-1} = \beta^{2\,+\,4k\,+\,2} = \beta^{4(k+1)}$. Значит, любой квадрат имеет квадратные корни и корни 4-й степени при $p \equiv 3 mod$. Существование первых координат в (5) с учетом условий (i) доказано. Учитывая условия (i) и принимая значение $\left(\frac{-\sqrt{ad}}{p}\right) = 1$ (т.е. как квадратичного вычета, при этом $\sqrt{ad}$ – квадратичный невычет), 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 теоремы существуют. Необходимость условий теоремы доказана.

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

Точки $\pm\boldsymbol{F_{2,3}}$ можно рассматривать как точки деления на два точек 2-го порядка $\boldsymbol{D_{1,2}}/2$ [5].

Например, для кривой $x^2 - y^2 = (1 + 3x^2y^2)\,\mathrm{mod}7$ (здесь $a = -1$ и $d = 3$ – квадратичные невычеты 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 $\mathbf{O}$, $\boldsymbol{D_{0,1,2}}$, $\pm\boldsymbol{F_{2,3}}$, равен 8, группа точек нециклическая с типом $T = (2, 2^2)$.

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

Т е о р е м а 2. *Необходимыми условиями существования точек 8-го порядка кривой* (1) *являются:*

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

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

Д о к а з а т е л ь с т в о. Пусть **S** = (x_1, y_1) – 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

$$\frac{x_1^2-ay_1^2}{(1-dx_1^2y_1^2)} = 0\,, \qquad \frac{2x_1y_1}{(1+dx_1^2y_1^2)} = \frac{1}{\sqrt{a}}\,. \qquad (6)$$

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

Координаты точек S_k, k = 1..4, или k = 1..8 определяются из

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

Так как справедливо

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

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 квадратичный невычет из этой альтернативы на невычет $\frac{a}{d}$, получим значение x_1^2 координаты одной из точек S_k. Извлекая из квадрата x_1^2 два корня, определяем значения координат ± x_1 в (7). Учитывая условие $\left(\frac{a}{p}\right) = 1$ и разделив эти значения на $\sqrt{a}$, получим координаты ± 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 квадратичные вычеты или невычеты. 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 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 – квадратичные невычеты 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.

Т е о р е м а 3. *Необходимым и достаточным условием существования точек 8-го порядка полной кривой* Эдвардса $E_{E,1,d}$ *является* $\left(\frac{1-d}{p}\right) = 1$.

Д о к а з а т е л ь с т в о. Необходимость. Имеют место условия (i) теоремы 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 $\left(1 - \sqrt{1-d}\right)$ является квадратичным невычетом, и, следовательно, его произведение с 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. ▲

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, т.е. являются точками кривой.

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

§3. Классификация кривых в обобщенной форме Эдвардса

В пионерской работе [3] впервые введено понятие скрученной кривой Эдвардса. Нам представляется, в ней имеются некорректные утверждения и результаты, которые мы ниже обсуждаем. Основные теоремы в работе [3] опираются на бирациональную эквивалентность между кривыми (1) и кривыми в форме Монтгомери

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

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 [3] доказана 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 [3]), мы также проведем отображение точек (9) в точки кривой (1) .

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

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

Отсюда

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

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

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

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.**§2**), то можно утверждать, что кривые $E_{M,A,B}$ и $E_{Ea,d}$ изоморфны.

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

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

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

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

Иначе говоря, для построения пары квадратичного кручения к кривой в форме (1) переходим к новым параметрам кривой (11) в форме Эдвардса $a' = ca, d' = cd$, т.е. квадратичные вычеты обращаются в невычеты и обратно.

Во 2-м разделе работы [3] утверждается, что кривая $E_{E,1,d/a}$ есть пара квадратичного кручения (quadratic twist) кривой $E_{E,a,d}$, т.е. $E^t_{E,a,d} \sim E_{E,1,d/a}$. Видимо, следует признать это утверждение в общем случае некорректным. Как следует из нашего анализа, оно справедливо лишь при $\left(\frac{a}{p}\right) = -1$, если принять $c = a^{-1}$. При $\left(\frac{a}{p}\right) = 1$ кривые $E_{E,a,d}$ и $E_{E,1,d/a}$ изоморфны. Здесь же авторы [3] заключают, что кривая $E_{E,1,d}$ есть квадратичное кручение кривой $E_{E,1,1/d}$, ссылаясь на известный факт из [4]. Но в [4] это справедливо в условиях $\left(\frac{d}{p}\right) = -1$, тогда как в [3] допускается $\left(\frac{d}{p}\right) = 1$, и тогда эта пара кривых изоморфна: $E_{E,1,d} \sim E_{E,1,1/d}$. Действительно, заменив $d \to d^{-1}$ в уравнении (9), получим изоморфную кривую при условии $\left(\frac{d}{p}\right) = 1$.

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

$C1$: $\left(\frac{ad}{p}\right) = -1$.

$C1.1$: $\left(\frac{a}{p}\right) = 1$, $\left(\frac{d}{p}\right) = -1$. 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) $D_{M0} = (0,0)$ и $\pm F_{M0} = (1, \pm\sqrt{a})$. Этот случай определен в работе [4]. 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 $E_{E,a,d} \sim E_{E,1,d/a}$.

$C1.2$: $\left(\frac{a}{p}\right) = -1$, $\left(\frac{d}{p}\right) = 1$. Здесь параметры a и d просто меняются местами. С помощью замены $(x,y) \to (1/X, Y)$ получим изоморфную кривую $X^2 + dY^2 = 1 + aX^2Y^2$. Ее квадратичное кручение образуется заменой $d' = cd$, $a' = ca$, $\left(\frac{c}{p}\right) = -1$, при этом попадаем в условия $C1.1$. 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 [4].

Итак, рассмотренные в $C1$ условия для a и d порождают класс изоморфизмов *полных кривых Эдвардса*, и каждая кривая в условиях C1.1 заменой $d \to d^{-1}$ отображается в кривую квадратичного кручения C1.2 и обратно.

C2: $\left(\frac{ad}{p}\right) = 1$.

C2.1: $\left(\frac{a}{p}\right) = -1$, $\left(\frac{d}{p}\right) = -1$. Согласно (9) имеем $(Bad)^2 = (A + 2)(A - 2)$ и, следовательно, дискриминант квадратного уравнения в правой части (9) $(A^2 - 4)$ является квадратом. Тогда уравнение $u^3 + Au^2 + u = 0$ имеет 3 корня в поле F_p: $\{0, -(A \pm \sqrt{A^2 - 4})/2\}$, а кривая Монтгомери содержит 3 точки 2-го порядка: $D_{M0} = (0,0)$, $D_{M1,2} = (-(A \pm \sqrt{A^2 - 4})/2, 0)$. Преобразованием координат (10) точка D_{M0} кривой (9) переходит в точку $\boldsymbol{D_0} = (-1, 0)$ кривой (1), а две другие точки $D_{M1,2}$ 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 $y = u/v$. Точки 4-го порядка $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$ на оси y для этого случая не существуют. Согласно теоремы 1, кривая (1) имеет точки 4-го порядка (5) лишь при $p \equiv 3 \bmod 4$. На основе замены $(x,y) \rightarrow (1/X, Y)$ и умножения на X^2 получаем изоморфизм $E_{E,a,d} \sim E_{E,d,a}$.

$C2.2$: $\left(\frac{a}{p}\right) = 1$, $\left(\frac{d}{p}\right) = 1$. Как и в предыдущем случае, имеются 3 точки 2-го порядка с теми же координатами, что и в C2.1. Кроме того, имеются точки 4-го порядка $\pm\boldsymbol{F_0} = (0, \pm 1/\sqrt{a})$ на оси y кривой (1). Вместе с тем возникают особые точки 4-го порядка (4) $\pm\boldsymbol{F_1} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$. Для данного случая преобразование координат $(x,y) \rightarrow (\frac{X}{\sqrt{a}}, ,Y)$ дает изоморфную кривой (1) кривую $X^2 + Y^2 = 1 + d'X^2Y^2$, где $d' = d/a$ и имеет место изоморфизм $E_{E,a,d} \sim E_{E,1,d/a}$.

Очевидно, что кривые в C2.1. и C2.2. образуют пару квадратичного кручения, т.е. $E^t_{E,a,d} \sim E_{E,ca,cd}$.

Итак, мы разбиваем все кривые в обобщенной форме Эдвардса (1) на 3 непересекающиеся класса изоморфизмов:

- *полные кривые Эдвардса* (с условиями C1: $\left(\frac{ad}{p}\right) = -1$;
- *скрученные кривые Эдвардса* (с условиями C2.1: $\left(\frac{a}{p}\right) = -1$. $\left(\frac{d}{p}\right) = -1$;
- *квадратичные кривые Эдвардса* (с условиями C2.2: $\left(\frac{a}{p}\right) = 1$. $\left(\frac{d}{p}\right) = 1$.).

Обратимся к классификации кривых в форме Эдвардса, данной в работе [3]. Кривая Эдвардса в этой работе определена как $E_{E,1,d}$ без ограничений на параметр d. По нашей классификации это объединяет два класса: полных кривых Эдвардса и кривых Эдвардса с квадратичным параметром. Между тем в статистические таблицы порядков кривых в разделе 4 [3 вошли классы кривых Эдвардса (Edwards), полных кривых Эдвардса (complete Edwards), скрученных кривых Эдвардса (twisted Edwards). Но последние в [3] определены как кривые в обобщенной форме Эдвардса (1) (по нашей терминологии) и, следовательно, включают все другие классы. Трудно понять,

как с такой классификацией можно строить таблицы распределения числа кривых, входящих в разные классы. Предлагаемая нами классификация кривых в обобщенной форме Эдвардса с разбиением их на непересекающиеся классы является логичной и однозначной. Далее мы опираемся на нашу классификацию.

В работе [4] 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 × 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.

В работе [2] доказаны теоремы 3.3 – 3.5. о бирациональной эквивалентности кривых Эдвардса и Монтгомери В теореме 3.3 [3] доказано, что кривые Эдвардса $E_{E,1,d}$ и Монтгомери $E_{M,A,B}$ бирационально эквивалентны лишь при наличии в них точек 4-го порядка. Далее в теореме 3.4 доказана бирациональная эквивалентность этих кривых и наличие в них точек 4-го порядка при $p \equiv 3 \bmod 4$. В частности, для скрученных кривых Эдвардса (с условиями п.2.1) порядок кривой $N^t_E \equiv 0 \bmod 8$. Действительно, для нее парой квадратичного кручения является кривая с условием П.2.2,имеющая подгруппы 8-го порядка. Следовательно, ее порядок $N_E \equiv 0 \bmod 8$. Тогда сумма числа точек

пары кривых кручения при $p \equiv 3\mathrm{mod}4$ равна $N_E + N^t_E = 2(p+1) = 2(4k+3+1) \equiv 0\mathrm{mod}8$. Отсюда следует $N^t_E \equiv 0\mathrm{mod}8$.

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

§4. Число кривых в обобщенной форме Эдвардса порядка 4*n*

Изучив свойства кривых в обобщенной форме Эдвардса, нет смысла изучать статистику порядков этих кривых, как это сделано в [3]. На основе нашей классификации в **§3**, и свойств кривых, мы можем найти точное число этих кривых с минимальным четным кофактором 4 порядка $4n$ кривой (n – нечетное). Для этого рассмотрим 2 случая.

A. $p \equiv 1\mathrm{mod}4$.

Для полных кривых Эдвардса с условием П.1 число всех кривых равно числу квадратичных невычетов [6] $(p-1)/2$. Так как для пары квадратичного кручения справедливо $N_E + N^t_E = 2(p+1) \equiv 0\mathrm{mod}4$, то из $N_E = p + 1 - t \equiv 0\mathrm{mod}4$ и $p + 1 \equiv 2\mathrm{mod}4$ имеем $\pm t \equiv 2\mathrm{mod}4$. При этом $N^t_E \equiv 0\mathrm{mod}8$. Итак, если порядок одной из кривых имеет минимальный кофактор 4, то порядок кривой кручения имеет минимальный кофактор 8 и наоборот. Поскольку каждой кривой отвечает одна кривая кручения с инверсией $d \to d^{-1}$, то число полных кривых Эдвардса с минимальным кофактором $M_{A1} = M_{1.1} + M_{1.2} = (p-1)/4$. Злесь обозначены $M_{i.k}$ – число кривых в классах с условиями П.i.k раздела 2.

Для кривых с условиями П.2 классификации кривые Эдвардса с квадратичным параметром (условия П.2.2) строятся с помощью квадратов $\left(\frac{d}{a}\right)$, из которых выбрасываются квадраты 1 и – 1, так что остается $(p-5)/2$ квадратичных вычетов. Так как инверсия $\left(\frac{a}{d}\right) \to \left(\frac{d}{a}\right)$ дает изоморфную кривую, мы отбрасываем половину значений квадратов и получаем число кривых с минимальным кофактором 8 $M_{2.2} = (p-5)/4$. Переход к скрученным кривым Эдвардса с минимальным кофактором 4 как квадратичному кручению кривых п.2.2 дает то же число кривых $M_{2.1} = (p-5)/4$. Все скрученные кривые Эдвардса при $p \equiv 1\mathrm{mod}4$ имеют минимальный кофактор 4 порядка кривой. Таким образом, в условиях П.2 число кривых с порядком $4n$ равно $M_{A2} = (p-5)/4$.

Общее число кривых в форме (1) порядка $4n$ при $p \equiv 1\mathrm{mod}4$ равно $M_A = (p - 3)/2$.

B. $p \equiv 3\mathrm{mod}4$.

Для этого случая кривые (1) порядка $4n$ существуют лишь в классе полных кривых Эдвардса (условия П.1). Любая кривая при этом содержит ровно 2 точки 4-го порядка и половина кривых – 4 точки 8-го порядка. Из $(p - 1)/2$ квадратичных невычетов d мультипликативной группы F_p^* в соответствии с условием теоремы 3 следует оставить значения, для которых $\left(\frac{1-d}{p}\right) = -1$. Иными словами, следует найти число пар произведений $d(1 - d)$, в которых оба сомножителя – квадратичные невычеты. Подобная задача рассматривалась в работе [7] одним из авторов данной работы. Введем обозначение N для квадратичного невычета, S – для квадрата (квадратичного вычета), при этом (NN), (SS), (NS), (SN) – число пар в схеме Гаусса для всех произведений $m(m+1)$, $m = 1, 2, 3, \ldots, p - 1$. Перепишем $d(1 - d) = -d'(d' + 1)$, $d' = d - 1$, что отвечает схеме Гаусса. В этой схеме следует найти число пар (SN), так как $(-d')$ – квадратичный вычет, а $(d' + 1)$ – невычет. Согласно формулы (15) в [7] получим искомое число $(SN) = \frac{p - \varepsilon}{4}$, $\varepsilon = (-1)^{\frac{p-1}{2}}$. В нашем случае при $p \equiv 3\mathrm{mod}4$, $\varepsilon = -1$ и $(SN) = \frac{p + 1}{4}$. Таким образом, число кривых (1) порядка $4n$ для данного случая $M_B = (p + 1)/4$.

Итак, практически половина всех кривых (1) в обобщенной форме Эдвардса при $p \equiv 1\mathrm{mod}4$ и четверть их при $p \equiv 3\mathrm{mod}4$ имеет минимальный четный кофактор 4 порядка кривой. Их число в классе полных кривых Эдвардса вдвое больше, чем в классе скрученных кривых Эдвардса.

В этом свете не может не удивить статистика порядков кривых, приведенная в 4-м разделе работы [2]. Она, разумеется, возникла в связи с пересечением классов кривых, определенных в этой работе. В частности, кривые Эдвардса и полные кривые Эдвардса наполовину пересекаются. В таблицах распределения порядков протестированных кривых они записаны как разные классы. Такое же пересечение мы видим между классами скрученных и полных кривых Эдвардса. Неясно, откуда при $p \equiv 3\mathrm{mod}4$ в таблице порядков кривых (p =1019) возникает 236 скрученных кривых Эдвардса с минимальным кофактором 4. Согласно теореме 3.5 [2] в классе скрученных кривых (с условиями П.2.1) таких кривых не существует. Значит, они заимствованы из кривых, изоморфных полным кривым Эдвардса, т.е. одни и те же кривые регистрируются в разных классах. Определения классов кривых Эдвардса, принятые в [2], в принципе не могут дать достоверной статистики.

В статистике для построения распределений частот событий используются несовместные события. Классификация кривых в обобщенной форме Эдвардса с непересекающимися классами, предложенная нами в разделе 2, исключает

подобные вышеописанным парадоксы. Кроме того, она позволила найти точное решение для числа кривых в обобщенной форме Эдвардса с минимальным кофактором 4. При этом нет необходимости в статистике порядков кривых.

Заметим, что введение нового параметра a в обобщенную форму (1) кривой Эдвардса лишь в 1.5 раза расширяет множество кривых в форме Эдвардса с минимальным кофактором 4. Множество скрученных кривых с этим свойством существует лишь при $p \equiv 1 \bmod 4$. Кроме того, при сложении точек появляется дополнительная операция умножения на параметр a, что замедляет вычисления. Этот аргумент теряет значение, если зафиксировать a как минимальный квадратичный невычет в поле F_p и перейти к параметру $d' = \left(\frac{d}{a}\right)$ при поиске приемлемых кривых. Позитивным аргументом в пользу скрученных кривых Эдвардса является то, что при $p \equiv 1 \bmod 4$ все они имеют порядок $4n$, что упрощает поиск полезных для криптосистем кривых.

СПИСОК ЛИТЕРАТУРЫ

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

3. *Bernstein Daniel J. , Birkner Peter , Joye Marc , Lange Tanja, 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.

4. *Bernstein D.J., Lange T.* Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.

5. *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.

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

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