УДК 621.391.15: 519.7

# УНИКАЛЬНЫЕ КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЦИКЛИЧЕСКИХ СКРУЧЕННЫХ КРИВЫХ ЭДВАРДСА

*А. В. БЕССАЛОВ*

Дан анализ свойств точек 4-го и 8-го порядков в классах нециклических скрученных и квадратичных кривых Эдвардса. Доказаны теоремы о существовании не особых точек 4-го и 8-го порядков в этих классах. Дан обзор свойств трех классов кривых в обобщенной форме Эдвардса. Обсуждаются полезные для криптографии свойства скрученных кривых Эдвардса.

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

## ВВЕДЕНИЕ

Авторы работ [1,2] впервые определили кривые Эдвардса к той форме, которая сделала их весьма перспективными для задач современной асимметричной криптографии. Они же дали детальный, но не всегда корректный анализ свойств этих кривых. В работах [3,4] мы обосновали свою критику и предложили новую классификацию *кривых в обобщенной форме Эдвардса* с разбиением их на 3 непересекающихся класса *полных*, *скрученных* и *квадратичных* кривых Эдвардса. В работе [2] все эти классы с кардинально отличающимися свойствами объединены термином «Twisted Edwards Curves» (скрученные кривые Эдвардса), что сразу внесло путаницу в их же статистику, приведенную в разделе 4 [2]. В этой связи после работы [4] мы пользуемся нашей классификацией.

Кривые Эдвардса с одним параметром, определенные в работе [1], имеют очень привлекательные для криптографии преимущества: максимальная скорость экспоненцирования точки [1,3], полнота и универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек, повышенная безопасность в отношении атак бокового канала [1]. Программирование групповых операций становится более эффективным и ускоряется в связи с отсутствием особой точки на бесконечности как нуля абелевой группы точек. Введение второго параметра кривой в работе [2] расширяет класс кривых Эдвардса и ставит вопрос: насколько это может оказаться полезным для криптографических приложений? В данной статье этот вопрос обсуждается.

В разделе 1 статьи вводятся основные определения и обозначения, приводятся законы сложения и удвоения точек в форме, адаптированной к горизонтальной симметрии обратных точек [5]. В разделе 2 дается анализ свойств точек малых порядков, и доказывается теорема 1 о точках 4-го порядка с формулировкой, более общей в сравнении с подобной теоремой в работе [4]. В ней определены условия существования не особых точек 4-го порядка для двух классов нециклических кривых Эдвардса. Здесь же доказана теорема 2 об условиях существования точек 8-го порядка. В разделе 3 резюмируются определения и свойства 3-х классов кривых в форме Эдвардса согласно новой классификации [4]. В названии статьи термин «нециклические скрученные кривые Эдвардса» позволяет избежать неоднозначности термина «скрученные кривые Эдвардса» в мировой литературе. В разделе 4 обсуждаются некоторые особые свойства и преимущества скрученных кривых Эдвардса для криптографических приложений.

## 1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

В работе [2] *скрученные кривые Эдвардса* (twisted Edwards curves) определены как обобщение кривых [1]

$$x^2 + y^2 = 1 + dx^2y^2, \left(\frac{d}{p}\right) = -1$$

введением нового параметра $a$ в уравнение

$$ax^2 + y^2 = 1 + dx^2y^2, a, d \in F_p^*, d \neq 1, a \neq d, p \neq 2 .$$

Наряду с вводом параметра $a$ авторы [2] сняли ограничения на пару параметров $a$ и $d$, допуская любые свойства квадратичности $\left(\frac{ad}{p}\right) = \pm 1$. При $a = 1$ такая кривая получила в [2] название *кривой Эдвардса*, а если у нее $d$ – квадратичный невычет (т.е. символ Лежандра $\left(\frac{d}{p}\right) = -1$), то – *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [1]. 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

$$E_{a,d}: \quad x^2 + ay^2 = 1 + dx^2y^2 , \; a , \; d \in F_p^* , \; d \neq 1 ,$$

$$a \neq d\ ,\ p \neq 2\,. \qquad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) =$$

$$= \left( \frac{x_1 x_2 - a y_1 y_2}{(1 - d x_1 x_2 y_1 y_2)}, \frac{x_1 y_2 + x_2 y_1}{(1 + d x_1 x_2 y_1 y_2)} \right). \qquad (2)$$

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

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

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), координаты нейтрального элемента группы $O = (x_1, y_1) + (x_1, -y_1) = (1, 0)$. Кроме нейтрального элемента $O$ на оси $x$ также всегда лежит точка $D_0 = (-1, 0)$ второго порядка, для которой в соответствии с (3) $2D_0 = (1, 0) = O$ В зависимости от свойств параметров $a$ и $d$ можно получить еще 2 особые точки 2-го порядка и 2 или 4 точки 4-го порядка. Как следует из (1), на оси $y$ могут лежать точки $\pm F_0 = \left(0, \pm 1/\sqrt{a}\right)$ 4-го порядка, для которых $\pm 2F_0 = D_0 = (-1, 0)$. Эти точки существуют над полем $F_p$, если параметр $a$ является квадратом (квадратичным вычетом).

Из уравнения (1) определим квадраты:

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

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

$$D_{1,2} = \left( \pm\sqrt{\frac{a}{d}}, \infty \right),\ \pm F_{11} = \left( \infty, \pm\frac{1}{\sqrt{d}} \right). \qquad (4)$$

Они возникают в случаях $\left(\frac{ad}{p}\right) = 1$ и $\left(\frac{d}{p}\right) = 1$ соответственно. По правилам предельного перехода и закона удвоения (3) можно проверить, что $2D_{1,2} = O$, $\pm 2F_1 = D_0 = (-1, 0)$. Иными словами, при выполнении условий их существования особые точки $D_{1,2}$ есть точки 2-го порядка, а особые точки $\pm F_1$ – точки 4-го порядка.

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

## 2. СВОЙСТВА ТОЧЕК 4-ГО И 8-ГО ПОРЯДКОВ КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА

Дадим анализ некоторых новых свойств точек 4-го и 8-го порядков.

**Теорема 1**. Не особые точки 4-го порядка

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

*кривой в форме (1) при* $x \neq 0$ *существуют тогда и только тогда, когда выполняются условия:*

(i) *при* $p \equiv 3 mod 4$: $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$;

(ii) *при* $p \equiv 1 mod 4$: $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = 1,\ ad = c^4$.

**Доказательство**. *Необходимость.* Особые точки $\pm F_1 = \left( \infty, \pm\frac{1}{\sqrt{d}} \right)$ согласно формул (4), возникающие при $\left(\frac{d}{p}\right) = 1,$ исключаются из рассмотрения в соответствии с формулировкой теоремы. Не рассматриваются также точки $\pm F_0 = \left(0, \pm 1/\sqrt{a}\right)$ при $x = 0$. Пусть $F_2 = (x_1, y_1)$ – точка 4-го порядка кривой (1), тогда $2F_2 = 2(x_1, y_1) = D_1$. Согласно (3) и (4) запишем два уравнения:

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

Отсюда $\left(1 + d x_1^2 y_1^2\right) = 0\,,\ \ \Rightarrow x_1^2 + a y_1^2 = 0\,,\ \ \Rightarrow$ $x_1^2 = -a y_1^2$. Из $x_1 \neq 0$ следует $y_1 \neq 0$. Здесь второе равенство записано на основании уравнения (1) кривой. Согласно первому из уравнений и равенства $x_1^2 = -a y_1^2$ имеем

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

$$y_1^2 = \frac{-1}{\sqrt{ad}}\,.$$

Итак, получаем 4 точки с координатами:

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

которые определены в формулировке теоремы. При $p \equiv 3 \bmod 4$ элемент (–1) есть квадратичный невычет [7], тогда $(-a)$ – квадратичный вычет в условиях (i) и равенство $x_1^2 = -ay_1^2$ корректно связывает квадраты координат точки $F_2$. Пусть $\beta$ – примитивный элемент мультипликативной группы $\mathrm{F}_p^*$, и $\beta^2$ – квадрат этой группы, тогда при условии (i) имеем $\beta^2 = \beta^2\beta^{p-1} = \beta^{2+4k+2} = \beta^{4(k+1)}$. Значит, любой квадрат имеет квадратные корни и корни 4-й степени при $p \equiv 3 \bmod 4$. Необходимость существования первых координат в (5) с учетом условий (i) доказана. 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 (i) теоремы доказана.

При $p \equiv 1 \bmod 4$ (условия теоремы) элемент (–1) есть квадратичный вычет [7], тогда равенство $x_1^2 = -ay_1^2$ выполняется при $\left(\frac{a}{p}\right) = 1$. Для квадрата мультипликативной группы имеем $\beta^2 = \beta^2\beta^{p-1} = \beta^{2+4k} = \beta^{2(2k+1)}$. Для этого случая при $\beta = c^2$ число элементов $c^4$ при всех ненулевых значениях $c$ равно $(p-1)/4$. Обе координаты точек (5) существуют, если $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = 1$, и $ad = c^4$ (или $a/d = c^4$ для $c \in \mathrm{F}_p$). Тогда и для второй координаты справедливо $\frac{1}{ad} = \frac{c^4}{a^2} = e^4$. Итак, необходимость условий (ii) теоремы доказана.

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

Точки $\pm F_{2,3}$ можно рассматривать как точки деления на 2 особых точек 2-го порядка $D_{1,2}/2$ [3,6].

**Пример 1**. Для кривой $x^2 - y^2 = (1 + 3x^2y^2) mod 7$ (здесь $a = -1$, $d = 3$ – квадратичные невычеты при $p = 7 \equiv 3 \bmod 4$ и выполняются условия (i) теоремы 1) точки 4-го порядка (5) имеют координаты $\pm F_{2,3} = (\pm 2, \pm 2)$. При удвоении их согласно (3) получим $2F_2 = (\pm 3, \infty) = D_{1,2}$. Порядок $N_E$ этой кривой, включающей точки $O$, $F_{2,3}$, $D_{0,1,2}$, равен 8, группа точек нециклическая с типом $T = (2, 2^2)$.

**Пример 2**. В условиях (ii) теоремы 1 рассмотрим кривую $x^2 + y^2 = (1 + 3x^2y^2) mod 13$ (здесь $a = 1$, $d = 3$ – квадратичные вычеты при $p = 13$). Согласно (5) находим точки 4-го порядка $\pm F_{2,3} = (\pm 6, \pm 4)$. Кроме того, согласно (4) кривая имеет две особые точки 4-го порядка $\pm F_1 = (\infty, \pm 3)$. Подстановка значений координат точек $F_{2,3}$ в уравнение кривой дает $6^2 + 4^2 = 1 + 3 \cdot 6^2 \cdot 4^2 = 0$. Удвоение точек $F_{2,3}$ согласно (3) дает точки $2F_2 = \left(\pm\sqrt{\frac{a}{d}}, \infty\right) = (\pm 3, \infty) = D_{1,2}$. Эта кривая имеет порядок $N_E = 16$ и является нециклической с типом $T = (2^2, 2^2)$.

**Утверждение 1.** *Все кривые Едвардса* (1) с условиями $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$ *при* $p \equiv 1 \bmod 4$ *имеют порядок* $N_E = 4n$ ($n$ *– нечетное*).

**Доказательство**. В условиях $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$ теоремы 1 при $p \equiv 1 \bmod 4$ кривая не содержит точек 4-го порядка, но включает нециклическую подгруппу 4-го порядка точек 2-го порядка $G_4 = \{O, D_0, D_1, D_2\}$. Следовательно, порядки всех других точек могут быть равными $n$ и $2n$ (вместе с возможными нечетными сомножителями $n$). Итак, подгруппа $G_4$ есть подгруппа минимального четного порядка 4 кривой, и порядок кривой $N_E = 4n$ Утверждение доказано. ▲

Найдем необходимые условия существования точек 8-го порядка, порожденных делением на 2 точки $F_0$.

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

**Доказательство**. Пусть $S=(x_1,y_1)$ – точка 8-го порядка, тогда $2S_1=F_0=(0,\ 1/\sqrt{a})$ – точка 4-го порядка на оси *y*. Согласно (3) и координат точки $F_0$ имеем

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

Тогда $x_1^2=ay_1^2\Rightarrow\frac{d}{a}x_1^4-2x_1^2+1=0,\quad\Rightarrow x_{1,2}{}^2=$ $=\frac{a}{d}\left(1\pm\sqrt{1-\frac{d}{a}}\right)$. Координаты точек $S_k$, $k=1..4$ или $k=1..8$ определяются из

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

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 (7). 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 (i) 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 $\left(\frac{1-\frac{d}{a}}{p}\right)=1$ должны выполняться условия $\left(\frac{1+\sqrt{1-\frac{d}{a}}}{p}\right)=1$ и $\left(\frac{1-\sqrt{1-\frac{d}{a}}}{p}\right)=1$. 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, т. к. 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 1 кривой с $a=-1$, $d=3$ 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.

При условии существования особых точек (4) вместе с точками $D_0,\pm F_0=(0,\ \pm1/\sqrt{a})$, 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.

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 [2,3].

## 3. КЛАССИФИКАЦИЯ КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА

Обоснование новой классификации кривых в обобщенной форме Эдвардса дано в работах [3,4]. Здесь даны определения 3-х классов этих кривых и перечень фундаментальных свойств кривых разных классов.

В зависимости от свойств параметров $a$ и $d$ кривые в обобщенной форме Эдвардса (1) разбиваются на 3 непересекающиеся класса изоморфизмов:

- *полные кривые Эдвардса* (с условием С1: $\left(\frac{ad}{p}\right)=-1$ :
- *скрученные кривые Эдвардса* (с условиями С2.1: $\left(\frac{a}{p}\right)=-1, \left(\frac{d}{p}\right)=-1$;
- *квадратичные кривые Эдвардса* (с условиями С2.2: $\left(\frac{a}{p}\right)=1, \left(\frac{d}{p}\right)=1$.

Основные свойства этих классов кривых:

3.1 В отношении точек 2-го порядка первый класс полных кривых Эдвардса над простым полем является классом *циклических* кривых, скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых. Максимальный порядок точек кривых последних классов равен $N_E / 2$.

3.2 Класс полных кривых Эдвардса не содержит особых точек.

3.3 Скрученные кривые Эдвардса содержат лишь две особых точки 2-го порядка $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$.

3.4 Квадратичные кривые Эдвардса содержат две особые точки 2-го порядка $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$ и две особые точки 4-го порядка $\pm F_{11}=\left(\infty,\pm\frac{1}{\sqrt{d}}\right)$.

3.5 Скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения на основе преобразования параметров: $a=ca, d=cd, \left(\frac{c}{p}\right)=-1$.

3.6 Полные и квадратичные кривые Эдвардса изоморфны кривым с параметром $a$ = 1: $E_{a,d} \sim E_{1.,d/a}$. Введение нового параметра $a$ в уравнение кривой (1) оправдано лишь для класса скрученных кривых Эдвардса.

3.7 Для точек нечетного порядка закон сложения точек (2) всегда является полным (т.е. сумма любой пары точек не дает особой точки).

## 4. СПЕЦИФИЧЕСКИЕ СВОЙСТВА СКРУЧЕННЫХ КРИВЫХ ЭДВАРДСА ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЙ

Для криптографических приложений следует искать кривые Эдвардса порядка $N_E = 4n$ с минимальным кофактором 4 при нечетном *n*, из которых отбираются кривые с простым значением *n*. Среди полных кривых Эдвардса (условие С.1) практически половина имеют порядок 4*n* (*n* – нечетное). Они являются циклическими, и их порядки пробегают все кратные 4-м числа в границах Хассе. Квадратичные кривые Эдвардса с параметром $\left(\frac{d}{p}\right)=1$ (условия С.2.2) являются нециклическими с тремя точками 2-го порядка и четырьмя или восемью точками 4-го порядка (в последнем случае согласно теореме 1 $p \equiv 1 \bmod 4$ ). Отсюда следует, что они содержат нециклическую подгруппу, изоморфную Z/2 × Z/4 порядка 8, а порядок этих кривых имеет минимальный кофактор 8. Они наименее привлекательны для криптографии. Поэтому кривые порядка $N_E = 4n$ наряду с полными кривыми Эдвардса можно искать лишь среди скрученных кривых Эдвардса в условиях С.2.1.

Согласно утверждению 1, при $p \equiv 1 \bmod 4$ все скрученные кривые Эдвардса имеют порядок $N_E = 4n$. Это первое уникальное свойство скрученных кривых, сводящее поиск криптостойких кривых к поиску кривых с почти простым порядком 4*n* (*n* – простое) при условии $p \equiv 1 \bmod 4$. Генератор криптосистемы выбирается как точка *G* простого порядка *n* (Ord*G* = *n*). Так как практически любая случайная точка *P* нециклической скрученной кривой имеет порядок *n* или 2*n*, генератор криптосистемы легко находится простым удвоением случайной точки: *G* = 2*P*. Это второе уникальное свойство скрученных кривых Эдвардса, полезное на этапе вычисления общесистемных параметров.

Наличие двух особых точек 2-го порядка $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$ на скрученной кривой не является основанием для отказа от их внедрения в стандарты асимметричной криптографии. Эти точки лежат за пределами подгруппы точек < *G* > простого порядка *n*, с которыми оперирует криптосистема. Согласно свойству 3.7, для точек этой подгруппы закон сложения (2) точек полный.

Наконец, выбирая минимальное значение параметра $a \in \{2,3\}$ как квадратичного невычета, можно достичь, как и для полных кривых, максимальной производительности имплементации крипто алгоритмов. Средний выигрыш в производительности экспоненцирования точки на кривой Эдвардса в сравнении с кривой в форме Вейерштрасса достигает 1.6 раза [3].

**Литература**

[1] *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.

[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, PP. 1–17.

[3] *Бессалов А.В.* Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. – 272 с.

[4] *Бессалов А.В., Цыганкова О.В.* Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. Проблемы передачи информации, – Том 53 (1), 2017. – С. 101–111.

[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. 92–98.

[6] *Бессалов А.В.* Метод нахождения порядка точки скрученной кривой Эдвардса. Радиотехника, №.186, 2016. – С. 110–118.

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

Поступила в редколлегию 06.06.2018

**Бессалов Анатолий Владимирович**, доктор технических наук, профессор, профессор НТУУ «КПИ им. Игоря Сикорского». Область научных интересов – асимметричная криптография.

УДК 621.391.15: 519.7

Бессалов А.В. **Унікальні криптографічні властивості нециклічних скручених кривих Єдвардса** / А.В. Бессалов // Прикладна радіоелектроніка: науково – техн. журнал. – 2018. – Том 17, №. 1, 2. – С. 49–54.

Дано аналіз властивостей точок 4-го і 8-го порядків у класах нециклічних скручених і квадратичних кривих Едвардса. Доведено теореми про існування точок 4-го і 8-го порядків у цих класах. Дано огляд властивостей трьох класів кривих в узагальненій формі Едвардса. Обговорюються корисні для криптографії властивості скручених кривих Едвардса.

*Ключові слова:* крива в узагальненій формі Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, додавання точок, ізоморфізм, квадратичне кручення, квадратичний лишок, табквадратичний нелишок.

Бібліогр. 07 найм.

UDC 621.391.15: 519.7

Bessalov A.V. **Unique cryptographic properties of acyclic twisted Edwards curves** / A.V. Bessalov // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 1, 2. – P. 49–54.

Analysis of properties of 4th and 8th order points in classes of acyclic twisted and quadratic Edwards curves is given. The theorems of existence of not singular 4th and 8th order points in these classes are proved. Reviewing the properties of three classes of curves in a generalized Edwards form is given. The properties of twisted Edwards curves useful for cryptography are discussed.

*Keywords*: curve in a generalized Edwards form, twisted Edwards curve, quadratic Edwards curve, curve order, point order, addition of points, isomorphism, quadratic twist, quadratic residue, quadratic nonresidue.

Ref.: 07 items.