УДК 681.3.06

А.В. БЕССАЛОВ, д-р техн. наук

МЕТОД НАХОЖДЕНИЯ ПОРЯДКА ТОЧКИ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА

Введение

Эллиптические кривые в форме Эдвардса над простым полем наиболее перспективны для современных криптосистем. В работе [1] показано, что производительность операции экспоненцирования точки такой кривой в среднем не менее чем в 1,5 раза превышает производительность экспоненцирования точки кривой в форме Вейерштрасса. Арифметика этих кривых и ее программирование существенно упрощаются в связи с наличием нейтрального элемента группы как аффинной точки кривой **O** = (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 ранее в [3], – полными кривыми Эдвардса. Мы обнаружили, что кривые в форме Эдвардса разбиты в работе [2] на пересекающиеся классы, в результате чего в статистических таблицах разд. 4 этой работы одни и те же кривые попадают в разные классы, что дает недостоверную статистику.

В работе [4] дан критический анализ некорректных утверждений и классификации кривых в форме Эдвардса, данных в работе [2], и предложили новую их классификацию с разбиением на непересекающиеся классы в зависимости от свойств квадратичности (неквадратичности) параметров a и d.

В данной работе мы даем анализ свойств точек порядков 2, 4, 8 скрученных кривых Эдвардса (по нашей классификации). В разд. 1 предлагается арифметика для групповых операций с особыми точками этих кривых, дан анализ точек малых порядков и формулы, связывающие их с другими точками кривой. В разд. 2 доказана теорема о необходимых и достаточных условиях делимости точки кривой на 2, предложен алгоритм нахождения четырех точек, возникающих при делении точки на 2. В разд. 3 на основе свойств делимости точки на 2 предлагается быстрый метод нахождения порядка точки скрученной кривой Эдвардса почти простого порядка $4n$.

1. Свойства точек малых порядков скрученных кривых Эдвардса

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

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

Наряду с вводом параметра a авторы [2] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{ad}{p}\right) = \pm 1$. При $a = 1$ такая кривая получила в [2] название *кривой Эдвардса*, а если у нее d – квадратичный невычет (т.е. $\left(\frac{d}{p}\right) = -1$), 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

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

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 точек

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

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), $(x_1, y_1) + (x_1, -y_1) = \mathbf{O} = (1, 0)$. 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 две особые точки второго порядка и две или четыре 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

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

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

$$\boldsymbol{D}_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \quad \pm\boldsymbol{F}_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \quad (4)$$

Они возникают в случаях, если символы Лежандра $\left(\frac{ad}{p}\right) = 1$ и $\left(\frac{d}{p}\right) = 1$ соответственно.

Введем арифметику с особыми точками (4) кривой. Так как в наших обозначениях $\infty = \frac{1}{0}$ и $0 = \frac{1}{\infty}$, появление бесконечной координаты в (2) или в (3) равнозначно умножению числителей и знаменателей на 0 или 0^2. При этом остаются лишь слагаемые, являющиеся сомножителями при знаке ∞. Это отвечает правилам обычного предельного перехода. В частности, с помощью закона удвоения (3) легко проверить, что $2\boldsymbol{D}_{1,2} = \mathbf{O}$, $\pm 2\boldsymbol{F}_1 = \boldsymbol{D_0} = (-1, 0)$. Например,

$$2\left(\pm\sqrt{\frac{a}{d}}, \infty\right) = \left(\frac{\frac{a}{d} - a\cdot\infty^2}{1 - \frac{da}{d}\infty^2}, \frac{\pm 2\sqrt{\frac{a}{d}}\infty}{1 + \frac{da}{d}\infty^2}\right) = \left(\frac{0^2\frac{a}{d} - a}{0^2 1 - a}, \frac{0\cdot\left(\pm 2\sqrt{\frac{a}{d}}\right)}{0^2 1 + a}\right) = (1, 0).$$

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 $\mathbf{O}$ и точки 2-го, 4-го и 8-го порядков кривой в форме Эдвардса здесь и далее выделяются жирным шрифтом.

При условии существования вместе с точкой $\boldsymbol{D_0}$ особых точек 2-го порядка из (4), принимая правила предельного перехода в (2), можно найти координаты сумм:

$$\begin{gathered}(x_1, y_1) + (-1, 0) = (-x_1, -y_1), \\ (x_1, y_1) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}}\cdot x_1^{-1}, \frac{1}{\sqrt{ad}}\cdot y_1^{-1}\right), \\ (x_1, y_1) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}}\cdot x_1^{-1}, -\frac{1}{\sqrt{ad}}\cdot y_1^{-1}\right).\end{gathered} \quad (5)$$

Все найденные суммы удовлетворяют уравнению (1) при подстановке, т.е. являются точками кривой. Сумма $(x_1, y_1) + \boldsymbol{D_0} = \boldsymbol{P^*} = (-x_1, -y_1)$ меняет знаки координат точки P, тогда как сложение с особыми точками 2-го порядка инвертирует их с весами. Важно также заметить, что если точка (x_1, y_1) имеет нечетный порядок n, то суммарные с точками 2-го порядка точки (5) имеют порядки $2n$.

Некоторые свойства точек малых порядков были рассмотрены в работе [4]. В данной работе мы рассматриваем кривые в форме (1) при условиях $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$, что в соответствии с классификацией [4] относит их к скрученным кривым Эдвардса. Здесь даем анализ

новых свойств точек 4-го и 8-го порядков для скрученных кривых Эдвардса, имеющих полезные криптографические приложения.

Как следует из (4), эти кривые имеют вместе с точкой $\boldsymbol{D_0}$ еще две особые точки 2-го порядка $\boldsymbol{D_{1,2}}$, и структура кривой становится нециклической. Особых точек 4-го порядка $\pm\boldsymbol{F_1}$ и точек на оси y $\pm\boldsymbol{F_0}$ скрученные кривые Эдвардса не содержат. Вместе с тем при $p \equiv 3 mod 4$ на этой кривой всегда существуют четыре не особые точки 4-го порядка.

Теорема 1.1. *Точки 4-го порядка скрученной кривой в форме* (1) *существуют тогда и только тогда, когда выполняются условия*:

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

Доказательство. Необходимость. Особых точек $\pm\boldsymbol{F_1} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ из (4) кривая не содержит. 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 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 $(1 + d x_1^2 y_1^2) = 0, \Rightarrow x_1^2 + a y_1^2 = 0, \Rightarrow x_1^2 = -a y_1^2$. Из $x_1 \neq 0$ следует $y_1 \neq 0$. Согласно первому из уравнений и равенству $x_1^2 = -a y_1^2$ имеем

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

Итак, получаем четыре точки с координатами:

$$\pm\boldsymbol{F_2} = \left(\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right), \; \pm\boldsymbol{F_3} = \left(-\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right). \tag{6}$$

Необходимыми условиями существования таких точек являются условия (i) и (ii) теоремы. Действительно, при $\left(\frac{a}{p}\right) = -1$ равенство $x_1^2 = -a y_1^2$ справедливо лишь при $p = 3 mod 4$, так как в этом случае элемент (-1) есть квадратичный невычет [5], 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 $p \equiv 3 mod 4$. 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 два решения для вторых координат в точках (6). 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 четыре 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 (6) точки есть точки 4-го порядка. Это доказывает достаточность условий теоремы. Теорема доказана.

Важным следствием теоремы 1.1 является то, что для скрученных кривых с выполнением (i) при $p \equiv 1 mod 4$ точек 4-го порядка не существует. Порядок любой скрученной кривой в этих условиях равен $4n$ при нечетном n.

Точки $\pm\boldsymbol{F_{2,3}}$ можно рассматривать как точки деления на 2 точек 2-го порядка $\boldsymbol{D_{1,2}}/2$ [6]. Из теоремы 1.1 следует, что при $p \equiv 1 mod 4$ на скрученной кривой Эдвардса этих точек не существует.

Например, для кривой $x^2 - y^2 = (1 + 2x^2y^2)\mathrm{mod}11$ (здесь $a = -1$ и $d = 2$ – квадратичные невычеты при $p = 11$) точки 4-го порядка имеют координаты $\boldsymbol{F}_{2,3} = (\pm 2, \pm 2)$. При удвоении согласно (3) получим $2\boldsymbol{F}_2 = (4, \infty) = \boldsymbol{D}_1$. Порядок этой кривой $N_E = 16$, группа точек нециклическая с типом T = (2, 2^3). Она содержит кроме точек **O**, $\boldsymbol{D}_{0,1,2}$, $\pm\boldsymbol{F}_{2,3}$, 8 точек 8-го порядка $(\pm 3, \pm 1)$ $(\pm 5, \pm 4)$.

Найдем условия существования точек 8-го порядка скрученной кривой, порожденных делением на две точки $\boldsymbol{F}_2$.

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

i. $\left(\frac{a}{p}\right) = -1$, $\left(\frac{d}{p}\right) = -1$, ii. $\left(\frac{\sqrt{da^{-1}}}{p}\right) = 1$, $\left(\frac{1+\sqrt{da^{-1}}}{p}\right) = 1$, iii. $p \equiv 3 \bmod 4$.

Доказательство.

Пусть **S** = (x_1, y_1) – точка 8-го порядка, тогда $2\boldsymbol{S}_1 = \boldsymbol{F}_2 = \left(\sqrt[4]{\frac{a}{d}}, \sqrt{\frac{-1}{\sqrt{ad}}}\right)$ – точка 4-го порядка на оси y. Согласно (3) и координат $\boldsymbol{F}_0$ имеем

$$\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2} = \sqrt[4]{\frac{a}{d}}, \qquad \frac{2x_1y_1}{1 + dx_1^2y_1^2} = \sqrt{\frac{-1}{\sqrt{ad}}} = Y. \tag{7}$$

Обозначим $V = x_1y_1$. Тогда второе уравнение в (7) с учетом (1) можно записать в виде двух квадратных уравнений:

$$dV^2 - 2Y^{-1}V + 1 = 0, \quad aV^2 - 2Y^{-1}V + 1 = 0$$

Их дискриминанты после подстановки Y^2 из (7):

$$\Delta_1 = 4\sqrt{ad}\left(1 + \sqrt{\frac{d}{a}}\right), \quad \Delta_2 = 4\sqrt{ad}\left(1 + \sqrt{\frac{a}{d}}\right).$$

Оба дискриминанта являются квадратичными вычетами в условиях теоремы 1.2. Теорема доказана.

При поиске кривых в обобщенной форме Эдвардса с минимальным четным кофактором 4 порядка кривой следует исключать кривые, для которых выполняются оба условия теоремы 1.1.

Утверждение 1.1. *Для скрученных кривых Едвардса* с условиями (i) теоремы 1.1 *при* $p \equiv 1 \bmod 4$ *все кривые имеют порядок* $N_E = 4n$, *а при* $p \equiv 3 \bmod 4$ – порядок $N_E = 2^m n$, $m > 2$, $n \equiv 1 \bmod 2$.

Доказательство. В условиях (i) теоремы 1.1 при $p \equiv 1 \bmod 4$ кривая не содержит точек 4-го порядка, но включает нециклическую подгруппу 4-го порядка точек 2-го порядка $\mathbf{G}_4 = \{\mathbf{O}, \boldsymbol{D}_0, \boldsymbol{D}_1, \boldsymbol{D}_2\}$. Следовательно, порядки всех других точек могут быть равными лишь n и $2n$ (вместе с возможными нечетными сомножителями n). Итак, подгруппа $\mathbf{G}_4$ есть подгруппа минимального четного порядка 4 кривой, и порядок кривой $N_E = 4n$.

При $p \equiv 3 \bmod 4$ возникают четыре точки 4-го порядка (6) и на кривой существуют 2 циклические подгруппы 4-го порядка $\mathbf{G}_4'$, $\mathbf{G}_4''$ с генераторами $\boldsymbol{F}_2$ и $\boldsymbol{F}_3$. (причем $2\boldsymbol{F}_2 = \boldsymbol{D}_1$ и $2\boldsymbol{F}_3 = \boldsymbol{D}_2$). Тогда если $\mathbf{G}_2 = \{\mathbf{O}, \boldsymbol{D}_0\}$, то любая кривая содержит подгруппу $\mathbf{G}_8 = \mathbf{G}_2 \oplus \mathbf{G}_4'$ 8-го порядка. Порядок такой кривой с минимальным четным кофактором $N_E = 8n$. При наличии также точек 8-го порядка он станет равным $N_E = 16n$, при наличии точек 16-го порядка $N_E = 32n$, и т.д. Доказательство завершено.

В приведенном выше примере кривой $x^2 - y^2 = (1 + 2x^2y^2)\mathrm{mod}11$, имеющей восемь точек 8-го порядка, порядок $N_E = 16$. Для точек 8-го порядка выполняются условия теоремы 1.2. Кривая же $x^2 - y^2 = (1 + 3x^2y^2)\mathrm{mod}7$ с точками до 4-го порядка имеет порядок $N_E = 8$.

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 [4].

2. Необходимые и достаточные условия делимости точки скрученной кривой Эдвардса на 2

Задача деления точки на 2 на полной кривой Эдвардса, обратная удвоению, рассматривалась в работах [6, 7]. Здесь приводим ее решение для скрученной кривой Эдвардса с параметрами $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$.

Пусть $P = (x_1, y_1)$, и $2P = R = (X,Y)$. В этом случае можно записать обратную удвоению (3) точки операцию деления точки на 2 как $(X, Y)/2 = P$. Для нециклической скрученной кривой с тремя точками 2-го порядка существуют еще три решения операции деления на 2: $(X, Y)/2 \in \{P + D_0, P + D_1, P + D_2\}$. Ясно, что удвоение этих точек дает один результат $2P$. Деление на 2 точки аддитивной группы имеет аналогию с извлечением корня квадратного из элемента мультипликативной группы поля характеристики $p \neq 2$, однако вместо двух квадратных корней здесь появляется четыре корня.

Воспользуемся формулой удвоения (3). Исключим из рассмотрения 2 точки кривой (1) с нулевой y-координатой: нуль группы $\mathbf{O} = (1,0)$ и точку 2-го порядка $\boldsymbol{D} = (–1, 0)$. На оси y (при $x = 0$) точек скрученной кривой Эдвардса не существует. Согласно (1) вторую координату Y в (3) можно выразить формулами:

$$\frac{2x_1y_1}{x_1^2+ay_1^2} = Y, \qquad \frac{2x_1y_1}{1+dx_1^2y_1^2} = Y.$$

Обозначим $Z = y_1/x_1 \neq 0$, $V = y_1x_1 \neq 0$. Тогда с учетом введенных обозначений для любой точки P кривой, не лежащей на окружности радиуса 1, одновременно справедливы два квадратных уравнения:

$$aZ^2 - 2Y^{-1}Z + 1 = 0, \qquad dV^2 - 2Y^{-1}V + 1 = 0, \; X, Y \neq 0,1 \tag{8}$$

с дискриминантами:

$$\Delta_1 = 4Y^{-2}(1 - aY^2), \quad \Delta_2 = 4Y^{-2}(1 - dY^2), \tag{9}$$

и решениями:

$$Z_{1,2} = (aY)^{-1}(1 \pm \sqrt{1 - aY^2}), \quad V_{1,2} = (dY)^{-1}(1 \pm \sqrt{1 - dY^2}). \tag{10}$$

Эти решения имеют свойства:

$$Z_1Z_2 = a^{-1}, \quad V_1V_2 = d^{-1}. \tag{11}$$

В частности, для скрученной кривой с параметрами $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$ одно из решений в (10) всегда есть квадратичный вычет, а другое – квадратичный невычет. Далее в соответствии с (11) полагаем, что Z_1 и V_1 – квадратичные вычеты (соответственно, Z_2 и V_2 – квадратичные невычеты).

Изложенное позволяет сформулировать и доказать следующую теорему.

Теорема 2.1. *Для любой точки (X,Y) скрученной кривой Эдвардса* с параметрами $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$ *и координатой $Y \neq 0$ существуют четыре точки деления на* 2 $(X,Y)/2 \in \{P, P + D_{0,1,2}\}$ *тогда и только тогда, когда выполняются условия*

(ii)

$$\text{(i)} \quad \left(\frac{1-aY^2}{p}\right) = 1, \quad \text{(ii)} \quad V_1(Z_1 - Y) = XZ_1(V_1 - Y).$$

При невыполнении любого из них точка (X,Y) на 2 *не делится.*

Доказательство.

Необходимость. Удвоение любой точки $(x_1, y_1) = P$ согласно закону (3) порождает единственную точку $2P = (X,Y)$, причем координаты точек P и $2P$ являются решениями двух квадратных уравнений (8) в поле $\boldsymbol{F}_p$. Как следует из (9), необходимым условием существования решения первого из уравнений (8) является то, что элемент поля $(1 - aY^2)$ есть ненуле-

вой квадрат в этом поле, т.е. $\left(\frac{1-aY^2}{p}\right) = 1$. Это доказывает необходимость условия (i) теоремы. Это условие определяется лишь одной координатой точки (X,Y). Из (1) очевидно, что кривая имеет две точки $(+X,Y)$, из которых равенство $2P = (X,Y)$ справедливо лишь для одной. Тогда согласно (3) на основе вычисленных по формулам (10) значений Z_1 и V_1 получим

$$\frac{x_1^2 - ay_1^2}{(1-dx_1^2y_1^2)} = X \;\Rightarrow\; \frac{x_1^2(1-aZ_1^2)}{1-dV_1^2} = X \;\Rightarrow\; \left(\frac{V_1}{Z_1}\right)\frac{1-aZ_1^2}{1-dV_1^2} = X. \qquad (12)$$

Из уравнений (10) справедливы равенства:

$$aZ_1^2 - 1 = 2(Z_1Y^{-1} - 1), \qquad dV_1^2 - 1 = 2(V_1Y^{-1} - 1).$$

Тогда вместо (12) можно записать

$$V_1(Z_1 - Y) = XZ_1(V_1 - Y).$$

Последнее равенство определяет второе необходимое условие (ii) теоремы. По сути оно позволяет при выполнении условия (i) определить уникальное значение координаты X точки, которая делится на 2.

Достаточность. Пусть для координат точки $R = (X,Y)$ выполняются условия теоремы. Так как уравнение (1) можно записать в форме $(1 - aY^2) = X^2(1 - dY^2)$, то для любой точки из условия $\left(\frac{1-aY^2}{p}\right) = 1$ следует $\left(\frac{1-dY^2}{p}\right) = 1$. Итак, при выполнении условия (i) теоремы существуют все четыре решения (10), из которых Z_1 и V_1 – квадратичные вычеты, а Z_2 и V_2 – квадратичные невычеты. Тогда существуют решения для квадратов $y_{1,2}^2 = Z_{1,2}V_{1,2}$, $x_{1,2}^2 = \frac{V_{1,2}}{Z_{1,2}}$ координат точек $R/2$. Их корни порождают восемь точек $(\pm x_1, \pm y_1)$, $(\pm x_2, \pm y_2)$. Из них только для четырех точек справедливы равенства $x_1y_1 = V_1$, $x_2y_2 = V_2$, при выполнении которых отбираются точки $\mathrm{P}_1 = (x_1,y_1)$, $\mathrm{P}_1^* = (-x_1,-y_1)$, $\mathrm{P}_2 = (x_2,y_2)$, $\mathrm{P}_2^* = (-x_2,-y_2)$. Тот же результат можно получить с помощью равенств $Z_i = y_i/x_i$ $i = 1,2$. Как следует из (5), точки P_i и P_i^* связаны точкой D_0, а точки P_1 и P_2 – точкой D_1 или D_2. Итак, при выполнении условия (i) теоремы существуют четыре точки деления на 2:

$$\{\mathrm{P}_1 = (x_1,y_1),\ \mathrm{P}_1^* = (-x_1,-y_1),\ \mathrm{P}_2 = (x_2,y_2),\ \mathrm{P}_2^* = (-x_2,-y_2)\}.$$

Удвоение любой из них дает уникальную точку $2P_i = 2P_i^* = (X,Y), i = 1,2$. Условие (ii) теоремы, записанное для точек $\mathrm{P}_1 = (x_1,y_1)$, является достаточным, так как его выполнение тождественно выполнению такого условия для всех четырех точек. При $\left(\frac{1-aY^2}{p}\right) = -1$ оба уравнения (8) решений в поле $\mathbf{F}_p$ не имеют и точек деления на 2 не существует. При проверке второго условия теоремы точка $(-X,Y)$, удовлетворяющая условию (i), но не отвечающая условию (ii), также на 2 не делится. Теорема доказана.

Утверждение 2.1. *Для скрученной кривой Эдвардса порядка* $4n$ *с простым* n *на* 2 *делятся лишь точки подгруппы* $\langle G\rangle$ *порядка* n*, причем одна из точек* $\frac{G}{2}$ *имеет порядок* n*, и три точки – порядок* $2n$.

Доказательство. Нециклическая скрученная кривая Эдвардса с тремя точками второго порядка содержит ровно $(n - 1)$ точек простого порядка n и $3(n - 1)$ точек порядка $2n$. Следовательно, существуют ровно три точки порядка $2n$, удвоение которых даст уникальную точку подгруппы $\langle G\rangle$ порядка n. В подгруппе $\langle G\rangle$ простого порядка n деление на две точки тождественно умножению точки на единственный элемент $2^{-1} = \frac{n+1}{2}$ поля F_n, что порождает при делении на две точки порядка n одну точку порядка n. Утверждение доказано.

В следующей теореме определяется новое свойство обеих координат точки скрученной кривой Эдвардса.

Теорема 2.2. *Для любой точки* (x_1, y_1) *кривой* (1) *справедливо равенство* $\left(\frac{1-x_1^2}{p}\right)\left(\frac{1-ay_1^2}{p}\right) = \left(\frac{a-d}{p}\right)$.

Доказательство.

Для точки (x_1, y_1) с учетом определения (1) запишем произведение

$$(1 - x_1^2)(1 - ay_1^2) = 1 - x_1^2 - ay_1^2 + ax_1^2y_1^2 = (a - d)x_1^2y_1^2 .$$

Отсюда сразу следует, что произведение $(1 - ay_1^2)(1 - x_1^2)$ является квадратичным невычетом при $\left(\frac{a-d}{p}\right) = -1$ и наоборот, что и доказывает утверждение теоремы.

Данная теорема позволяет заменить тестирование величины $(1 - aY^2)$ тестированием значения $(1 - X^2)$ точки (X,Y).

3. Метод определения порядков точек скрученной кривой Эдвардса

В криптосистемах приемлемыми являются кривые Эдвардса с минимальным кофактором 4-го порядка кривой $N = 4n$, где n – достаточно большое простое число. Такое значение N называют почти простым числом. Для скрученных кривых Эдвардса все кривые имеют минимальный кофактор 4 при $p \equiv 1 \bmod 4$, остается лишь подобрать кривую с простым значением n. Далее полагаем, что n – простое число. Особенностью этих кривых является то, что максимальный порядок точки равен $2n$ вместо $4n$ для циклических кривых. Вместе с тем, число точек порядка $2n$ втрое больше, чем порядка n. Для нахождения генератора криптосистемы как точки $G = 2P$ достаточно удвоить любую (кроме точек $\boldsymbol{D}_i$) случайную точку кривой, что требует выполнения одной групповой операции. Альтернативным является метод, основанный на свойстве делимости точки на 2.

Согласно утверждению 2.1, для точек максимального порядка $2n$ кривой Эдвардса не существует точек деления на 2, но они существуют для точек порядка n. Другими словами, если для случайной точки $\boldsymbol{R} = (X,Y)$ не выполняется условие (i) теоремы 2.1, то порядок такой точки равен $2n$. В противном случае (с вероятностью 1/2) порядок точки равен n или $2n$. При выполнении обоих условий теоремы 2.1 порядок точки равен n. Ее можно принять в качестве генератора G криптосистемы.

Таким образом, для определения порядка точек скрученной кривой Эдвардса вовсе не требуется выполнять сложную операцию скалярного произведения $n\boldsymbol{R}$, что рекомендуется существующими стандартами. Точка (X,Y) максимального порядка $2n$ определяется лишь одним условием

$$\left(\frac{1-aY^2}{p}\right) = -1.$$

С учетом теоремы 2.2 это условие можно упростить:

$$\left(\frac{1-X^2}{p}\right) = -\left(\frac{a-d}{p}\right). \qquad (13)$$

Итак, вместо в среднем $1.5\log(n)$ групповых операций удвоения и сложения при вычислении скалярного произведения $n\boldsymbol{R}$ [5], со сложностью порядка 10 операций в поле каждая, требуется выполнить всего две полевые операции: возведение в квадрат S и нахождение символа Лежандра. Большой выигрыш в экономии вычислений очевиден. Этот же метод для полных кривых Эдвардса описан в работе [7].

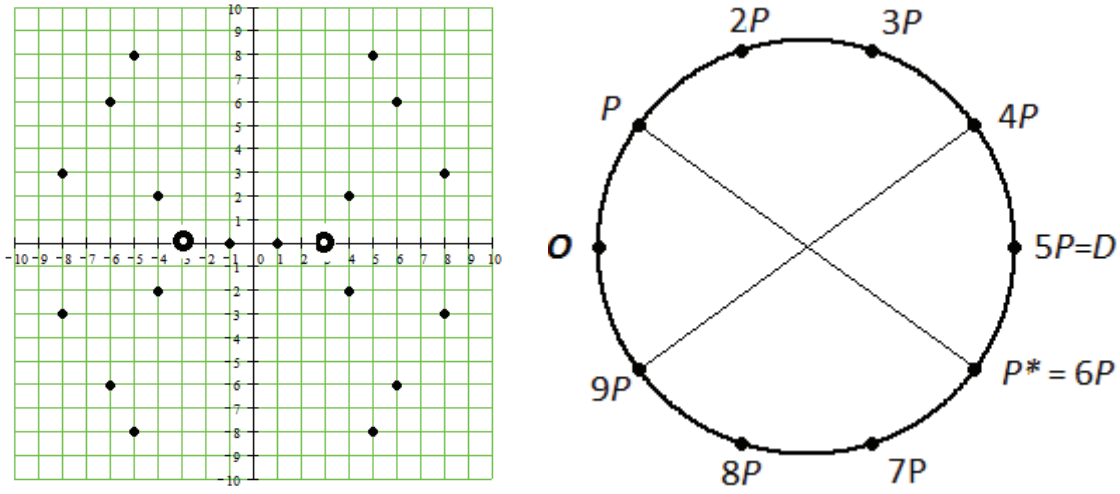
Для определения генератора G криптосистемы как точки скрученной кривой Эдвардса порядка n вместо условия (i) теоремы 2.1 по аналогии с (13) справедливо

$$\left(\frac{1-X^2}{p}\right) = \left(\frac{a-d}{p}\right).$$

Тестирование второго условия (ii) теоремы 2.1 требует дополнительных вычислительных затрат в соответствии с формулами (10) вместе с тремя умножениями M в формуле (ii). Эти затраты превосходят сложность удвоения точки (3M+4S) [1], поэтому для скрученных

кривых Эдвардса генератор G целесообразно вычислять одной групповой операцией удвоения случайной точки кривой. И в этом случае выигрыш в производительности вычислений достигает огромных значений. Например, при длине модуля 400 бит экспоненцирование точки [5] требует в среднем 600 групповых операций (400 удвоений и 200 сложений), тогда замена этой процедуры одним удвоением дает выигрыш в экономии вычислений более чем в 600 раз. Этот выигрыш пропорционален длине модуля.

Пример. При p = 17 скрученная кривая Эдвардса $x^2 + 3y^2 = 1 + 6x^2y^2$ имеет порядок N_E = 20 (здесь a = 3 и d = 6 – квадратичные невычеты). Кривая отвечает условиям теоремы 1.1, имеет три точки 2-го порядка $\boldsymbol{D_0 = (-1,0)}$, $\boldsymbol{D_1 = (3,\infty)}$ и $\boldsymbol{D_2 = (-3,\infty)}$ и не имеет точек 4-го порядка. Она содержит четыре точки 5-го и 12 точек 10-го порядков, рис.1, *а*. Особые точки $\boldsymbol{D_{1,2}}$здесь обозначены кружками. Прямые суммы подгруппы точек 5-го порядка с подгруппами 2-го порядка образуют три подгруппы точек 10-го порядка. Они представлены как точки $\boldsymbol{kP_{1,2}}$ и $\boldsymbol{kP_1^*}$ в таблице. Каждая из них образует одну циклическую подгруппу на колесе точек, рис.1, *б*.



а *б*

Рис.1

	k	1	2	3	4	5	6	7	8	9	10
$\boldsymbol{kP_1}$	x_k	4	–8	–6	–5	–3	–5	–6	–8	4	1
	y_k	2	3	6	–8	∞	8	–6	–3	–2	0
$\boldsymbol{kP_1^*}$	x_k	–4	–8	6	–5	3	–5	6	–8	–4	1
	y_k	–2	3	–6	–8	∞	8	6	–3	2	0
$\boldsymbol{kP_2}$	x_k	5	–8	8	–5	–1	–5	8	–8	5	1
	y_k	–8	3	3	–8	0	8	–3	–3	8	0

Пусть $\boldsymbol{P_1 = (4,2)}$, $\boldsymbol{G = 2P_1 = (-8,3)}$. Точка G имеет 5-й порядок и, как и все четыре точки 5-го порядка, делится на 2, образуя четыре корня 2-й степени $\frac{G}{2} \in \{P_1, P_1 + D_{0,1,2}\}$. Действительно, согласно (11) и условию (i) теоремы 2.1 $\Delta_1 = (1 - 3 \cdot 3^2) = 8$ – квадратичный вычет, тогда и $\Delta_2 = (1 - 6 \cdot 3^2) = 15$ – также квадратичный вычет, и существуют решения (12) $Z_{1,2} = (3)^{-2}(1 \pm 7) \in \{-8, -5\}$, $V_{1,2} = (1 \pm 7) \in \{8, -6\}$. Здесь Z_1 и V_1, – квадратичные вычеты, а Z_2, V_2 – квадратичные невычеты в поле F_{17}. Легко проверить выполнение условия (ii): $8(-8 - 3) = (-8)^2(8 - 3) \Rightarrow 6 = 6$. Определяем далее квадраты $Z_1V_1 = y_1^2 = 4, Z_2V_2 = y_2^2 = 13$, $\frac{V_1}{Z_1} = x_1^2 = 16, \frac{V_2}{Z_2} = x_2^2 = 8$. Отсюда $(\pm x_1, \pm y_1) = (\pm 4, \pm 2)$, $(\pm x_2, \pm y_2) = (\pm 5, \pm 8)$. Из этих восьми точек отбираем четыре точки, для которых $x_1\, y_1 = V_1 = 8$, $x_2\, y_2 = V_2 = -6$, и получаем точки

$P_1 = (4,2)$, $P_1^* = (-4,-2)$, $P_2 = (5,-8)$, $P_2^* = (-5,8)$. Из них три точки 10-го порядка, и одна точка $(-5,8)$ – 5-го порядка. В поле F_5 деление на 2 есть умножение на $2^{-1} = 3$, поэтому данная точка $(-5,8) = 3G$. Это видно и из таблицы, из которой также легко определяются все четыре точки $\frac{G}{2} = \{(4,2),(-4,-2),(5,-8),(-5,8)\}$.

Для нахождения порядка случайной точки, например R=(4,2), согласно (13) вычисляем $(1-4^2) = 2$ – квадратичный вычет. Так как $(a - d) = 3 - 6 = 14$ – квадратичный невычет, условие (i) теоремы 2.1 не выполняется и точка $(4,2)$ имеет порядок $10 = 2n$.

Точки колеса, соединенные диаметральными линиями, связаны как P и $P^* = P + \boldsymbol{D_0}$. Для любой точки семейство из четырех связанных линиями на рис.1, *б* точек лежат на одной окружности на графике кривой рис.1, *а*.

Утверждение 3.1. *Для скрученной кривой Эдвардса почти простого порядка* $4n$ *любое семейство из четырех точек* $(\pm x_1, \pm y_1)$, включающее точку порядка *n, содержит две точки порядка* $2n$, *и две точки порядка* n.

Доказательство. Пусть $\mathrm{Ord}(\pm kP) = n$, тогда пара точек $\pm kP^* = + D_i$ имеют порядок $2n$ как наименьшее общее кратное суммы точек с взаимно простыми порядками. Если $\mathrm{Ord}(\pm kP) = 2n$, то сложение этих точек с точкой $D = nP$ из той же циклической подгруппы порядка $2n$ дает точки $(n \pm k)P$ с четным значением $(n \pm k)$, т.е. точки порядка n. При сложении точек $\pm kP$ порядка $2n$ с точками 2-го порядка из смежных подгрупп образуются точки порядка $2n$. Утверждение доказано.

Несмотря на взаимосвязь четырех точек $(\pm x_1, \pm y_1)$, включающих точки порядка *n,* сложность вычисления дискретного логарифма в подгруппе точек $<G>$ простого порядка *n* не снижается. Как и для кривых в форме Вейерштрасса, она снижается лишь вдвое за счет обратных точек.

Можно заключить, что циклические подгруппы простого порядка *n* скрученных кривых Эдвардса порядка $4n$ при $p \equiv 1 \bmod 4$. приемлемы для использования в криптосистемах. Эти подгруппы обходят особые точки кривой, и в них имеет место универсальность и полнота закона сложения точек. Они удобны для программирования и, как и полные кривые Эдвардса, имеют рекордное быстродействие. Свойства делимости точки на 2 на таких кривых позволяет находить точки заданного порядка в сотни раз быстрее, чем предлагают стандартные алгоритмы.

Список литературы: 1. *Бессалов, А.В., Цыганкова, О.В.* Производительность групповых операций на скрученной кривой Эдвардса над простым полем // Радиотехника. – 2015. – Вып.181. – С.58-63. 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. *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*. Классификация кривых в форме Эдвардса над простым полем // Прикладная радиоэлектроника. – 2015. – Т. 14. №4. – С.197 – 203. 5. *Бессалов, А.В., Телиженко, А.Б.* Криптосистемы на эллиптических кривых : учеб. пособие. – К. : ІВЦ «Політехніка», 2004. – 224с. 6. *Бессалов, А.В.* Деление точки на два для кривой Эдвардса над простым полем // Прикладная радиоэлектроника. – 2013. – Т. 12, №2. – С. 278-279. 7. *Бессалов, А.В., Цыганкова, О.В.* Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем // Проблемы передачи информации. – 2015. – Т. 51, вып 4. – С.92-98.

НТТУ «Киевский политехнический университет» *Поступила в редколлегию 09.09.2016*