ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 51 **2015** **Вып. 4**

УДК 621.391.15 : 519.7

© 2015 г. **А.В. Бессалов, О.В. Цыганкова**

ВЗАИМОСВЯЗЬ СЕМЕЙСТВ ТОЧЕК БОЛЬШИХ ПОРЯДКОВ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Предложена модификация закона сложения точек на кривой Эдвардса над простым полем. Доказаны три теоремы о свойствах координат точек больших порядков и вырожденной паре кривых кручения. Предложен алгоритм реконструкции всех неизвестных точек kP кривой Эдвардса лишь при 1/8 части известных точек.

§ 1. Введение

Эллиптические кривые в форме Эдвардса сегодня являются наиболее быстрыми и перспективными в асимметричных криптосистемах. Введенный Эдвардсом в работе [1] закон сложения точек оказался не вполне удобным в эллиптической криптографии, где принята горизонтальная симметрия обратных точек. В данной статье вносятся коррективы в этот закон с целью унификации определения обратных точек.

В теореме 1 доказывается необходимое и достаточное условие делимости на 2 для точек кривой большого порядка (более четырех). В теореме 2 доказано важное свойство, связывающее координаты таких точек. В статье доказана теорема 3 о необходимых условиях существования вырожденных пар кривых кручения, порождающих суперсингулярные кривые с порядком $p+1$. Доказываются также два предложения о порядках точек кривой. Приводится пример, показывающий, как знание 1/8 части точек кривой Эдвардса позволяет реконструировать все точки вида kP этой кривой. Это, тем не менее, не упрощает проблему дискретного логарифмирования для точек простого порядка.

Семейством точек большого порядка мы называем восемь точек кривой, лежащих на плоскости $x-y$ на одной окружности с радиусом, не равным единице. В статье дается анализ таких семейств, на основе которого удается находить точки различных порядков и реконструировать точки вида kP без применения групповых операций.

§ 2. Модификация закона сложения точек кривой Эдвардса

В работах [1, 2] приводится унифицированный и полный закон сложения точек эллиптической кривой вида

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

над любым полем характеристики $p \neq 2$ с помощью следующей формулы:

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

При совпадении складываемых точек закон удвоения точки становится частным случаем формулы (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 $\mathrm{O} = (0, e)$ как нейтрального элемента абелевой группы точек. На осях x и y находятся еще три базовых точки: точка 2-го порядка $D = (0, -e)$ и две точки 4-го порядка $\pm F = (\pm e, 0)$, такие что $2F = D$, $2D = \mathrm{O}$. Если $P = (x_1, y_1)$, то обратная точка $-P = (-x_1, y_1)$, и в соответствии с (2) $(x_1, y_1) + (-x_1, y_1) = \mathrm{O}$. Здесь имеет место вертикальная симметрия обратных точек относительно оси y. Заметим, что с целью геометрической наглядности мы вместо $x > p/2$ записываем элементы $-x \equiv (p - x) \bmod p$.

Мы предлагаем модификацию закона (2) сложения точек, имеющую вид

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

Она позволяет сохранить сходство с вейерштрассовой формой эллиптической кривой, для которой $\pm P = (x_1, \pm y_1)$. Определяя теперь обратную точку как $-P = (x_1, -y_1)$, согласно (4) получим $(x_1, y_1) + (x_1, -y_1) = \mathbf{O} = (e, 0)$. Итак, координаты базовых точек для закона (4), которые далее будем выделять жирным шрифтом, следующие: $\mathbf{O} = (e, 0)$, 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 сохранить горизонтальную симметрию (относительно оси x) обратных точек, общепринятую в теории эллиптических кривых.

Так как любая ненулевая константа e в форме (1) кривой дает изоморфную кривую над простым полем $\mathbb{F}_p$, мы в дальнейшем принимаем $e = 1$. Достаточным условием полноты закона (4) служит условие $\left(\frac{d}{p}\right) = -1$, т.е. параметр d является квадратичным невычетом [2].

Из (1) ясно, что любая не базовая точка (x_1, y_1) порождает семейство из восьми точек $(\pm x_1, \pm y_1), (\pm y_1, \pm x_1)$, лежащих симметрично на одной окружности радиуса $\sqrt{x_1^2 + y_1^2}$ (по две в каждом квадранте). Все они связаны между собой с помощью трех базовых точек: $\boldsymbol{D}$ и $\pm\boldsymbol{F}$. По формуле (4) имеем

$$P + \boldsymbol{D} = (x_1, y_1) + (-1, 0) = (-x_1, -y_1) = P^*,$$
$$P \pm \boldsymbol{F} = (x_1, y_1) + (0, \pm 1) = (\pm(-y_1), \pm x_1).$$

Остальные четыре точки семейства строятся аналогично с помощью обратной точки $-P$.

Рассмотрим ряд новых свойств кривых (1) в форме Эдвардса над полем $\mathbb{F}_p$.

§ 3. Необходимое и достаточное условие делимости точки кривой Эдвардса на 2

Пусть $P = (x_1, y_1)$, $2P = (a, b)$. Запишем обратную удвоению операцию деления точки на 2 как $(a, b)/2 \in \{P, P^* = P + \boldsymbol{D}\}$. Ясно, что удвоение этих двух решений дает один результат $2P = 2P^*$.

Воспользуемся законом удвоения (5) при $e = 1$. Исключим четыре базовые точки кривой (1): $\mathbf{O}$, $\boldsymbol{D}$ и $\pm\boldsymbol{F}$. Обозначим $Z = x_1/y_1$, $V = x_1y_1$, $Z, V \neq 0$. Согласно (1) и значению второй координаты b в (5) для одной точки P кривой, не лежащей на окружности радиуса 1, справедливы два квадратных уравнения

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

с дискриминантами

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

и решениями

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

Вышеизложенное позволяет сформулировать и доказать следующую теорему.

Т е о р е м а 1. *Для любой точки (a, b) кривой Эдвардса* (1), *не лежащей на окружности радиуса* 1, *существуют две точки деления $(a, b)/2 \in \{P, P + \boldsymbol{D}\}$ 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.*

Д о к а з а т е л ь с т в о. 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 $\mathbb{F}_p$. 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, т.е. $\left(\frac{1 - b^2}{p}\right) = 1$. При выполнении этого условия кроме точки P, для которой $2P = (a, b)$, существует точка $P^* = P + \boldsymbol{D} = (-x_1, -y_1)$, для которой $2P^* = 2P + 2\boldsymbol{D} = (a, b)$ с учетом $2\boldsymbol{D} = \mathbf{O}$. При $\left(\frac{1 - b^2}{p}\right) = -1$ уравнение (6) решений в поле $\mathbb{F}_p$ не имеет, и точек деления на 2 не существует. Необходимость доказана.

Достаточность. Для любой не базовой точки P кривой (1), для которой имеет место равенство (5), справедливы оба тождества (6). Достаточно потребовать, чтобы один из дискриминантов (7) был квадратом, из чего сразу следует, что и второй дискриминант – квадрат. Пусть (a, b) – точка кривой (1). Тогда равенство $a^2 + b^2 = 1 + da^2b^2$ можно записать в виде $1 - b^2 = a^2(1 - db^2)$. Отсюда видим, что для любой точки (a, b) кривой обе величины $1 - b^2$ и $1 - db^2$ являются либо квадратичными вычетами, либо невычетами. В первом случае существуют две точки деления $(a, b)/2$, и наоборот. ▲

Это свойство точек позволяет без использования групповых операций находить точки максимального порядка $4n$ кривой Эдвардса. Для четырех базовых точек кривой Эдвардса на 2 делится обычно лишь точка $\boldsymbol{D}$, так что $\boldsymbol{D}/2 = \pm\boldsymbol{F}$ (или $\pm 2\boldsymbol{F} = \boldsymbol{D}$).

В следующей теореме доказываются новые свойства координат точек кривой Эдвардса.

Т е о р е м а 2. *Для любой не базовой точки (x_1, y_1) кривой* (1) *при $e = 1$ справедливо равенство $\left(\frac{1 - x_1^2}{p}\right)\left(\frac{1 - y_1^2}{p}\right) = \left(\frac{1 - d}{p}\right)$.*

Д о к а з а т е л ь с т в о. Для точки (x_1, y_1) с учетом определения (1) при $e = 1$ запишем произведение $(1 - dy_1^2)(1 - x_1^2) = 1 + dx_1^2y_1^2 - x_1^2 - dy_1^2 = y_1^2 - dy_1^2 = (1 - d)y_1^2$.

Из доказательства теоремы 1 известно, что элементы поля $1 - y_1^2$ и $1 - dy_1^2$ для всех точек (x_1, y_1) кривой являются одновременно квадратичными вычетами

или невычетами. Тогда из последнего соотношения сразу следует, что произведение $(1-y_1^2)(1-x_1^2)$ является квадратичным невычетом при $\left(\frac{1-d}{p}\right) = -1$, и наоборот, что и доказывает условие теоремы. ▲

Теорема 2 легко обобщается и на изоморфные кривые (1) с параметром $e \neq 1$. Действительно, с помощью замены $u = x/e$, $v = y/e$, $d' = de^4$ получаем уравнение изоморфной (1) кривой $u^2 + v^2 = 1 + d'u^2v^2$. Для него условие теоремы справедливо после замены $(x, y) \mapsto (u, v)$ и $d \mapsto d'$.

Для кривых Эдвардса, не имеющих точек 8-го порядка, элемент $1 - d$ является квадратичным невычетом [3]. Тогда из теоремы 2 следует, что любая небазовая точка такой кривой имеет пару значений $1-y_1^2$ и $1-x_1^2$, одно из которых – квадратичный вычет, а другое – квадратичный невычет. В частности, для точки максимального порядка $4n$ элемент $1 - y_1^2$ – квадратичный невычет, а $1 - x_1^2$ – квадратичный вычет.

Определение координат точек деления на 2 рассмотрено в работе [4]. По формулам (8) можно найти решения квадратных уравнений (6) и координаты точек деления на 2.

§ 4. Вырожденные пары кривых кручения

Переход к кривой кручения для формы (1) Эдвардса осуществляется простой заменой $d \mapsto d^{-1}$ (см. [2, 3]), тогда порядки пары этих кривых $N_E = p + 1 \pm t$. Пара кручения называется вырожденной, если след Фробениуса $t = 0$, т.е. порядок обеих кривых $N_E = p + 1$. Такая кривая является суперсингулярной. Этот случай возможен лишь при $p \equiv 3 \bmod 4$, и тогда $4 \mid (p + 1)$. Например, при $d = d^{-1} = -1$ имеем тривиальный случай вырожденной пары кручения. Авторы обнаружили еще один нетривиальный пример вырожденной пары кручения для кривой Эдвардса. Докажем следующую теорему.

Т е о р е м а 3. *При $p \equiv 3 \bmod 4$ и $p \equiv \pm 3 \bmod 8$ пара кривых кручения в форме Эдвардса над $\mathbb{F}_p$ с параметрами $d \in \{2, 2^{-1}\}$ является вырожденной.*

Д о к а з а т е л ь с т в о. Первое условие теоремы обсуждалось выше и связано с делимостью порядка кривой на 4. При выполнении второго условия элемент 2 поля $\mathbb{F}_p$ не является квадратом, т.е. $\left(\frac{2}{p}\right) = -1$ (см. [5]). 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 $\boldsymbol{D}$ с координатами $x = \pm 1$, $y = 0$, можно записать равенство

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

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

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

причем в левой части имеем квадрат, так как $-d$ – квадратичный вычет. При $d = 2$ эти уравнения имеют вид

$$y^{-2} = 2 + V^{-1}, \quad V = x^2 - 1, \tag{9}$$

$$-2v^{-2} = -1 + V^{-1}. \tag{10}$$

Покажем, что оба уравнения дают одинаковое число решений. При всех $x^2 \neq 1$ переменная V^{-1} пробегает всевозможные ненулевые значения из множества $\{1, 2, 3, \ldots, p-1\}$, среди элементов которого $(p-1)/2$ квадратичных вычетов. Область возможных значений величины $2 + V^{-1}$ в уравнении (9) смещается к величинам $\{3, 4, 5, \ldots, p-1, 0, 1\}$, среди которых элемент 0 заменил квадратичный невычет 2 исходного множества V^{-1}. Соответственно, в уравнении (10) область возможных значений величины $-1 + V^{-1}$ включает элементы $\{0, 1, 2, 3, \ldots, p-2\}$ 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 (9), (10) с ненулевыми y-координатами (т.е. $p-1$ точек кривой). Добавляя две отброшенные при анализе точки $\mathbf{O} = (1, 0)$ и $\boldsymbol{D} = (-1, 0)$, получаем порядок обеих кривых $N_E = p + 1$. ▲

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

§ 5. Определение точек kP кривой Эдвардса и их порядков

Кривые Эдвардса подходят для использования в криптосистемах, если их порядок $N = 4n$, где n – большое простое число ($n > 2^{163}$). Если порядок генератора кривой $\operatorname{Ord} P = 4n$, то генератор криптосистемы $G = 4P$ имеет порядок n. Точки 8-го порядка отсутствуют, если $1 - d$ – квадратичный невычет [3].

Предложение 1. *На кривой Эдвардса порядка $4n$ существуют точки деления на 2 для всех точек, кроме точек $\langle P \rangle$ максимального порядка и точек $\pm\boldsymbol{F}$ четвертого порядка.*

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

Если случайная точка Q кривой имеет порядок $2n$, то обе точки деления на 2 $\{Q/2, Q/2 + \boldsymbol{D}\}$ имеют максимальный порядок $4n$. Если точка Q имеет порядок n, то порядки точек деления на 2 $\{Q/2, Q/2 + \boldsymbol{D}\}$ равны n и $2n$ соответственно.

Прикладное значение доказанной в § 3 теоремы 1 очевидно. Для нахождения порядка точек кривой Эдвардса не требуется вычислять скалярное произведение nQ. Если у случайной точки кривой (x_Q, y_Q) величина $1 - y_Q^2$ – квадратичный невычет, то $\operatorname{Ord} Q = 4n$. В противном случае порядок точки равен n или $2n$. Получить такую точку можно непосредственно, меняя местами координаты x_Q и y_Q (см. теорему 2).

Пример. Рассмотрим кривые Эдвардса с модулем $p = 19$, для которого выполняются оба условия теоремы 3. При $d \in \{-1, 2, 2^{-1}\}$ имеем суперсингулярные кривые с порядком $N_E = p + 1 = 20$. Исключим также кривые с порядком, кратным 8, для которых $1 - d$ – квадратичный вычет. Получаем две кривые с параметрами $d = 8$ и $d^{-1} = 12$, которые дают пару кривых кручения с порядками 28 и 12 (для них $t = \pm 8$). Точки первой из них представлены на рис. 1.

Обозначим точки первого квадранта $P = (2, 9)$, $Q = (3, 5)$, $R = (4, 8)$, $S = (5, 3)$, $T = (8, 4)$, $U = (9, 2)$. Здесь точками максимального порядка 28 являются точки P, Q, R, для которых значения $1 - y^2$ являются квадратичными невычетами. Всего таких точек двенадцать, по три точки в каждом квадранте. Кроме них имеется

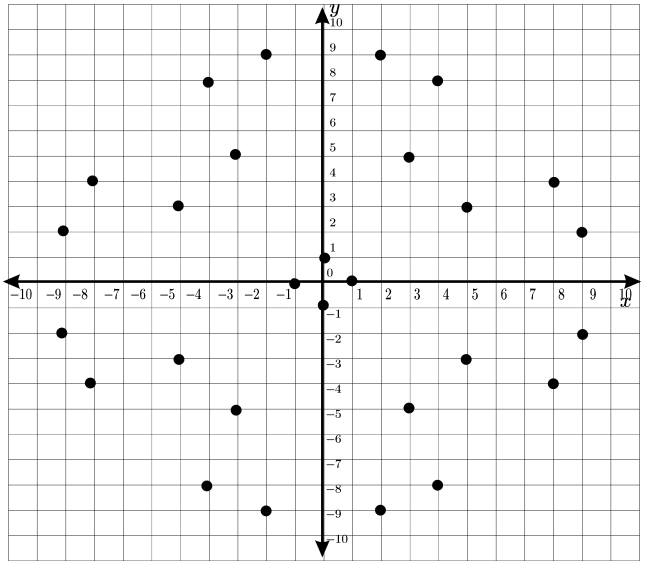

Рис. 1.

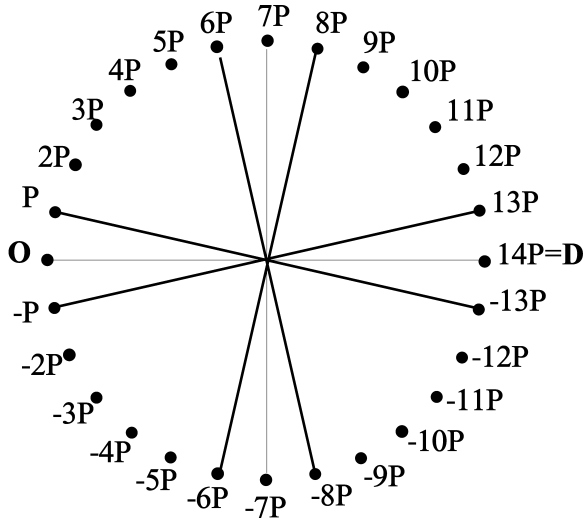

Рис. 2.

шесть точек 14-го и шесть точек 7-го порядков. Удвоение точек P, Q, R согласно (5) дает точки 14-го порядка $2P = (-8, 4) = -T^*$, $2Q = (-9, 2) = -U^*$, $2R = (5, -3) = -S$. Итак, в первом квадранте имеем одну точку S 14-го порядка и две точки T и U 7-го порядка.

Циклическую группу точек кривой kP можно представить в виде последовательности точек на окружности в порядке роста скалярного числа $k = 0, 1, 2, \ldots, N_E - 1$ по часовой стрелке. Для нашего примера такая точечная окружность представлена на рис. 2. Назовем этот график колесом точек. Точки колеса, соединенные линиями, связаны как P и $P^* = P + \boldsymbol{D}$. Для любой не базовой точки семейство из восьми связанных линиями точек на рис. 2 лежат на одной окружности на графике кривой на рис. 1.

Знание около $1/8$ части всех точек позволяет реконструировать все другие точки кривой. Пусть точка P порождает все точки кривой и известны четыре точки: $P = (2, 9)$, $2P = (-8, 4)$, $4P = (-5, 3)$, $7P = -\boldsymbol{F} = (0, -1)$. В силу свойства $(x_1, y_1) + (-y_1, -x_1) = (0, -1) = -\boldsymbol{F}$ легко находятся точки $6P = (-9, -2)$, $5P = (-4, 8)$, $3P = (-3, 5)$, меняя местами координаты $x \leftrightarrow y$ и их знаки для точек P, $2P$ и $4P$ соответственно. Координаты точек kP при $k = 0, \ldots, 14$ представлены в таблице:

kP	**O**	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$
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 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 колеса рис. 2 обратны точкам верхней половины с инверсией знака y-координаты. Например, точка $17P = 28P - 11P = -11P = (3, -5)$.

Итак, при известных точках 4-го порядка (причем одна из них базовая $-\boldsymbol{F}$) мы без вычислений получили координаты всех 28 точек kP кривой Эдвардса. Этот метод годится очевидным образом для кривой любого порядка, при этом предвычисления состоят в расчете координат точек kP для $k = 2, 3, \ldots, (n+1)/2$, что составляет практически $1/8$ часть порядка кривой.

По 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 $S = (5, 3) = 10P$ – порядок 14, а две точки $U = (9, 2) = -8P$ и $T = (8, 4) = 12$ – порядок 7. Это отвечает выводам предыдущего анализа.

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

Доказательство. Пусть $\mathrm{Ord}(kP) = 4n$, тогда пары точек $\pm kP$ в левой и $\pm kP^*$ в правой частях колеса точек на рис. 2 имеют одинаковый порядок $4n$. В верхней части этого колеса имеем точки $nP \pm kP$, причем $n \pm k$ – четные числа, одно из которых сравнимо с 0 mod 4, а второе – с 2 mod 4. 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, порядки 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 $2n(\pm kP + \boldsymbol{D}) = \mathbf{O}$. Аналогично предыдущему случаю остальные четыре точки имеют порядок $4n$. ▲

Замечание. Приведенные выше свойства кривой Эдвардса не должны снижать сложность вычисления дискретного логарифма в группе точек $\langle G\rangle$ простого порядка n. Действительно, согласно предложению 2 из восьми точек каждого семейства на колесе точек рис. 2 лишь две обратные точки имеют порядок n подгруппы $\langle G\rangle$. Поэтому, как и для кривых в канонической форме, сложность DLP [5] здесь снижается лишь вдвое за счет обратных точек. Тем не менее эти свойства могут послужить основой для поиска новых методов решения проблемы дискретного логарифма.

СПИСОК ЛИТЕРАТУРЫ

1. *Edwards H.M.* A Normal Form for Elliptic Curves // Bull. Amer. Math. Soc. (N.S.). 2007. V. 44. № 3. P. 393–422.
2. *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.
3. *Бессалов А.В.* Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. Вып. 167. Харьков: ХНУРЕ, 2011. 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 кривых. Киев: Политехника, 2004.
6. *Бессалов А.В.* Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме // Прикладная радиоэлектроника. 2014. Т. 13. № 3. С. 286–289.

Бессалов Анатолий Владимирович
Цыганкова Оксана Валентиновна
Физико-технический институт Национального технического университета Украины "Киевский политехнический институт"
bessalov15@mail.ru
cig@pti.kpi.ua

Поступила в редакцию
03.12.2014
После переработки
15.06.2015