УДК 681.3.06

КЛАССИФИКАЦИЯ КРИВЫХ В ФОРМЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

А.В. БЕССАЛОВ, О.В. ЦЫГАНКОВА

Дан анализ свойств точек малых порядков скрученной кривой Эдвардса. Введена арифметика для групповых операций с особыми точками этих кривых. Предложена классификация кривых в форме Эдвардса на 3 непересекающихся класса. Получены точные формулы для числа кривых разных классов минимального порядка. Дан критический анализ результатов в работах других авторов.

Ключевые слова: эллиптическая кривая, скрученная кривая Эдвардса, параметры кривой, порядок точки, сложение точек, изоморфизм, квадратичное кручение, квадрат, неквадрат.

ВВЕДЕНИЕ

Эллиптические кривые в форме Эдвардса над простым полем, без сомнения, весьма перспективны в современной криптографии. Как мы доказали в работе [3], их производительность в среднем не менее чем в 1.5 раза превышает производительность 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 бесполезные изоморфные кривые, в кривых Эдвардса достаточно использовать один параметр d вместо обычных двух параметров a и b кривой в канонической форме Вейерштрасса.

В работе [2] авторы обобщили и расширили класс кривых Эдвардса [1] 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 [1] – полными кривыми Эдвардса. В работе [2] был дан детальный анализ некоторых свойств этих кривых, доказан ряд важных теорем, сделана попытка дать классификацию кривых в форме Эдвардса и привести некоторую статистику распределения порядков кривых, относящихся к разным классам этих кривых при небольших значениях модуля $p = 1009$ и $p = 1019$. 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 критический анализ свойств скрученных кривых Эдвардса. В первом разделе мы предлагаем арифметику для групповых операций с особыми точками этих кривых, даем анализ точек малых порядков и формулы, связывающие их с другими точками кривой. Во втором разделе мы обсуждаем и обосновываем некорректность некоторых утверждений и классификации кривых в [2], предлагаем классификацию кривых в форме Эдвардса с разбиением на три непересекающиеся класса в зависимости от свойств параметров a и d кривой. Мы анализируем свойства кривых всех трех классов и возможные значения порядков этих кривых. Наконец, в третьем разделе нами получены точные формулы для числа кривых различных классов с минимальным кофактором 4 и дан критический анализ результатов, приведенных в [2].

1. ТОЧКИ МАЛЫХ ПОРЯДКОВ СКРУЧЕННЫХ КРИВЫХ ЭДВАРДСА

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

$$E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2,$$

$$a \neq d,\ a,\ d \in F_p^*,\ d \neq 1,\ p \neq 2.$$

Наряду с вводом параметра a авторы [1, 2] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{ad}{p}\right) = \pm 1$. При $a = 1$ получаем *кривую Эдвардса*, а если у нее d – неквадрат или $\left(\frac{d}{p}\right) = -1$, то в [2] она названа *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [1]. В работе [4] мы предложили поменять местами x и y координаты в форме кривой Эдвардса с целью сохранения горизонтальной симметрии обратных точек, принятой в криптографии. Опираясь на это свойство, определим скрученную кривую Эдвардса уравнением

$$E_{E,a,d}: x^2 + ay^2 = 1 + dx^2y^2,$$

$$a, d \in F_p^*,\ d(d - a) \neq 0,\ p \neq 2. \quad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

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

При совпадении двух точек получим из (2) закон удвоения

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

Использование модифицированных законов (2), (3) позволяет сохранить горизонтальную симметрию (относительно оси x) обратных точек, общепринятую в теории эллиптических кривых. Определяя теперь обратную точку как $-P = (x_1, -y_1)$, получаем согласно (1) $(x_1, y_1) + (x_1, -y_1) = \mathbf{O} = (1, 0)$. 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 $\pm 2\boldsymbol{F_0} = \boldsymbol{D_0} = (-1, 0)$. Ясно, что эти точки существуют над полем F_p, если параметр a является квадратом.

Из уравнения (1) определим квадраты

$$x^2 = \frac{1-ay^2}{1-dy^2},\ y^2 = \frac{1-x^2}{a-dx^2}, \tag{4}$$

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

$$\boldsymbol{D_{1,2}} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right),\ \pm\boldsymbol{F_1} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \tag{5}$$

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 (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 $\mathbf{O}$ и точки 2-го и 4-го порядков кривой Эдвардса здесь и далее выделяются жирным шрифтом.

Кроме перечисленных, точки 4-го порядка могут существовать как неособые при ненулевых координатах x и y. Положим, например, $2\boldsymbol{F_2} = 2(x_1, y_1) = \boldsymbol{D_1}$. Тогда согласно (2) и (5) запишем два уравнения

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

Отсюда

$$\left(1 + dx_1^2 y_1^2\right) = 0,\ \Rightarrow\ x_1^2 + ay_1^2 = 0, \Rightarrow\ x_1^2 = -ay_1^2.$$

Согласно первому из записанных выше уравнений имеем

$$\frac{2x_1^2}{1 + \frac{d}{a}x_1^4} = \sqrt{\frac{a}{d}} \Rightarrow \frac{d}{a}x_1^4 - 2\sqrt{\frac{d}{a}}x_1^2 + 1 = 0 \Rightarrow$$

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

Итак, координаты возможных точек 4-го порядка

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

Необходимыми и достаточными условиями существования таких точек 4-го порядка являются:

$$\left(\frac{ad}{p}\right) = 1,\ p \equiv 3 \bmod 4. \tag{6}$$

Для этого случая множества всех квадратов и всех 4-х степеней элементов совпадают, т.е. если $\left(\frac{a}{p}\right) = 1$, то $a^2 \neq a$ для всех $a \neq 1$. При этом любой из квадратов имеет 2 квадратных корня и 2 корня 4-й степени. Действительно, если α – примитивный элемент мультипликативной группы F_p^*, и α^2 – квадрат этой группы, то $\alpha^2\alpha^{p-1} = \alpha^{2+4k+2} = \alpha^{4(k+1)}$. Значит, любой квадрат имеет и корни 4-й степени.

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 проверке 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. Пусть $S = (x_1, y_1)$ – точка 8-го порядка, тогда $2S_1 = \boldsymbol{F_0} = (0, 1/\sqrt{a})$ – точка 4-го порядка. Согласно (2)

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

Тогда

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

Так как справедливо

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

то возникают следующие необходимые и достаточные условия существования точек 8-го порядка:

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

$$\left(\frac{1 - \frac{d}{a}}{p}\right) = 1 \text{ и } \left(\frac{1 + \sqrt{1 - \frac{d}{a}}}{p}\right) = 1.$$

Например, 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, т. к. группа нециклическая.

При условии существования особых точек (5) 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:

$$(x_1, y_1) + (-1, 0) = (-x_1, -y_1),$$

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

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

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

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

Все найденные суммы удовлетворяют уравнению (1) при подстановке, т.е. 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.

Важно заметить, что использование правил предельного перехода сохраняет операцию сложения любых пар точек, включая особые. Это позволит говорить об изоморфизме кривых в различной форме.

2. КЛАССИФИКАЦИЯ КРИВЫХ В ФОРМЕ ЭДВАРДСА

В работе [2], как нам представляется, допущен ряд некорректных утверждений и результатов, которые мы выносим на обсуждение. Основные теоремы в этой работе опираются на бирациональную эквивалентность между кривыми (1) и кривыми в форме Монтгомери, заданными уравнением

$$E_{M,A,B}: Bv^2=u^3+Au^2+u,\ A=2\frac{a+d}{a-d},\ B=\frac{4}{a-d},$$

$$a=\frac{A+2}{B},\ d=\frac{A-2}{B},\ A^2\neq 4. \tag{7}$$

Она основана на замене координат с помощью рациональных функций

$$y=\frac{u}{v},\ \ x=\frac{u-1}{u+1}\ \ u=\frac{1+x}{1-x},\quad v=\frac{u}{x}. \tag{8}$$

В работе [2] доказывается теорема 3.2: *любая скрученная кривая Эдвардса* (1) *бирационально эквивалентна кривой* (7) *в форме Монтгомери.*

Так как нам придется далее обращаться к паре квадратичного кручения (quadratic twist [2]), мы также проведем отображение точек (7) в точки кривой (1) .

Разделим (7) на v^2 и с учетом (8) получим

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

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

Отсюда

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

и, наконец, получаем изоморфную кривой (7) кривую в форме (1)

$$E_{M,A,B}\sim E_{E,a,d}:\ (1-x^2)=y^2(a-dx^2). \tag{9}$$

Нетрудно с помощью (8) 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 $E_{Ea,d}$ изоморфны. Этот изоморфизм сохраняет порядки всех точек.

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

$$E^t_{M,A,B}\sim E_{M,A,cB}: cBv^2=u^3+Au^2+u,$$

$$A=2\frac{a+d}{a-d},\ B=\frac{4}{a-d}. \tag{10}$$

Изоморфная ей скрученная кривая Эдвардса, как можно видеть из выполненных выше преобразований, записывается как

$$E^t_{E,a,d}\sim E_{E,ca,cd}:$$

$$(1-x^2)=cy^2(a-dx^2)=y^2(ca-cdx^2). \tag{11}$$

Иначе говоря, для построения пары квадратичного кручения к кривой в форме (1) необходимо перейти к новым параметрам кривой $a=ca, d=cd$, т.е. квадраты обращаются в неквадраты и обратно.

Во втором разделе пионерской работы [2] 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.

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

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

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 (8) им отвечают точки кривой Монтгомери (7) $D_{M0}=(0,0)$ и $\pm F_{M0}=(1,\pm\sqrt{a})$. 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, имеет место изоморфизм $E_{E,a,d}\sim E_{E,1,d/a}$.

1.2. $\left(\frac{a}{p}\right)=-1, \left(\frac{d}{p}\right)=1$. Здесь также нет особенностей, т. к. 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 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 *полные кривые Эдвардса*.

2. $\left(\frac{ad}{p}\right) = 1$. Именно этот случай образует класс скрученных кривых Эдвардса и класс кривых Эдвардса с квадратичным параметром d. Как мы показали, квадратичное кручение образуется смещением параметров $d' = cd$, $a' = ca$, где c – неквадрат. Поэтому кривые в п.2.1. и 2.2. образуют пару квадратичного кручения. Свойства одной из кривых пары кручения полезны для определения свойств другой.

2.1. $\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$. Согласно (7) имеем $(Bad)^2 = (A+2)(A-2)$ и, следовательно, дискриминант квадратного уравнения в правой части (7) $(A^2 - 4)$ является квадратом. Тогда кубическое 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: $D_{M0} = (0,0)$, $D_{M1,2} = (-(A \pm \sqrt{A^2-4})/2,\ 0)$, с координатами $v_{0,1,2} = 0$. Преобразованием координат (8) точка D_{M0} кривой (7) переходит в точку $\boldsymbol{D_0} = (-1,\ 0)$ кривой (1), а две другие точки $D_{M1,2}$ трансформируются 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), такие точки могут лежать не на оси кривой при выполнении $\left(\frac{ad}{p}\right) = 1$ и $p \equiv 3 mod 4$. Итак, данный случай характерен наличием трех точек 2-го порядка (из них две точки – особые точки на бесконечности) и наличием точек 4-го порядка лишь при $p \equiv 3 \mathrm{mod} 4$. 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 он существует.

Рассмотренный здесь случай наиболее интересен для практических приложений, т. к. кривая $E_{E,a,d}$ имеет минимальное число особенностей.

2.2. $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1$. Как и в предыдущем случае, при $v = 0$ дискриминант уравнения (7) $(A^2 - 4) = (Bad)^2$ является квадратом и вновь мы имеем 3 точки 2-го порядка с теми же координатами, что и в п. 2.1. Две из них преобразованием (8) переходят в особые точки 2-го порядка 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 (7) содержит две точки 4-го порядка с координатой $u_1 = -1$, которые отображением (8) порождают особые точки кривой Эдвардса (1). Действительно, из уравнения касательной к кривой (3) в точке 4-го порядка $P_M = (u_1, v_1)$, проходящей через точку (0,0) 2-го порядка, имеем

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

Тогда с учетом (7) получим $u_1^2 = 1 \Rightarrow u_1 = \pm 1$. Одна из пар точек 4-го порядка имеет координаты $\pm F_M = (-1,\ \pm\sqrt{(A-2)B})$. Как следует из (8), эти две точки кривой Монтгомери с координатой $u_1 = -1$ преобразуются в особые точки 4-го порядка кривой (1) с x-координатами $\pm\sqrt{(A-2)B}$, и с делением на 0 y-координаты $y = (u_1 - 1)/(u_1 + 1)$. В итоге в рассматриваемом случае получили 4 особые точки (на бесконечности): по две точки 2-го и 4-го порядков. Для данного случая преобразование координат $(x,\ y) \to (X/\sqrt{a},\ Y)$ дает изоморфную кривой (1) кривую Эдвардса с квадратичным параметром $X^2 + Y^2 = 1 + d'X^2Y^2$, где $d' = d/a \Rightarrow \left(\frac{d'}{p}\right) = 1$ и имеет место изоморфизм $E_{E,a,d} \sim E_{E,1,d/a}$. Кривые этого пункта мы относим к *кривым Эдвардса* (с квадратичным параметром d в поле F_p). У них наихудшие свойства из рассмотренных.

Важно отметить, что для 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 $\left(\frac{ad}{p}\right) = 1$.

Итак, можно разбить все кривые в форме Эдвардса на непересекающиеся классы:

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

В работе [1] 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.

Докажем полноту закона сложения (2) для скрученных кривых Эдвардса.

Теорема 2.1. *При* $\left(\frac{a}{p}\right)=-1$, $\left(\frac{d}{p}\right)=-1$ *и любых входах знаменатели в* (2) $1+dx_1x_2y_1y_2 \neq 0$, $1-dx_1x_2y_1y_2 \neq 0$.

Доказательство. Допустим обратное:

a) $1+dx_1x_2y_1y_2=0$ или *b*) $1-dx_1x_2y_1y_2=0$.

Пусть справедливо равенство *a*). Тогда $x_1y_1=\frac{-1}{dx_2y_2}$. Рассмотрим квадрат

$$\left(x_1+\sqrt{a}y_1\right)^2=x_1{}^2+ay_1{}^2+2\sqrt{a}x_1y_1=$$

$$1+dx_1{}^2\,y_1{}^2+2\sqrt{a}x_1y_1=$$

$$=1+\frac{1}{dx_2{}^2\,y_2{}^2}-\frac{2\sqrt{a}}{dx_2y_2}=(dx_2{}^2\,y_2{}^2)^{-1}\left(x_2-\sqrt{a}y_2\right)^2.$$

Аналогично получим

$$\left(dx_2{}^2\,y_2{}^2\right)\left(x_1-\sqrt{a}y_1\right)^2=\left(x_2+\sqrt{a}y_2\right)^2.$$

При $\left(\frac{d}{p}\right)=-1$ эти равенства справедливы лишь при $x_i=y_i=0$, но такая точка не существует, либо при $x_i=\pm\sqrt{a}y_i$, что невозможно при $\left(\frac{a}{p}\right)=-1$. Итак, допущение *a*) привело к противоречию. Тот же результат получим при допущении *b*). Теорема доказана.

Для криптографических приложений следует искать кривые порядка $N_E = 4n$ с минимальным кофактором 4 при нечетном n, из которых отбираются кривые с простым n. Среди полных кривых Эдвардса (условия пп. 1.1 и 1.2) 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. Кривая Эдвардса в этой работе определена как $E_{E,1,d}$ без ограничений на параметр d. По нашей классификации это объединяет полные кривые Эдвардса и кривые Эдвардса с квадратичным параметром. Предлагаемая нами классификация кривых в форме Эдвардса с разбиением их на непересекающиеся классы является логичной и исключающей возможные недоразумения.

В теореме 3.3 [2] 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 $p \equiv 3 \bmod 4$ равна

$$N_E + N^t_E = 2(p + 1) = 2(4k+3 + 1) \equiv 0 \bmod 8.$$

Отсюда следует $N^t_E \equiv 0 \bmod 8$.

При $p \equiv 1 \bmod 4$ мы получим

$$N_E + N^t_E = 2(p + 1) = 2(4k+1 + 1) \equiv 0 \bmod 4,$$

т.е. с учетом $N_E \equiv 0 \bmod 8$ для скрученной кривой Эдвардса порядок $N^t_E \equiv 0 \bmod 4$. Ясно, что в этом случае она имеет три точки 2-го порядка и не имеет точек 4-го порядка. Это подтверждается условием (6). 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 $p \equiv 1 \bmod 4$.

Условия, порождающие скрученные кривые Эдвардса с минимальным кофактором порядка $N_E = 4n$, можно найти также, опираясь на свойства кривой Монтгомери (7). Мы знаем, что на кривой Монтгомери $E_{M,A,B}$ для первой координаты точки 4-го порядка выполняется равенство $u_1^2=1 \Rightarrow u_1=1$. Подставляя эти значения в (7), получим $Bv^2 = A + 2 = Ba$ и $Bv^2 = A - 2 = Bd$. Следовательно, в условиях п.2.1 при $p \equiv 1 \bmod 4$ точек 4-го порядка на кривой Монтгомери и изоморфной ей скрученной кривой Эдвардса не существует. Любая такая кривая имеет порядок $4n$ при нечетном n и $p \equiv 1 \bmod 4$.

Обращаясь к примеру кривой

$$E_{M,9,1} : v^2 = u^3 + 9u^2 + u,\ p = 17$$

приведенному в [2] и отвечающего согласно (7) условиям п.2.1., получаем уравнение скрученной кривой $E_{E,11,7} : x^2 + 11y^2 = 1 + 7x^2y^2$ (здесь параметры $a = 11$ и $d = 7$ являются квадратичными невычетами по модулю 17). Кривая Монтгомери $v^2 = u(u + 3)(u + 6)$ имеет порядок $N_E = 20$, содержит три точки 2-го порядка и не имеет точек 4-го порядка. Она является нециклической с типом T = (2,2,5) и представляется прямой суммой циклических подгрупп 2-го и 10-го порядков. Ясно, что она содержит две различные подгруппы простого порядка 5 (всего имеется 8 точек 5-го и

8 точек 10-го порядков). Если уравнение $E_{E,11,7}$ записать как $x^2 = (y^2 - 1)/(7y^2 - 11)$, то и числитель, и знаменатель здесь обращаются в 0 при соответственно $y^2 = 1$ и $y^2 = 4$. Особые точки для координаты x возникают при $y = \pm 2$. Согласно (8) $x = (u - 1)/(u + 1)$ и эти значения отвечают корням $u_{2,3} \in \{-3, -6\}$ кубического уравнения в $E_{M,9,1}$, т.е. особым точкам 2-го порядка $\boldsymbol{D_{2,3}} = (\pm 2, \infty)$. Например, примем $P = (8,1)$, тогда $2P = (3, -5,)$, $4P = (-4,6)$, $8P = (3,5)$. Так как $8P = -2P$, то $10P = \mathrm{O}$ и $\mathrm{Ord}P = 10$. Но в подгруппу $<P>$ входит особая точка 2-го порядка $5P = 4P + P = (2, \infty)$. Приняв генератором подгруппы 5-го порядка точку $G = 2P$ простого порядка 5, можно в подгруппе точек $<G>$, не включающей особых точек, использовать арифметику кривых с групповой операцией (2) без особенностей. Это справедливо для любых точек нечетного порядка.

3. ЧИСЛО СКРУЧЕННЫХ КРИВЫХ ЭДВАРДСА ПОРЯДКА 4*n*

Изучив свойства скрученных кривых Эдвардса, нет необходимости обращаться к статистике порядков этих кривых, как это сделано в [2]. На основе нашей классификации, данной во втором разделе, и свойств кривых, мы можем найти точное число этих кривых с минимальным четным кофактором 4-го порядка $4n$ кривой (n — нечетное). Для этого мы рассматриваем лишь случай $p \equiv 1 \bmod 4$, при котором они существуют.

Для полных кривых Эдвардса с условием п.1 число всех кривых равно числу неквадратов (квадратичных невычетов [7]) $(p - 1)/2$. Так как для пары квадратичного кручения справедливо $N_E + N^t_E = 2(p + 1) \equiv 0 \bmod 4$, то из $N_E = p + 1 - t \equiv 0 \bmod 4$ и $p + 1 \equiv 2 \bmod 4$ имеем $\pm t \equiv 2 \bmod 4$. При этом $N^t_E \equiv 0 \bmod 8$. 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 $M_1 = M_{11} + M_{12} = (p - 1)/4$.

Для кривых с условиями п.2 классификации кривые Эдвардса с квадратичным параметром (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 $\left(\frac{a}{d}\right)\left(\frac{d}{a}\right)$ 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 $p \equiv 1 \bmod 4$ имеют минимальный кофактор 4-го порядка кривой.

Итак практически половина всех кривых Эдвардса имеет минимальный кофактор 4. Их число для полных кривых Эдвардса и скрученных кривых Эдвардса также приблизительно одинаково.

В этом свете не может не удивить статистика порядков кривых, приведенная в [2]. Она, разумеется, возникла в связи с пересечением классов кривых, определенных в этой работе (например, 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. Иначе откуда при $p \equiv 3 \bmod 4$ 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. Ситуация напоминает двойное налогообложение, и одни и те же кривые регистрируются в разных классах.

В теории вероятностей для построения распределений вероятностей событий используются несовместные события. Классификация кривых в форме Эдвардса с непересекающимися классами, предложенная нами в разделе 2, исключает подобные вышеописанные недоразумения. Кроме того, она позволила найти точное решение для числа скрученных кривых Эдвардса с минимальным кофактором 4, что конструктивно для криптографии и делает бессмысленным обращение к статистике.

Заметим, что введение нового параметра a в определение скрученной кривой Эдвардса практически не дает новых полезных свойств и лишь вдвое расширяет множество кривых в форме Эдвардса с минимальным кофактором 4. Вместе с тем такие скрученные кривые существуют лишь при $p \equiv 1 \bmod 4$. Кроме того, в групповой операции появляется дополнительная операция умножения на параметр a, что лишь замедляет вычисления. Правда, этот аргумент несущесвенный, если принять a как минимальный неквадрат в поле F_p и варьировать параметром $\left(\frac{d}{a}\right)$ при поиске простого n. 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.

Литература

1. *Bernstein Daniel J., Lange Tanja.* Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007. – P. 1–20.
2. *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. – P. 1–17.
3. *Бессалов А.В., Цыганкова О.В.* Производительность групповых операций на скрученной кривой Эд-

вардса над простым полем. Радиотехника №181, 2015. – С. 58–63.

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.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. – С. 203–208.
6. *Бессалов А.В., Дихтенко А.А.,Третьяков Д.Б.* Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, №4, 2011. – С. 33–36.
7. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224 с.

Поступила в редколлегию 3.11.2015

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

Цыганкова Оксана Валентиновна, аспирант кафедры ММЗИ ФТИ НТУУ «КПИ». Научные интересы: эллиптические кривые в форме Эдвардса.

УДК 621. 3.06

Класифікація кривих у формі Едвардса над простим полем / А.В. Бессалов, О.В. Циганкова // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – № 4. – С. 277–283.

Дано аналіз властивостей точок малих порядків скрученої кривої Едвардса. Введено арифметику для групових операцій з особистими точками цих кривих. Запропоновано класифікацію кривих у формі Едвардса на 3 непересічних класи. Отримано точні формули для кількості кривих різних класів мінімального порядку. Дано критичний аналіз результатів у работах інших авторів.

Ключові слова: еліптична крива, скручена крива Едвардса, параметри кривої, порядок точки, додавання точок, ізоморфізм, квадратичне кручення, квадрат, неквадрат.

Бібліогр.: 7 найм.

UDC 621. 3.06

Classification of curves in the Edwards form over a prime field / A.V. Bessalov, O.V. Tsygankova // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 277–283.

The paper analyzes the properties of points of small orders of the twisted Edwards curve. Arithmetic for group operations with critical points of these curves is introduced. A classification of curves in the Edwards form into three nonoverlapping classes is suggested. Exact formulas for the number of curves of differen classes of minimum order are obtained. A critical analysis of the results of the other authors' works is provided.

Keywords: elliptic curve, twisted Edwards curve, curve parameters, point order, addition of points, isomorphism, square twist, square, nonsquare.

Ref.: 7 items.