УДК 681.3.06

Л.В. КОВАЛЬЧУК, А.В. БЕССАЛОВ, А.Ю. БЕСПАЛОВ

АЛГОРИТМЫ ГЕНЕРАЦИИ БАЗОВОЙ ТОЧКИ КРИВОЙ ЭДВАРДСА С ИСПОЛЬЗОВАНИЕМ КРИТЕРИЕВ ДЕЛИМОСТИ ТОЧКИ

Аннотация. Сформулированы и доказаны критерии делимости точки кривой Эдвардса на 2, 4 и другие натуральные числа. С использованием этих критериев построены алгоритмы извлечения корня произвольной степени в группе точек кривой Эдвардса, а также получены новые алгоритмы генерации базовой точки кривой, которые, как показал сравнительный анализ, имеют ряд преимуществ.

Ключевые слова: кривые Эдвардса, делимость точки, генерация базовой точки.

ВВЕДЕНИЕ

В настоящее время эллиптические кривые в форме Эдвардса являются наиболее перспективными для использования в асимметричных криптосистемах. При построении криптосистем особенно важны такие свойства кривых Эдвардса [1, 2], как максимальная скорость выполнения операций с точками, универсальность закона сложения, а также возможность представления нейтрального элемента в аффинных координатах.

Симметрия уравнения кривых Эдвардса относительно обеих координат обусловливают полезные свойства этих кривых. Если изучать кривые Эдвардса с точностью до изоморфизма, то достаточно использовать лишь один параметр d вместо двух обычных: a и b, классической кривой в канонической форме Вейерштрасса.

В работе [3] обобщен и расширен класс кривых Эдвардса, названный скрученными кривыми Эдвардса (twisted Edwards curves), добавлением нового параметра a. Исследование новых свойств этого класса скрученных кривых Эдвардса описано в [4], где найдены альтернативные формулы для закона сложения точек кривой, определены их особенности, предложен метод расчета координат суммы точек в расширенных проективных координатах, а также сокращено количество операций при сложении различных точек с $10\mathbf{M}+2\mathbf{S}+2\mathbf{D}$ до $9\mathbf{M}+1\mathbf{D}$ ($\mathbf{M}$ — умножение в поле, $\mathbf{S}$ — возведение в квадрат, $\mathbf{D}$ — умножение на параметр кривой), что увеличило быстродействие операции сложения точек примерно в 1,36 раз.

В работе [5] приведены необходимые и достаточные условия того, что эллиптическая кривая, заданная в канонической форме, является изоморфной некоторой кривой Эдвардса. На основе этих критериев найдено точное число кривых Эдвардса над произвольным конечным полем в зависимости от его характеристики.

В настоящей статье сформулированы и обоснованы критерии делимости точки кривой Эдвардса на произвольное натуральное число, с использованием которых разработаны алгоритмы получения корня произвольной степени из точки кривой, или в терминах аддитивной группы алгоритмы нахождения точки деления на произвольное натуральное число. На основании этих критериев созданы новые алгоритмы вычисления координат базовой точки кривой (или образующего элемента подгруппы простого порядка n группы точек кривой), а также выполнен детальный сравнительный анализ новых и классического алгоритмов

вычисления базовой точки кривой и показано, что предложенные далее алгоритмы в сотни раз быстрее существующего. Этот показатель увеличивается с ростом характеристики простого поля, над которым построена кривая.

Заметим, что приведенные критерии делимости и алгоритмы получения корня в группе точек эллиптической кривой во многом подобны аналогичным критериям, описанным в [6] для простых полей и конечных колец. Однако для эллиптических кривых эти алгоритмы имеют намного большее прикладное значение.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Пусть кривая Эдвардса задана уравнением

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

Согласно [2] все кривые, заданные уравнением (1) с параметрами c и d, в общем виде изоморфны кривым в форме

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

Далее используется именно форма (2).

Обозначим E_p кривую Эдвардса над полем F_p и $P = (x, y)$ или (x, y) — ее произвольную точку P, имеющую координаты (x, y), где $x, y \in F_p$.

Как известно, множество точек кривой образует группу относительно некой специфической операции, которую принято называть сложением. Далее будем использовать модифицированный закон сложения, определяемый следующим образом:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 x_2 - y_1 y_2}{1 - dx_1 x_2 y_1 y_2}, \frac{x_1 y_2 + x_2 y_1}{1 + dx_1 x_2 y_1 y_2}\right). \tag{3}$$

Данный закон выводится из «классического» методом выполнения так называемого «поворота на 90° вправо» точек кривой [7]. Его преимущество заключается в том, что точка, обратная к $P = (x, y)$, имеет вид $-P = (x, -y)$, как и для эллиптической кривой, заданной в форме Вейерштрасса. Нейтральным элементом является точка $O = (1, 0)$.

Множество точек кривой Эдвардса (2) образует циклическую группу, порядок которой кратен 4. В криптографических приложениях используются лишь кривые Эдвардса, порядки которых $N(E_p) = 4n$, где n — большое (от 180 бит) простое число. Поэтому далее рассматриваются только такие кривые.

Согласно свойствам циклической группы [8] в группе E_p обязательно должны существовать две точки четвертого порядка: $F = (0,1)$ и $-F = (0, -1)$, и одна точка второго порядка: $D = (-1, 0)$, а также $\varphi(n) = n - 1$ точек порядка n, столько же точек порядка $2n$ и еще $\varphi(4n) = 2(n - 1)$ точек порядка $4n$. Для криптографических приложений используется подгруппа кривой E_p, имеющая порядок n. Очевидно, что она состоит из нейтрального элемента $O = (1, 0)$ и всех точек порядка n. Образующий элемент этой подгруппы называется базовой точкой кривой E_p.

Рассмотрим формулы, которые являются простым следствием закона сложения (3). Для произвольной точки $P = (x, y)$ справедливы равенства

$$D = 2F,$$

$$P + D = P - D = (-x, -y),$$

$$P + D - F = P + F = (-y, x),$$
$$P + 3F = P + D + F = (y, -x). \quad (4)$$

Для дальнейшего изложения введем определения.

Определение 1. Пусть $P \in E_p$, $k \in N$. Будем говорить, что точка P делится на k, если $\exists R \in E_p : P = kR$, где kR — k-кратное сложение R (умножение точки R на скаляр k, или скалярное умножение).

Множество точек E_p, которые делятся на k, обозначим $T_k(E_p)$.

Определение 2. Пусть $P \in T_k(E_p)$. Будем говорить, что точка R является корнем k-й степени из P, если $kR = P$.

Далее формулируются критерии делимости точки на 2 и 4 с условиями, удобными для вычислений, и описывается, как эти критерии можно использовать для оптимизации построения криптосистем на кривых Эдвардса. Основное внимание уделяется построению на основании этих критериев алгоритмов генерации базовой точки кривой, время работы которых существенно меньше, чем, например, алгоритма генерации базовой точки в ДСТУ 4145-2002. Также приводятся сравнительный временной анализ этих алгоритмов и критерии делимости точек кривой на n, $2n$, $4n$ и k при $1 < k < 4n$, $(k, 4n) = 1$.

Заметим, что для значений $k = n, 2n, 4n$ очевидно справедлив критерий делимости $P \in T_k(E_p) \Leftrightarrow \frac{4n}{k} P = O$.

КРИТЕРИЙ ДЕЛИМОСТИ ТОЧКИ КРИВОЙ ЭДВАРДСА НА 2

В работе [7] сформулирован и доказан критерий делимости точки кривой на 2. Приведем его с более детальным доказательством, которое отличается от описанного в [7] тем, что является конструктивным, т.е. позволяет не только проверять делимость точки на 2, но и показывает, как можно вычислить все ее точки деления. Именно на основании этого доказательства разработан далее алгоритм деления точки на 2.

Теорема 1 [7] (критерий делимости на 2). Пусть $P = (a, b) \in E_p$. Тогда следующие условия равносильны:

$$1)\ P \in T_2(E_p);$$
$$2)\ \left(\frac{1 - b^2}{p}\right) = 1. \quad (5)$$

Доказательство.

1. Докажем, что из условия 1 в (5) следует условие 2. Пусть $P = (a, b) \in T_2(E_p)$, т.е. $\exists R = (x, y) : P = 2R$. Тогда согласно (2)

$$a^2 + b^2 = 1 + da^2 b^2 \quad (6)$$

и согласно (2), (3) для координат точки R справедлива система уравнений

$$\begin{cases} x^2 + y^2 = 1 + dx^2 y^2; \\ \dfrac{2xy}{1 + dx^2 y^2} = b; \\ \dfrac{x^2 - y^2}{1 - dx^2 y^2} = a. \end{cases} \quad (7)$$

Из первого и второго уравнений системы (7) получаем $\frac{2xy}{x^2+y^2}=b$, откуда $2\frac{y}{x}=b\left(1+\left(\frac{y}{x}\right)^2\right)$. В этом уравнении обозначим $V=\frac{y}{x}$ и получим $2V=b(1+V^2)$, или

$$V^2-2b^{-1}V+1=0. \tag{8}$$

Согласно условию 1 теоремы 1 уравнение (8) имеет решение. Поэтому его дискриминант является квадратичным вычетом по mod p, т.е. $D=4b^{-2}-4=$ $=4(b^{-2}-1)=\frac{4(1-b^2)}{b^2}$ — квадратичный вычет по mod p. Поскольку $4b^{-2}\in Q_p$, последнее условие эквивалентно условию $\left(\frac{D}{p}\right)=\left(\frac{1-b^2}{p}\right)=1$, т.е. выполняется условие 2 теоремы 1.

2. Докажем, что из условия 2 в (5) следует условие 1. Пусть $P=(a,b)\in E_p$ и $\left(\frac{1-b^2}{p}\right)=1$. Покажем, что $\exists\, x,\, y\in F_p$, которые являются решениями системы (7) при заданных $a,b\in F_p$.

Из условия 2 получаем, что уравнение (8) имеет два решения:

$$V_{1,2}=\frac{2b^{-1}\pm 2b^{-1}\sqrt{1-b^2}}{2}=b^{-1}(1\pm\sqrt{1-b^2}). \tag{9}$$

Поскольку $P=(a,b)\in E_p$, т.е. выполняется условие (6), получаем $\frac{1-b^2}{1-db^2}=a^2$, откуда $(1-db^2)(1-b^2)\in Q_p$, и следовательно, $\left(\frac{1-db^2}{p}\right)=$ $=\left(\frac{1-b^2}{p}\right)=1$. Поэтому уравнение

$$Z^2-\frac{2}{bd}Z+\frac{1}{d}=0, \tag{10}$$

дискриминант которого $D=\frac{4}{b^2d^2}-\frac{4}{d}=\frac{4-4b^2d}{b^2d^2}=\frac{4}{b^2d^2}(1-b^2d)$, также имеет два решения:

$$Z_{1,2}=\frac{\frac{2}{bd}\pm\frac{2}{bd}\sqrt{1-b^2d}}{2}=\frac{1}{bd}(1\pm\sqrt{1-b^2d}). \tag{11}$$

При этом

$$V_1\cdot V_2=1\in Q_p,\ Z_1Z_2=\frac{1}{d}\notin Q_p, \tag{12}$$

т.е. корни V_1 и V_2 — одновременно либо квадратичные вычеты, либо квадратичные невычеты, а один из корней Z_1 и Z_2 — всегда квадратичный вычет, а другой — квадратичный невычет.

Уравнения (8) и (10) эквивалентны уравнениям

$$\frac{2V}{1+V^2} = b, \tag{13}$$

$$\frac{2Z}{1+dZ^2} = b, \tag{14}$$

которые выполняются для V_1, V_2 и Z_1, Z_2 соответственно.

Если $V_1 \in Q_p$ (при этом также $V_2 \in Q_p$, как показано выше), то обозначим Z_1 тот из корней уравнения (10), который является квадратичным вычетом. В ином случае (если $V_1 \notin Q_p$), обозначим Z_1 тот из корней уравнения (10), который является квадратичным невычетом. Тогда $V_1 Z_1 \in Q_p, V_2 Z_1 \in Q_p, \frac{Z_1}{V_1} \in Q_p, \frac{Z_1}{V_2} \in Q_p$.

Обозначим

$$y_1 = \sqrt{V_1 Z_1},\ y_2 = -y_1,\ y_3 = \sqrt{V_2 Z_1},\ y_4 = -y_3,$$

$$x_1 = \sqrt{\frac{Z_1}{V_1}},\ x_2 = -x_1,\ x_3 = \sqrt{\frac{Z_1}{V_2}},\ x_4 = -x_3.$$

Тогда

$$x_i y_i = Z_1,\ i = \overline{1,4}; \tag{15}$$

$$y_i / x_i = V_1,\ i = \overline{1,2};\ \ y_i / x_i = V_2,\ i = 3,4. \tag{16}$$

Подставив формулы (15) в уравнение (14), получим

$$\frac{2x_i y_i}{1+dx_i^2 y_i^2} = b, \tag{17}$$

т.е. (x_i, y_i), $i = \overline{1,4}$, являются решениями второго уравнения в системе (7). Аналогично, подставив формулы (16) в уравнение (13), получим $2\frac{y_i}{x_i} = b\left(1+\left(\frac{y_i}{x_i}\right)^2\right)$, откуда

$$\frac{2x_i y_i}{x_i^2 + y_i^2} = b. \tag{18}$$

Приравняв левые части в (17) и (18), получим

$$x_i^2 + y_i^2 = 1 + dx_i^2 y_i^2. \tag{19}$$

Из (19) следует, что пары (x_i, y_i) являются решениями первого уравнения системы (7).

Заметим, что если (x, y) — решения первого и второго уравнений системы (7), то пары (y, x), $(-x, -y)$, $(-y, -x)$ также являются их решениями. Именно эти пары получены в формулах (15) и (16). Однако точка $P = (a, b) \in T_2(E_p)$ имеет всего два корня степени 2. Чтобы избавиться от двух лишних точек, используем третье уравнение системы (7). Вначале покажем, что (x_i, y_i), $i = \overline{1,4}$, также являются решениями уравнения

$$a^2 = \left(\frac{x^2 - y^2}{1 - dx^2 y^2}\right)^2. \tag{20}$$

Действительно, из (6) следует, что

$$a^2 = \frac{1-b^2}{1-db^2}, \tag{21}$$

а из второго уравнения системы (7) получаем

$$b^2 = \frac{4x^2y^2}{(1+dx^2y^2)^2}. \tag{22}$$

Подставив (22) в правую часть (21), получим

$$a^2 = \frac{1-\dfrac{4x^2y^2}{(1+dx^2y^2)^2}}{1-\dfrac{4dx^2y^2}{(1+dx^2y^2)^2}} = \frac{(1+dx^2y^2)^2-4x^2y^2}{(1+dx^2y^2)^2-4dx^2y^2} = \frac{(x^2+y^2)^2-4x^2y^2}{(1+dx^2y^2)^2-4dx^2y^2} =$$

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

откуда следует (20). Поэтому выполняется только одно из равенств: либо $a = \dfrac{x^2-y^2}{1-dx^2y^2}$, либо $a = \dfrac{y^2-x^2}{1-dx^2y^2}$. Таким образом, из всех пар вида

$$(x, y),\ (-x,-y),\ (y,x),\ (-y,-x), \tag{23}$$

которые являются решениями первого и второго уравнений системы (7), только две будут решениями третьего уравнения этой системы. Исходя из левой части третьего уравнения (7), делаем вывод, что решениями будут такие две пары из (23), которые имеют вид $R_1 = (x, y)$ и $R_2 = (-x,-y)$. Именно точки R_1 и R_2 являются корнями степени 2 из точки $P = (a, b)$.

Теорема доказана.

Обозначим Z тот корень уравнения (10), для которого

$$VZ \in Q_p, \tag{24}$$

где V — любой из корней уравнения (8).

Следствие 1. Пусть $P = (a, b) \in T_2(E_p)$, $R = (x, y) \in E_p$, $P = 2R$. Тогда в принятых обозначениях $y^2 = \dfrac{(a+1)d \cdot Z^2 - a + 1}{2}$.

Доказательство. Поскольку $P = (a, b) \in T_2(E_p)$, согласно теореме 1 существуют решения V_1, V_2 уравнения (8) и решения Z_1, Z_2 уравнения (10). Вследствие (9) и (11) либо $V_1Z_1 \in Q_p$, либо $V_1Z_2 \in Q_p$, поэтому всегда можно выбрать Z в соответствии с (24). Если $P = 2R$, где $R = (x, y)$, то согласно теореме 1 (x, y) является решением системы (7). Тогда из третьего уравнения системы (7), учитывая (15), получаем $a = \dfrac{x^2-y^2}{1-dZ^2}$, откуда

$$x^2 - y^2 = a(1-dZ^2), \tag{25}$$

а из первого уравнения системы (7) имеем

$$x^2 + y^2 = 1 + dZ^2. \tag{26}$$

Вычитая (25) из (26), получаем $2y^2 = 1 + dZ^2 - a + adZ^2$, откуда

$$y^2 = \frac{(a+1)dZ^2 - a + 1}{2}. \tag{27}$$

Следствие доказано.

Следствие 2. Пусть $P = (a, b) \in T_2(E_p)$, V и Z выбраны согласно (9), (11) и (24), $R = (x, y) \in E_p$, $P = 2R$. Тогда

$$1 - y^2 = \frac{(a+1)(1 - dZ^2)}{2}. \tag{28}$$

Доказательство выполняется соответствующим преобразованием (27).

Следствием теоремы 1 также можно считать следующий алгоритм вычисления корня степени 2 из точки $P = (a, b) \in T_2(E_p)$.

Алгоритм 1.

Вход: a, b такие, что $1 - b^2 \in Q_p$.

1. Вычислить $s_1 = \sqrt{1 - b^2}$, $s_2 = \sqrt{1 - db^2}$ (любые из двух возможных корней).
2. Если $(1 - s_1)(1 - s_2) \in Q_p$, то $s_2 \leftarrow p - s_2$.
3. Вычислить $Z = (bd)^{-1}(1 - s_2)$.
4. Вычислить $y = \sqrt{\dfrac{(a+1)dZ^2 - a + 1}{2}}$ (любой из двух возможных корней).
5. Вычислить $x = y^{-1}Z$.

Выход: $R_1 = (x, y)$, $R_2 = (-x, -y)$.

Вычислительная сложность. В алгоритме используются 16 операций умножения (каждая порядка $(\log p)^2$ битовых операций), шесть операций вычисления обратного по mod p (каждая порядка $(\log p)^3$ битовых операций), три операции вычисления квадратичного корня по mod p (каждая порядка $(\log p)^3$ битовых операций), а также десять операций сложения и вычитания, время работы которых значительно меньшее. Таким образом, вычислительную сложность алгоритма можно оценить как $O(\log^3 p)$.

КРИТЕРИЙ ДЕЛИМОСТИ ТОЧКИ КРИВОЙ ЭДВАРДСА НА 4

Сформулируем критерий делимости точки $P = (a, b)$ на 4.

Теорема 2. Пусть $P = (a, b) \in T_2(E_p)$. Обозначим s_1 произвольный корень из $1 - b^2$, а s_2 — корень из $1 - b^2 d$ такой, что $(1 - s_1)(1 - s_2) \notin Q_p$.

Тогда следующие условия равносильны:

$$P \in T_4(E_p);$$

$$(1 - s_1)s_2(1 - s_2) \notin Q_p. \tag{29}$$

Доказательство. Пусть $P = 2Q$, где $Q = (x, y)$.

Заметим, что вследствие (9), (11) и (12)

$$(1 - s_1)(1 + s_1) = b^2 \in Q_p, \tag{30}$$

$$(a+1)(1 - s) = db^2 \notin Q_p, \tag{31}$$

где s — произвольный (любой из двух возможных) корень из $1 - b^2 d$.

Поэтому для произвольного корня s_1 из величины $1-b^2$ всегда будет существовать единственный корень s_2 из величины $1-b^2 d$ такой, что

$$(1-s_1)(1-s_2)\notin Q_p. \tag{32}$$

В принятых обозначениях и согласно (9), (11), (30) и (31) выражение (32) эквивалентно тому, что $Z=\dfrac{1-s_2}{bd}$. Тогда согласно (28) и с учетом (32) имеем

$$1-y^2=\frac{a+1}{2}(1-dZ^2)=\frac{a+1}{2}s_2(1-s_2)\frac{2}{b^2d}=\frac{(a+1)s_2(1-s_2)}{b^2d}.$$

Поскольку по предположению $d\notin Q_p$, условие $\left(\dfrac{1-y^2}{p}\right)=1$ равносильно условию $(a+1)s_2(1-s_2)\notin Q_p$, т.е. оба условия в (29) эквивалентны.

Теорема доказана.

Замечание 1. Алгоритмы получения корня степени 4 из точки $P\in T_4(E_p)$ можно реализовать, либо непосредственно используя теорему 2, либо последовательным двукратным применением алгоритма 1.

Замечание 2. Если $|E_p|=4n$, где n — простое число (большое), то для любой точки $P=(a,b)$ выполняется одно из двух условий: $1-b^2\in Q_p$, либо $1-a^2\in Q_p$. Значит, это эквивалентно тому, что $P=(a,b)\in T_2(E_p)$ либо $P'=(b,a)\in \in T_2(E_p)$.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ГЕНЕРАЦИИ БАЗОВОЙ ТОЧКИ КРИВОЙ ЭДВАРДСА

Рассмотрим три алгоритма генерации базовой точки: классический (применяется, например, в алгоритме ДСТУ 4145:2002 [9]), основанный на теореме 1 и основанный на теореме 2. Проведем их сравнительный анализ по быстродействию и некоторым другим факторам.

Алгоритм 2 (ДСТУ 4145:2002).

Вход: эллиптическая кривая $E(F_p)$.

1. Случайно выбрать точку $P=(x,y)\in E(F_p)$.
2. Вычислить nP.
3. Если $nP\neq O$, вернуться к п. 1.

Выход: $P=(x,y)$ — базовая точка.

Вычислительная сложность. В алгоритме используются примерно $\log p$ сложений точек. При каждом их сложении выполняется шесть умножений ($6\log^2 p$ битовых операций), шесть делений с остатком ($6\log^2 p$ битовых операций) и два алгоритма Евклида ($2\log^3 p$ битовых операций). Поэтому общее время работы алгоритма составляет $96\log^3 p+4\log^4 p$ (с учетом того, что среднее количество шагов до желаемого результата равно четырем).

Следующий алгоритм 3 основан на теореме 1. В п. 2 алгоритма 3 проверяется выполнение условия 2 теоремы 1; если оно выполняется, то полученная точка делится на 2 и для построения базовой точки ее достаточно удвоить. В протвном случае точка, полученная перестановкой координат, будет делиться на 2, а точка, полученная в результате ее удвоения, будет делиться на 4, т.е. будет базовой точкой.

Алгоритм 3.

Вход: эллиптическая кривая $E(F_p)$.

1. Случайно выбрать точку $P=(a,b)\in E(F_p)$.
2. Если $a\in\{0,1,-1\}$, то перейти к п. 1.
3. Если $1-b^2\notin Q_p$, то $c\leftarrow a$, $a\leftarrow b$, $b\leftarrow c$.
4. Вычислить $P\leftarrow 2P$.

Выход: P — базовая точка.

Вычислительная сложность. В алгоритме используются одно умножение и одно деление с остатком ($2\log^2 p$ битовых операций), одна проверка квадратичности ($2\log^3 p$ битовых операций) и одно удвоение точки ($12\log^2 p+2\log^3 p$ битовых операций). Всего $4\log^3 p+14\log^2 p$ битовых операций.

Следующий алгоритм 4 построен аналогично алгоритму 3, но снован на теореме 2. Он фактически является алгоритмом проверки делимости точки на 4. Действительно, любая точка $P\in T_4(E_p)$, такая, что $P\neq O$, где $O=(1,0)$, является базовой точкой кривой.

Алгоритм 4.

Вход: эллиптическая кривая $E(F_p)$.

1. Случайно выбрать точку $P=(a,b)\in E(F_p)$.
2. Если $a\in\{0,1,-1\}$, то перейти к п. 1.
3. Если $1-b^2\notin Q_p$, то $c\leftarrow a$, $a\leftarrow b$, $b\leftarrow c$.
4. Вычислить $s_1=\sqrt{1-b^2}$, $s_2=\sqrt{1-ab^2}$ (любые из двух возможных корней).
5. Если $(1-s_1)(1-s_2)\in Q_p$, то $s_2\leftarrow p-s_2$.
6. Если $(a+1)s_2(1-s_2)\in Q_p$, то перейти к п. 1.

Выход: P — базовая точка.

Вычислительная сложность. В алгоритме используются два умножения и два деления с остатком ($4\log^2 p$ битовых операций), одно вычисление корня ($2\log^3 p$ битовых операций) и две проверки квадратичности ($4\log^3 p$ битовых операций). Отметим, что алгоритм 4 является вероятностным; при этом среднее количество шагов до желаемого результата равно двум. Поэтому время его работы составляет $12\log^3 p+8\log^2 p$ битовых операций.

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ КОРНЕЙ ДРУГИХ СТЕПЕНЕЙ

Приведем критерии и алгоритмы вычисления корней (точек деления) степени n, $2n$, $4n$ и степени k при $1<k<4n$, $(k,4n)=1$. Хотя эти критерии и не имеют таких очевидных приложений, как критерии делимости точки на 2 и на 4, но без них вопросы делимости точек кривой и вычисления точек деления не будут решены полностью.

Заметим, что корни степени $2n$ и $4n$ можно вычислить, используя последовательно алгоритмы вычисления корня степени 2 и степени n. Также будут приведены соответствующие критерии делимости точки.

Поскольку все точки кривой E_p образуют циклическую группу порядка $4n$, справедливы следующие утверждения:

— ровно две точки кривой E_p (точка второго порядка $D=(-1,0)$ и точка первого порядка $O=(1,0)$) делятся на $2n$;

— ровно одна точка кривой E_p (точка $O=(1,0)$) делится на $4n$;

— ровно четыре точки кривой E_p (точки $D = (1,0)$, $F = (0,1)$, $-F = (0,-1)$ и $O = (1,0)$) делятся на n;

— каждая точка кривой делится на k при $1 < k < 4n$, $(k, 4n) = 1$.

Кроме того, как было доказано раньше, ровно n точек делятся на 4 (все базовые и точка $O = (1, 0)$) и ровно $2n$ точек делятся на 2 (все базовые и точка $O = (1,0)$ и все точки вида $2P$ (P — базовая точка)).

Из всего приведенного выше следуют критерии и алгоритмы делимости точек кривой на n, $2n$, $4n$ и на k, $1 < k < 4n$, $(k, 4n) = 1$.

Приведем теперь алгоритмы вычисления корней соответствующих степеней из точек кривой. Для этого понадобятся формула 4 и точка $G = (x, y)$, которая является образующим элементом группы E_p. Ее можно получить стандартным алгоритмом для нахождения образующего элемента группы или как корень степени 4 из базовой точки P.

Алгоритм 5. Вычисление корня степени $2n$ из точки $Z \in T_{2n}(E_p)$.

Вход: точка $Z = D = (-1, 0)$ (или $Z = O = (0,-1)$).

Если $Z = D$, то $S = G$, иначе $S = 2G$.

Выход: S.

Алгоритм вычисления корня степени $4n$ не рассматривается, поскольку корнем степени $4n$ из точки $O = (0,-1)$ является любая точка кривой.

Алгоритм 6. Вычисление корня степени k из точки кривой при $1 < k < n$, $(k, 4n) = 1$.

Вход: произвольная точка $Z \in E_p$.

1. Используя алгоритм Евклида, вычислить $u, v \in Z$ такие, что $uk + v4n = 1$.

2. Вычислить $u = u \bmod 4n$.

Выход: $S = uZ$.

ЗАКЛЮЧЕНИЕ

Наиболее существенными математическими результатами настоящей работы являются:

— критерий делимости точки кривой Эдвардса на 2 и на 4, а также соответствующие алгоритмы деления точек;

— критерий делимости точки на n (простое число, равное порядку циклической подгруппы группы точек кривой Эдвардса) и на произвольное число k, взаимно простое с n.

Практическими результатами, основанными на перечисленных математических, являются, в первую очередь, новые алгоритмы генерации базовой точки кривой Эдвардса. Также приведен сравнительный анализ новых и классических алгоритмов генерации базовой точки. Кроме этого, получены алгоритмы вычисления корня произвольной степени из точки кривой:

— алгоритмы 3 и 4 имеют одинаковый порядок временной сложности (т.е. если учитывать лишь степень полинома, описывающего время работы, без учета мультипликативной константы) и значительно быстрее алгоритма 2;

— если использовать более точные оценки, то в порядке снижения быстродействия алгоритмы следуют в таком порядке: 3, 4 и 2;

— хотя алгоритм 4 немного уступает алгоритму 3 по быстродействию, у него есть одно бесспорное преимущество — использование только операции в конечном поле, над которым задана кривая без операций непосредственно на кривой.

СПИСОК ЛИТЕРАТУРЫ

1. Edwards H.M. A normal form for elliptic curves // Bulletin of the AMS. — 2007. — **44**(3). — P. 393–422.
2. Bernstein D.J., Lange T. Faster addition and doubling on elliptic curves // ASIACRYPT 2007. — LNCS. — 2007. — **4833.** — P. 29–50.
3. Bernstein D.J., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards curves // AFRICACRYPT 2008. — LNCS. — 2008. — **5023.** — C. 389–405.
4. Hisil H., Koon-Ho Wong K., Carter G., Dawson E. Twisted Edwards curves revisited // ASIACRYPT 2008. — LNCS. — 2008. — **5350.** — P. 326–343.
5. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем // Кибернетика и системный анализ. — 2015. — **51**, № 2. — С. 3–12.
6. Ковальчук Л.В., Беспалов О.Ю., Огнєв П.В. Рекурентні алгоритми обчислення кореню довільного степеню у кільці лишків // Правове, нормативне та метрологічне забезпечення захисту інформації в Україні. — 2013. — Вип. 25. — С. 58–66.
7. Бессалов А.В., Цыганкова О.В. Новые свойства кривой Эдвардса над простым полем // Радиотехника. — 2015. — № 180. — С. 137–143.
8. Лидл Р., Нидеррайтер Р. Конечные поля. — М: Мир., 1988. — Т. 1. — С. 273.
9. Державний стандарт України ДСТУ 4145:2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. — 2002. — 31 с.

Надійшла до редакції 18.03.2016

Л.В. Ковальчук, А.В. Бессалов, О.Ю. Беспалов

АЛГОРИТМИ ГЕНЕРАЦІЇ БАЗОВОЇ ТОЧКИ НА КРИВІЙ ЕДВАРДСА З ВИКОРИСТАННЯМ КРИТЕРІЇВ ПОДІЛЬНОСТІ ТОЧКИ

Анотація. Сформульовано та доведено критерії подільності точки кривої Едвардса на 2, 4 та інші натуральні числа. З використанням цих критеріїв побудовано алгоритми добування кореня довільного степеня у групі точок кривої Едвардса, а також отримано нові алгоритми генерації базової точки кривої, котрі, як показав порівняльний аналіз, мають низку переваг.

Ключові слова: криві Едвардса, подільність точки, генерація базової точки.

L.V. Kovalchuk, A.V. Bessalov, O.Yu. Bespalov

ALGORITHMS OF BASE POINT GENERATION ON EDWARDS CURVE USING POINT DIVISIBILITY CRITERIA

Abstract. New criteria for Edwards curve point divisibility by 2, 4, and other natural numbers are obtained and proved in this paper. These results are used to construct new algorithms for arbitrary power root extraction on the Edwards curve group and to create new algorithms of base point generation that are proved to have some advantages.

Keywords: Edwards curves, point divisibility, base point generation.

Ковальчук Людмила Васильевна,
доктор техн. наук, доцент Физико-технического института Национального технического университета Украины «Киевский политехнический институт», e-mail: lusi.kovalchuk@gmail.com.

Бессалов Анатолий Владимирович,
доктор техн. наук, профессор Физико-технического института Национального технического университета Украины «Киевский политехнический институт», e-mail: bessalov@ukr.net.

Беспалов Алексей Юрьевич,
аспирант Физико-технического института Национального технического университета Украины «Киевский политехнический институт», e-mail: alexb5e@gmail.com.