УДК 681.3.06

А.В. БЕССАЛОВ, О.В. ЦЫГАНКОВА

НОВЫЕ СВОЙСТВА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В ФОРМЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Введение

Элиптические кривые в форме Эдвардса [1] сегодня без сомнения являются наиболее быстрыми и перспективными для использования в асимметричных криптосистемах. Введенный Эдвардсом в этой работе закон сложения точек при всех его преимуществах оказался не вполне удобным для специалистов по эллиптической криптографии, привыкших к горизонтальной симметрии обратных точек. Авторы статьи сочли целесообразным внести коррективы в этот закон с целью унификации определения обратных точек, общепринятого в теории эллиптических кривых над простым полем.

Двойная симметрия точек кривой Эдвардса относительно координатных осей влечет за собой чрезвычайно интересные и удобные свойства этих кривых. Исключая бесполезные изоморфные кривые, в кривых Эдвардса достаточно использовать один параметр d вместо обычных двух параметров a и b классической кривой в канонической форме. Занимаясь проблемой деления точки кривой на 2, обратной удвоению точки, авторы обнаружили простое условие для точек максимального порядка кривой. Оно формулируется и доказывается в теореме 1. При изучении свойств кривых были также найдены нетривиальные вырожденные пары кривых кручения, порождающие суперсингулярные кривые с порядком $p + 1$. В работе сформулирована и доказана теорема 2 об условиях существования таких пар кривых кручения. Доказаны также 2 утверждения о порядках точек кривой. Далее мы показали на примере, что знание всего 1/8 части точек кривой Эдвардса позволяет реконструировать все остальные точки этой кривой, заданные скалярным произведением kP. Правда, такая возможность не упрощает проблемы дискретного логарифмирования для точек простого порядка.

Среди общесистемных параметров криптосистемы на эллиптических кривых важнейшим элементом является ее генератор как точка достаточно большого простого порядка n. При использовании кривых в форме Эдвардса над простым полем порядок кривой $N_E = 4n$ [1 – 3]. После нахождения случайной точки $Q = (x_Q, y_Q)$ кривой генератор криптосистемы порядка n нетрудно найти как точку $G = (x_G, y_G) = 4Q$, для чего потребуется два удвоения (т.е. две групповые операции). В данной работе мы показываем, что задача нахождения генератора решается проще – одной операцией в поле и одним удвоением в группе точек.

Идея и метод определения порядков точек кривых Эдвардса рассматривались в предыдущей работе [4]. Для этого мы привлекали решение задачи, обратной удвоению точки: деление точки на 2. В настоящей статье мы приводим новое решение этой задачи и доказываем необходимое и достаточное условие делимости точки на 2. Это условие позволило сформировать простой алгоритм вычисления точек требуемого порядка для использования в криптосистемах.

1. Модификация закона сложения точек кривой Эдвардса

Эдвардс в своей пионерской работе [1] впервые определил унифицированный закон сложения точек эллиптической кривой

$$x^2 + y^2 = e^2(1 + dx^2y^2) \tag{1}$$

над любым полем характеристики $p \neq 2$ следующей формулой

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{e(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - dx_1x_2y_1y_2)}\right). \tag{2}$$

Для формы (1) кривой уже не надо рассматривать два случая сложения для различных и совпадающих точек, что приходится делать для кривой в форме Вейерштрасса [5]. Здесь при совпадении точек закон удвоения точки становится частным случаем (2)

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

Другим важным преимуществом формы кривой (1) является замена точки на бесконечности аффинной точкой O = (0, e) как нейтрального элемента абелевой группы точек. Легко проверить согласно (2), что $(x_1,y_1) + (0, e) = (x_1,y_1)$. На осях x и y находятся еще три базовых точки: точка 2-го порядка $D = (0, -e)$ и две точки 4-го порядка $\pm F = (\pm e, 0)$, таких что $2F = D$, $2D = O$. Если $P = (x_1, y_1)$, то обратная точка $-P = (-x_1, y_1)$ и в соответствии с (2) $(x_1,y_1) + (-x_1,y_1) = O$. Здесь имеет место вертикальная симметрия обратных точек относительно оси y.

Для сохранения преемственности с кривыми в форме Вейерштрасса, где обратные точки $\pm P = (x_1, \pm y_1)$ симметричны относительно горизонтальной оси x, авторы предлагают модификацию закона Эдвардса (2) сложения точек. Она сводится к повороту вправо на $\pi/2$ всех точек кривой (1). Модифицированный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - y_1y_2}{e(1-dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{e(1+dx_1x_2y_1y_2)}\right). \tag{4}$$

Определяя теперь обратные точки как $\pm P = (x_1, \pm y_1)$, получим согласно (4) $(x_1, y_1) + (x_1, -y_1) = \mathbf{O} = (e, 0)$. Сложение точки с нулем группы дает $(x_1, y_1) + (e, 0) = (x_1, y_1)$. Итак, координаты базовых точек для закона (4), которые мы выделим жирным шрифтом, равны: $\mathbf{O} = (e, 0)$, точка 2-го порядка $\boldsymbol{D} = (-e, 0)$, точки 4-го порядка $\pm \boldsymbol{F} = (0, \pm e)$. Удвоение точки в соответствии с (4) принимает вид

$$2(x_1, y_1) = \left(\frac{x_1^2 - y_1^2}{e(1-dx_1^2y_1^2)}, \frac{2x_1y_1}{e(1+dx_1^2y_1^2)}\right). \tag{5}$$

Легко проверить, что $\pm 2\boldsymbol{F} = \boldsymbol{D} = (-e, 0)$ и $2\boldsymbol{D} = \mathbf{O} = (e, 0)$. Использование модифицированных законов (4), (5) позволяет возвратиться к горизонтальной симметрии (относительно оси x) обратных точек, общепринятой в теории эллиптических кривых.

Так как любая ненулевая константа e в форме (1) кривой дает изоморфную кривую над простым полем, мы в дальнейшем принимаем $e = 1$. Второй параметр d этой кривой является квадратичным невычетом простого поля, т.е.символ Лежандра для него $\left(\frac{d}{p}\right) = -1$ [2, 3].

Следует заметить, что каждая не базовая точка (x_1, y_1) порождает сімейство из 8 точек $(\pm x_1, \pm y_1), (\pm y_1, \pm x_1)$, лежащих симметрично на одной окружности (по 2 в каждом квадранте). Все они связаны между собой через 3 базовых точки: $\boldsymbol{D}$ и $\pm\boldsymbol{F}$. По формуле (4) имеем: $P + \boldsymbol{D} = (x_1, y_1) + (-1, 0) = (-x_1, -y_1) = P^*$, $P + \boldsymbol{F} = (x_1, y_1) + (0, 1) = (-y_1, x_1)$, $P - \boldsymbol{F} = (x_1, y_1) + (0, -1) = (y_1, -x_1)$ или иначе $(x_1, y_1) + (y_1, x_1) = \boldsymbol{F}$. Остальные 4 точки семейства формируются аналогично обратной точкой $-P$.

Рассмотрим далее ряд новых свойств кривых (1) в форме Эдвардса.

2. Необходимое и достаточное условие делимости точки кривой Эдвардса на два

Пусть $P = (x_1, y_1)$ и $2P = (a,b)$. В этом случае можно записать обратную удвоению операцию деления точки на 2 как $(a,b)/2 = P$. Вторым решением операции деления на 2 будет точка $(a,b)/2 = P + \boldsymbol{D}$, где $\boldsymbol{D}$ – точка 2-го порядка. Согласно (5) $P + \boldsymbol{D} = (-x_1, -y_1) = P^*$. Ясно, что удвоение этих двух точек дает один результат $2P = 2P^*$. Деление на 2 точки аддитивной группы имеет аналогию с извлечением корня квадратного из элемента мультипликативной группы поля характеристики $p \neq 2$. С этими операциями связаны родственные проблемы дискретного логарифмирования [5].

Воспользуемся формулой удвоения (5) при $e = 1$. Исключим из рассмотрения 4 базовые точки кривой (1), лежащие на окружности радиуса 1: нуль группы $\mathbf{O} = (1,0)$, точку 2-го порядка $\boldsymbol{D} = (-1, 0)$ и 2 точки 4-го порядка $(0, \pm 1)$. Обозначим $X = x_1^2$, $Y = y_1^2$, $Z = Y/X$, $V =$

XY, X,Y $\neq$ 0. Заменим знаменатели в (5) на 2 – X – Y и X + Y соответственно. Согласно (1) и второй координаты (5) для одной точки P кривой, не лежащей на окружности радиуса 1, одновременно справедливы два квадратных уравнения

$$Z^2 - 2b^{-1}Z + 1 = 0, \qquad dV^2 - 2b^{-1}V + 1 = 0,\ b \neq 0{,}1 \tag{6}$$

с дискриминантами

$$\Delta_1 = 4b^{-2}\,(1 - b^2),\ \Delta_2 = 4b^{-2}\,(1 - db^2), \tag{7}$$

и решениями

$$Z_{1,2,} = b^{-1}(1 \pm \sqrt{1-b^2}),\ V_{1,2,} = (bd)^{-1}\,(1 \pm \sqrt{1-db^2}). \tag{8}$$

Изложенное позволяет сформулировать и доказать следующую теорему.

Теорема 1. *Для любой точки (a,b) кривой Эдвардса (1), не лежащей на окружности радиуса 1, существуют 2 точки деления* $(a,b)/2 = \{P,\ P+\boldsymbol{D}\}$ *тогда и только тогда, когда* $\left(\frac{1-b^2}{p}\right) = 1$. *При* $\left(\frac{1-b^2}{p}\right) = -1$ *точка* (a,b) *на* 2 *не делится.*

Доказательство.

Необходимость. Удвоение любой точки P с ненулевыми координатами согласно закону (5) порождает единственную точку $2P = (a,b)$, причем координаты точек P и $2P$ являются решениями двух квадратных уравнений (6) в поле $\mathbf{F}_p$. Необходимым условием существования решения первого из уравнений (6), как следует из (5), является то, что элемент поля $(1 - b^2)$ есть ненулевой квадрат в этом поле или $\left(\frac{1-b^2}{p}\right) = 1$. При выполнении этого условия кроме точки P, для которой $2P = (a,b)$, существует еще одна точка $P^* = P + D = = (-x_1, -y_1)$, для которой $2P^* = 2P + 2D = (a,b)$, так как $2D = O$. При $\left(\frac{1-b^2}{p}\right) = -1$ уравнение (6) решений в поле не имеет. Необходимость условия теоремы доказана.

Достаточность. Для любой не лежащей на единичной окружности точки P кривой (1), для которой имеет место равенство (3), справедливы оба тождества (4). Достаточно потребовать, чтобы один из дискриминантов (5) был квадратичным вычетом, из этого сразу следует, что и второй дискриминант является квадратом. Действительно, пусть (a,b) – точка кривой (1). Тогда равенство $a^2 + b^2 = 1 + da^2b^2$ можно записать как $(1 - b^2) = a^2(1 - db^2)$. Отсюда очевидно, что для любой точки (a,b) кривой обе величины $(1 - b^2)$ и $(1 - db^2)$ либо являются квадратичными вычетами, либо – невычетами. В первом случае существуют две точки деления $(a,b)/2$, во втором – нет.

Достаточность условия теоремы доказана.

При невыполнении условия теоремы для точки (a,b) точек ее деления на 2 $(a,b)/2$ не существует. Это свойство позволяет без групповых операций находить точки максимального порядка $4n$ кривой Эдвардса.

Для 4-х базовых точек кривой Эдвардса $\mathbf{O} = (1,0)$, точки 2-го порядка $\boldsymbol{D} = (-1, 0)$ и точек 4-го порядка $(0,\pm1)$ на 2 делится обычно лишь точка $\boldsymbol{D}$, так что $\boldsymbol{D}/2 = \pm\mathbf{F}$ (или $\pm 2\mathbf{F} = \boldsymbol{D}$). Если кривая не имеет точек 8-го порядка, то точки $\pm\mathbf{F}$ не делятся на 2, в противном случае нетрудно получить 4 точки 8-го порядка с координатами $(\pm c, \pm c)$, где c есть решение биквадратного уравнения $dc^4 - 2c^2 + 1 = 0$ [3].

Определение координат точек деления на два рассмотрено в предыдущей работе [4]. Заметим, что при выполнении условия теоремы по формулам (8) можно найти все решения квадратных уравнений (6), после чего определяются квадраты для координат точек деления на 2

$$X = (V_{1,2}/Z_{1,2}),\ Y = (V_{1,2}Z_{1,2}). \tag{9}$$

В отличие от работы [4] , мы здесь используем лишь одну координату b точки (a,b), которая делится на два, с отбором квадратичных вычетов в (9). Результатом должны быть две точки $P = (x_1, y_1)$ и $P^* = (-x_1, -y_1)$, для которых $2P = 2P^* = (a,b)$. В силу симметрии первого из уравнений (6) для X и Y их значения могут поменяться местами, что требует проверки результата обратным удвоением.

3. Вырожденные пары кривых кручения

Переход к кривой кручения для формы (1) Эдвардса осуществляется простой заменой $d \to d^{-1}$ [2, 3], тогда порядки этих кривых $N_E = p + 1 \pm t$. Для вырожденной пары кривых кручения параметр $t = 0$, порядок обеих кривых совпадает и равен $N_E = p + 1$. Такая кривая относится к классу криптографически слабых суперсингулярных кривых. Этот случай возможен лишь при $p \equiv 3\bmod 4$, так как только тогда $4|(p + 1)$. Очевидным случаем вырожденной пары кручения является значение параметра кривой $d = -1$. Элемент (-1) при $p \equiv 3\bmod 4$ является квадратичным невычетом [5], т.е. допустимым параметром кривой (1). Так как при этом $d = d^{-1}$, уравнение кривой (1) $x^2 + y^2 = 1 - x^2y^2$ не изменяется, и пара кривых кручения вырождается в одну кривую.

Авторы обнаружили еще один нетривиальный пример вырожденной пары кручения для кривой Эдвардса. Докажем следующую теорему.

Теорема 2. *При* $p \equiv 3\bmod 4$ *и* $p \equiv \pm 3\bmod 8$ *пара кривых кручения в форме Эдвардса над простым полем с параметрами* $d = 2$ и $d^{-1} = 2^{-1}$ *является вырожденной с порядком* $N_E = p + 1$.

Доказательство.

Первое условие теоремы обсуждалось выше и связано с делимостью порядка кривой на 4. При выполнении второго условия элемент 2 поля F_p является квадратичным невычетом, т.е. $\left(\frac{2}{p}\right) = -1$ [5], и он принадлежит к допустимым значениям параметра d. Требуется доказать, что при $d = 2$ оба уравнения пары кривых кручения имеют одинаковый порядок $p + 1$.

Для всех точек кривой (1), кроме двух базовых точек **O** и ***D*** с координатами $x = \pm 1$, $y = 0$, можно записать равенство

$$y^{-2} = \frac{dx^2-1}{x^2-1} = d + (d-1)V^{-1}, \quad V = x^2 - 1. \tag{10}$$

Для кривой кручения после замены $y \to v$ и $d \to d^{-1}$ имеем

$$v^{-2} = \frac{d^{-1}x^2-1}{x^2-1} = d^{-1} + (d^{-1}-1)V^{-1}.$$

Умножив последнее равенство на $(-d)$, получим

$$-dv^{-2} = -1 + (d-1)V^{-1}, \tag{11}$$

причем в левой части имеем квадрат, так как $(-d)$ – квадратичный вычет (а (-1) – квадратичный невычет). В тривиальном случае вырожденной пары кручения при $d = -1$ уравнения (10) и (11) совпадают. При $d = 2$ эти уравнения имеют вид:

$$y^{-2} = 2 + V^{-1}, \qquad V = x^2 - 1, \tag{12}$$

$$-2v^{-2} = -1 + V^{-1}. \tag{13}$$

Покажем, что оба уравнения дают одинаковое число решений. При всех $x^2 \neq 1$ переменная V^{-1} пробегает всевозможные ненулевые значения из множества $\{1, 2, 3,\dots, p-1\}$, среди элементов которого $(p-1)/2$ квадратичных вычетов. Область возможных значений величины $(2 + V^{-1})$ в уравнении (12) смещается к величинам $\{3, 4, 5,\dots, p-1, 0, 1\}$, среди которых элемент 0 вытеснил квадратичный невычет 2. Соответственно, в уравнении (13) область возможных значений величины $(-1 + V^{-1})$ включает элементы $\{0, 1, 2, 3,\dots, p-2\}$ с вытеснением элементом 0 квадратичного невычета (-1). Отсюда следует, что число ненулевых квадратичных вычетов в обоих смещенных множествах одинаково и равно $(p-1)/2$. Они дают ровно $(p-1)$ решений уравнений (12) и (13) с ненулевыми y- координатами. Добавляя две отброшенные при анализе точки $\mathbf{O} = (1, 0)$ и $\boldsymbol{D} = (-1, 0)$, получаем порядок обеих кривых $N_E = p + 1$. Теорема доказана.

Значениями $d = -1$, 2 и 2^{-1} не исчерпывается перечень суперсингулярных кривых Эдвардса. В работе [6] доказано, что если элемент 3 поля F_p является квадратичным вычетом при $p \equiv 3\bmod 4$, то параметр $d = -(\sqrt{3}\pm 2)/(-\sqrt{3}\pm 2)$ также порождает суперсингулярную кривую.

4. Определение точек *kP* кривой Эдвардса и их порядков

В криптосистемах приемлемыми являются кривые Эдвардса с минимальным кофактором 4 порядка кривой $N = 4n$, где n – достаточно большое простое число ($n > 2^{163}$). Если порядок генератора P кривой E_{ED} равен Ord$P = 4n$, то генератор криптосистемы $G = 4P$ имеет порядок Ord$G = n$. Точки 8-го порядка отсутствуют, если $(1 - d)$ – квадратичный невычет [3].

Утверждение 1. *На кривой Эдвардса порядка* $4n$ *не существует точек деления на* 2 *для точек* $< P >$ *максимального порядка и точек* $\boldsymbol{F}$ *четвертого порядка, и существуют по две точки деления – для всех других точек кривой*.

Доказательство. Каждой точке kP кривой отвечает скалярный множитель k как элемент кольца целых чисел Z_N с операциями по модулю $N = 4n$. Все нечетные элементы $k \in \{1, 3, 5,\dots, 4n - 1\}$ кольца $\mathbf{Z}_N$, которым соответствуют точки кривой максимального порядка $4n$ и порядка 4 (равные $\pm nP$), не делятся на 2 в кольце $\mathbf{Z}_N$. С другой стороны, все четные элементы $k = 2s$ при делении на два по модулю N дают два значения s и $s + N/2$, удвоение которых дает вновь $2s = k$. Возвращаясь к точкам kP кривой, заключаем, что утверждение 1 доказано.

Если случайная точка кривой Q имеет порядок $2n$, то обе точки деления на 2 $\{Q/2, Q/2+\boldsymbol{D}\}$ имеют максимальный порядок $4n$. Действительно, удвоение этих точек порядка $4n$ дает одну точку Q порядка $2n$.

Если случайная точка кривой Q имеет порядок n, то порядки точек деления на 2 $\{Q/2, Q/2+\boldsymbol{D}\}$ отличаются вдвое и имеют значения n и $2n$. Например, если Ord$(Q/2) = n$, т.е. $n(Q/2) = O$, то $n(Q/2 + \boldsymbol{D}) = \boldsymbol{D} \Rightarrow 2n(Q/2 + \boldsymbol{D}) = \mathbf{O}$.

Прикладное значение доказанной в первом разделе статьи теоремы очевидно. Для определения порядка точек кривой Эдвардса вовсе не требуется выполнять сложную операцию скалярного произведения nQ. Если у случайной точки кривой $Q = (x_Q, y_Q)$ величина $(1 - y_Q^2)$ – квадратичный невычет, то Ord$(Q) = 4n$. В противном случае (с вероятностью 1/2) порядок точки равен n или $2n$. Удвоение любой такой точки дает генератор криптосистемы G – точку порядка n. Таким образом, для нахождения точки G требуется всего одна операция в поле и одно удвоение в группе точек.

Пример. Рассмотрим кривые Эдвардса с модулем $p = 19$, для которого выполняются оба условия теоремы 2. Три суперсингулярные кривые с порядком $N_E = p + 1 = 20$ сразу определяются при значениях $d \in \{ -1, 2, 10 = 2^{-1}\}$. Если исключить также кривые с порядком, кратным 8 (для них $1 - d$ – квадратичный вычет), останутся лишь две кривые с параметрами $d = 8$ и $d^{-1} = 12$, которые дают пару кривых кручения с порядками N_E соответственно 28 и 12 (след уравнения Фробениуса для них $t = \pm 8$). Точки первой из этих кривых $x^2 + y^2 = 1 + 8x^2y^2$ представлены на рис.1. Они располагаются на четырех окружностях: 4 базовых точки на единичной окружности (на осях x и y) и по 8 точек (семейства точек) на окружностях с радиусами $\sqrt{2^2 + 9^2}$, $\sqrt{3^2 + 5^2}$ и $\sqrt{4^2 + 8^2}$.

Обозначим $P = (2,9)$, $Q = (3,5)$, $R = (4,8)$, $S = (5,3)$. $T = (8,4)$, $U = (9,2)$ – точки первого квадранта. Здесь точками максимального порядка 28 являются точки P, Q, R, для которых согласно теоремы 1 значения $(1 - y^2)$ являются квадратичными невычетами. Всех таких точек $\varphi(28) = 12$, по 3 точки в каждом квадранте. Все они симметричны точкам P, Q, R относительно осей x и y. Кроме них, имеется $\varphi(14) = 6$ точек 14-го и $\varphi(7) = 6$ точек 7-го порядков. Удвоение точек P, Q, R согласно (5) дает точки 14-го порядка $2P = (-8,4) = -T^*$, $2Q = (-9,2) = -U^*$, $2R = (5, -3) = -S$. Обратные точки имеют равные порядки, а делимые на 2 точки, симметричные относительно оси y, имеют порядки 7 и 14, отличающиеся вдвое. Итак, в первом квадранте имеем одну точку S 14-го порядка, и 2 точки T и U 7-го порядка. Зеркальные им относительно y точки имеют, соответственно, порядки 7 и 14.

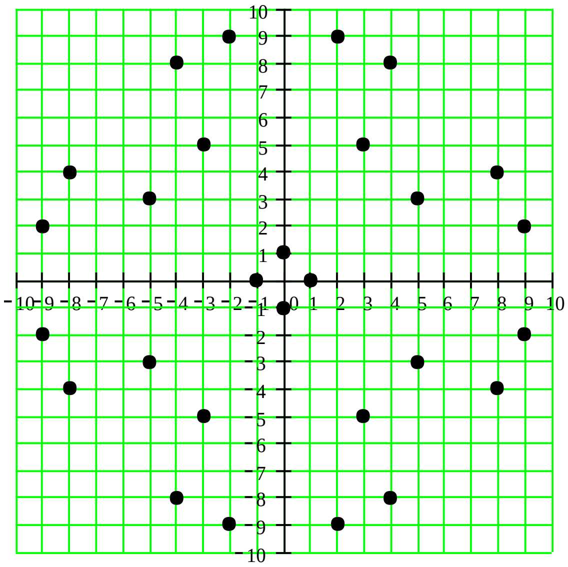

Рис. 1

Формально циклическую группу точек кривой kP можно расположить на окружности в порядке нарастания по часовой стрелке скалярного числа $k = 0, 1, 2,\ldots, N_E - 1$. Для нашего примера она представлена на рис.2. Назовем этот график колесом точек.

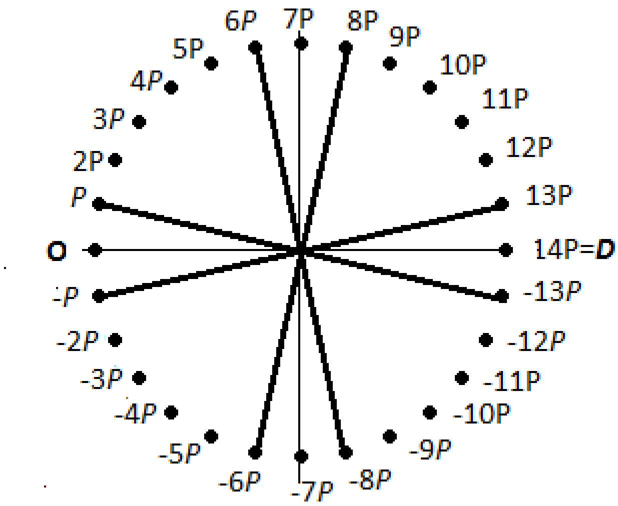

Рис. 2

Точки колеса, соединенные линиями, связаны как P и $P^* = P + \boldsymbol{D}$. Для любой не базовой точки семейство из 8 связанных линиями точек лежат на одной окружности на графике кривой рис.1.

Знание приблизительно 1/8 части всех точек позволяет реконструировать все другие точки кривой. Пусть точка P порождает все точки кривой и известны 4 точки: $P = (2,9)$, $2P = (-8,4)$, $4P = G = (-5,3)$, $7P = -\boldsymbol{F} = (0, -1)$. Так как справедливо свойство $(x_1, y_1) + (-y_1, -x_1) = (0, -1) = -\boldsymbol{F}$**,** мы далее легко находим точки $6P = (-9, -2)$, $5P = (-4,8)$, $3P = (-3,5)$, меняя местами координаты $x \leftrightarrow y$ и их знаки соответственно точек P, $2P$ и $4P$. Координаты точек kP при $k = 0 - 14$ представлены в таблице:

kP	**O**	P	$2P$	$3P$	$4P$	$5P$	$6P$	$\boldsymbol{7P}$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$\boldsymbol{14P}$
x_k	1	2	–8	–3	–5	–4	–9	0	9	4	5	3	8	–2	–1
y_k	0	9	4	5	3	8	–2	–1	–2	8	3	5	4	9	0

Для определения координат точек правее точки 4-го порядка мы используем свойство $P + \boldsymbol{D} = P^* = (-x_1, -y_1)$ или $P - P^* = \boldsymbol{D} = 14P$. Например, точка $13P$, симметричная точке P и равная $-P^*$, имеет координаты $(-x_1, y_1)$. В таблице хорошо видна симметрия (антисимметрия) координат точек верхней половины рис. 2: все y-координаты симметричны относительно точки $7P$, тогда как x-координаты обратны по знаку. Точки нижней половины рис. 2 обратны точкам верхней половины с инверсией знака y- координаты. Например, точка $17P = 28P - 11P = -11P = (3, -5)$.

Итак, при известных четырех точках мы без вычислений получили координаты всех 28 точек kP кривой Эдвардса. Разумеется, этот метод годится для любой кривой, при этом предвычисления состоят в расчете координат точек kP для $k = 2,3,\ldots,(n+1)/2$. Это составляет практически 1/8 часть порядка кривой.

Возвращаясь к графику кривой на рис. 1, находим в таблице все ее точки как скалярное произведение kP. Точки первого квадранта $Q = (3,5)= 11P$, $R = (4,8) = 9P$ имеют порядок 28, точка $S = (5,3) = 10P$ имеет порядок 14, а две точки $U = (9,2) = -8P = -2G$ и $T = (8,4) = 12P = 3G$ – порядок 7. Это подтверждает выводы предыдущего анализа. Почти все точки первого квадранта (кроме $8P$ и $13P$) попали в верхнюю правую часть колеса рис. 2, но это совпадение случайно. Статистика распределения знаков координат не известна, но скорее всего для больших полей их знаки (±) равновероятны.

Утверждение 2. *Для кривой Эдвардса порядка* $4n$ *любое семейство из* 8 *точек* $(\pm x_1, \pm y_1)$, $(\pm y_1, \pm x_1)$, *лежащих на одной окружности, содержит* 4 *точки порядка* $4n$, 2 *точки порядка* $2n$ и 2 *точки порядка* n.

Доказательство. Пусть $\mathrm{Ord}(kP) = 4n$, тогда пары точек $\pm kP$ в левой и $\pm kP^*$ в правой части колеса точек рис.2 имеют одинаковый порядок $4n$. В верхней части колеса точек имеем точки $nP \pm kP$, причем $(n \pm k)$ – четные числа, одно из которых сравнимо с 0mod4, а второе – с 2mod4. Отсюда следует, что порядки этих точек равны n и $2n$.

Пусть теперь $\mathrm{Ord}(\pm kP) = 2n$, тогда точки $\pm kP^* = \pm kP + \boldsymbol{D}$ имеют порядок n, так как $n(\pm kP + \boldsymbol{D}) = \pm nkP + n\boldsymbol{D} = \pm \boldsymbol{D} + \boldsymbol{D} = \mathbf{O}$. Точки $nP \pm kP$ в верхней части рис.2 имеют сомножителями $(n \pm k)$ – нечетные числа, поэтому их порядки (и, соответственно, обратных им точек) максимальны и равны $4n$.

Наконец, пусть $\mathrm{Ord}(\pm kP) = n$, тогда точки $\pm kP^* = \pm kP + \boldsymbol{D}$ имеют порядок $2n$, так как $2n(\pm kP + \boldsymbol{D}) = \mathbf{O}$. По аналогии с предыдущим абзацем остальные 4 точки имеют порядок $4n$. Утверждение 2 доказано.

Заметим, что существует лишь 2 точки максимального порядка, порождающие известный генератор G подгруппы точек простого порядка n – это точки P и P^*, для которых $2P^*=2P$, $G=4P$. Все четные точки колеса рис. 2 при переходе к порождающей точке P^* сохраняют свои координаты, а нечетные P^*, $3P^*$, $5P^*\ldots$ меняют знаки обеих координат.

Не следует считать, что приведенные выше замечательные свойства кривой Эдвардса снижают сложность вычисления дискретного логарифма в группе точек $<G>$ простого порядка n. Согласно утверждению 2 из 8-ми точек каждого семейства на колесе точек рис.2 лишь 2 обратных точки имеют порядок n подгруппы $<G>$. Поэтому, как и для эллиптических кривых в канонической форме, сложность DLP здесь снижается лишь вдвое за счет обратных точек. Тем не менее, эти свойства могут вдохновить исследователей на поиски новых методов решения проблемы дискретного логарифмирования.

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. *Bernstein Daniel J., Lange Tanja*. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20. 3. *Бессалов А.В.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. – 2011. - Вып. 167. - С. 203-208. 4. Бессалов А.В. Деление точки на два для кривой Эдвардса над простым полем // Прикладная радиоэлектроника. – 2013. – Т. 12, №2. - С. 278-279. 5.Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривих : учеб. пособие. – К. : ІВЦ «Політехніка», 2004. – 224с. 6. Бессалов А.В. Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме // Прикладная радиоэлектроника. - 2014. – Т. 13, №3. – С.286-289.

КПИ

Поступила в редколлегию 12.03.2015