АЛГОРИТМЫ ГЕНЕРАЦИИ БАЗОВОЙ ТОЧКИ С ИСПОЛЬЗОВАНИЕМ КРИТЕРИЕВ ДЕЛИМОСТИ ТОЧКИ КРИВОЙ

ВСТУПЛЕНИЕ

Эллиптические кривые в форме Эдвардса над простым полем на данный момент являются наиболее быстрыми и перспективными для использования в асимметричных криптосистемах. Наиболее важными их особенностями являются следующие:

- рекордная скорость,
- универсальность закона сложения,
- возможность представления нейтрального элемента в аффинных координатах.

Эти свойства были выявлены и обоснованы уже в первых работах [1, 2].

Симметрия точек кривых Эдвардса относительно обеих координат влечет за собой интересные и удобные особенности этих кривых. Исключая неактуальные изоморфные кривые, в кривых Эдвардса достаточно использовать лишь один параметр d вместо двух обычных a и b классической кривой в каноничной форме Вейерштрасса.

В роботе [3] авторы обобщили и расширили класс кривых Эдвардса добавлением нового параметра a. Они назвали этот класс скрученными кривыми Эдвардса (twisted Edwards curves). Дальнейший прогресс в исследовании новых свойств этого класса скрученных кривых Эдвардса получен в работе [4], в которой найдены альтернативные формулы для закона сложения точек кривой, определены особенности точек для этого закона и предложен метод расчета координат суммы точек в расширенных проективных координатах. Авторам удалось снизить количество операций при сложении различных между собой 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 увеличивает быстродействие операции сложения точек примерно в 1,36 раз.

Также в работе [5] были приведены необходимые и достаточные условия того, что эллиптическая кривая, заданная в канонической форме, является изоморфной некоторой

кривой Эдвардса. На основе этих критериев было найдено точное число кривых Эдвардса над произвольным конечным полем в зависимости от его характеристики.

В этой статье сформулированы и обоснованы критерии делимости точки кривой Эдвардса на произвольное натуральное число. С использованием этих критериев 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 и алгоритмов разработаны новые алгоритмы вычисления координат базовой точки кривой (или генератора криптосистемы как точки простого порядка n). Также выполнен детальный сравнительный анализ новых и классических алгоритмов вычисления базовой точки кривой, и показано, что предложенные в этой работе алгоритмы имеют выигрыш в быстродействии более, чем в 20 раз. Этот выигрыш возрастает с ростом характеристики простого поля, над которым построена кривая.

Заметим, что критерии делимости и алгоритмы получения корня в группе точек эллиптической кривой, приведенные в этой статье, во многом похожи на аналогичные критерии, полученные в [6] для простых полей и конечных колец. Однако для эллиптических кривых эти алгоритмы имеют намного большее прикладное значение.

1. КРИТЕРИЙ ДЕЛИМОСТИ ТОЧКИ КРИВОЙ НА 2 И НА 4

Пусть кривая Эдвардса задана уравнением:

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

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

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

Далее мы будем использовать именно форму (2).

Кривую Эдвардса над полем F_p мы будем обозначать E_p, а её произвольную точку P, имеющую координаты (x, y), где $x, y \in F_p$, обозначим через $P = (x, y)$ или просто (x, y).

Как известно, множество точек кривой образует группу относительно некой специфической операции, которую, вследствие её коммутативности, принято называть сложением. Тут мы будем использовать так называемый модифицированный закон сложения, который определяется следующим образом:

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

Этот закон сложения выводится из «классического» методом выполнения так называемого «поворота на 90° вправо» точек кривой [7]. Преимущество такого закона сложения состоит в том, что точка, обратная к $P = (x, y)$, будет иметь вид $-P = (x, -y)$, как и для эллиптической кривой, заданной в форме Вейерштрасса. Нейтральным элементом будет точка $O = (1,0)$.

Как правило, множество точек кривой Эдвардса (2) образует циклическую группу, порядок которой кратен 4. В криптографических приложениях используются исключительно такие кривые Эдвардса, порядки которых $N(E_p) = 4n$, где n – большое (от 180 бит) простое число. Поэтому далее мы будем рассматривать только кривые такого порядка.

Согласно свойствам циклической группы [8], в группе E_p обязательно должны существовать две точки четвёртого порядка: $F = (0,1)$ и $-F = (0,-1)$ и одна точка второго порядка: $D = (-1,0)$. Также в ней будет $\varphi(n) = n - 1$ точек порядка n и 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 мы называем базовой точкой кривой E_p.

Далее нам понадобятся следующие формулы, которые являются простым следствием закона сложения (3). Для произвольной точки $P=(x,y)$ справедливо:

$$\begin{gathered} D=2F; \\ P+D=P-D=(-x,-y); \\ P+D-F=P+F=(-y,x); \\ P+3F=P+D+F=(y,-x); \end{gathered} \tag{4}$$

Для дальнейшего изложения нам понадобятся такие определения.

Определение 1: Пусть $P\in E_p,\quad k\in N$. Будем говорить, что точка P делится на k, если $\exists R\in E_p : P=kR$, где под выражением kR мы понимаем k-кратное сложение R (как принято говорить, умножение точки R на скаляр k, или – скалярное умножение).

Множество точек E_p, которые делятся на k, мы будем обозначать $T_k(E_p)$ или $T_k(p)$.

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

Цель данной работы – сформулировать критерии делимости точки на $k,\ 1\le k\le 4n$, с условиями, удобными для вычислений, и показать, как эти критерии могут быть использованы в криптографических приложениях. Заметим, что для 3-х значений k, таких, что $k\mid 4n$, справедлив следующий критерий делимости: $P\in T_k(E_p)\Leftrightarrow \frac{4n}{k}P=O$.

2. КРИТЕРИЙ ДЕЛИМОСТИ ТОЧКИ НА 2

В работе [7] был сформулирован и доказан критерий делимости точки кривой на 2. Тут мы еще раз его приведем, правда, с более детальным доказательством.

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

1) $P \in T_2\left(E_p\right)$;

2) $$\left(\frac{1-b^2}{p}\right)=1 \qquad (5)$$

Доказательство:

1. Докажем, что из условия 1) следует условие 2). Пусть $P=(a,b)\in T_2\left(E_p\right)$, то есть $\exists R=(x,y): P=2R$. Тогда, согласно (2),

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

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

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

Из 1-го и 2-го уравнений системы (7) получаем $\frac{2xy}{x^2+y^2}=b$, откуда $2\frac{y}{x}=b\left(1+\left(\frac{y}{x}\right)^2\right)$. Обозначим в последнем уравнении $V=\frac{y}{x}$, получим уравнение $2V=b(1+V^2)$, или

$$V^2-2b^{-1}V+1=0. \qquad (8)$$

Вследствие условия 1) теоремы, уравнение (8) имеет решение. Как следствие, его дискриминант является квадратичным вычетом по $mod\ p$, то есть $D=4b^{-2}-4=4\left(b^{-2}-1\right)=\frac{4(1-b^2)}{b^2}$ – квадратичный вычет по модулю p. Так как

$4b^{-2} \in Q_p$, то последнее условие эквивалентно условию $\left(\frac{D}{p}\right) = \left(\frac{1-b^2}{p}\right) = 1$, то есть выполняется условие 2) теоремы 1.

2. Докажем, что из условия 2) следует условие 1).

Пусть $\left(\frac{1-b^2}{p}\right) = 1$. Покажем, что $\exists x, y \in F_p$, которые являются решениями системы (7) при заданных $a, b \in F_p$, где $P = (a,b) \in T_2\left(E_p\right)$.

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

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

Поскольку $P = \left(a,b\right) \in E_p$, то есть выполняется условие (6), получаем $\frac{1-b^2}{1-db^2} = a^2$, откуда $\left(1-db^2\right)\left(1-b^2\right) \in Q_p$, и, как следствие, $\left(\frac{1-db^2}{p}\right) = \left(\frac{1-b^2}{p}\right) = 1$.

Поэтому уравнение

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

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

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

При этом

$$V_1 \cdot V_2 = 1 \in Q_p,\ Z_1 Z_2 = \frac{1}{d} \notin Q_p, \tag{12}$$

то есть корни V_1 и V_2 одновременно либо квадратичные вычеты, либо квадратичные невычеты, а из корней Z_1 и Z_2 один всегда квадратичный вычет, а второй – квадратичный невычет.

Далее, уравнения (8) и (10) эквивалентны, соответственно, уравнениям

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

и

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

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, который является квадратичным невычетом. Тогда $V_1 Z_1 \in Q_p$, $V_2 Z_1 \in Q_p$.

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 в уравнение (10), получаем

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

то есть (x_i, y_i), $i = \overline{1,4}$ являются решениями 2-го уравнения в системе (7). Аналогично, подставив в (8), получаем $2\frac{y_i}{x_i} = b\left(1 + \left(\frac{y_i}{x_i}\right)^2\right)$, откуда

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

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

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

то есть пары (x_i, y_i) являются решениями 1-го уравнения системы (7).

Заметим, что если (x, y) являются решениями 1-го и 2-го уравнений системы (7), то пары $(y, x), (-x, -y), (-y, -x)$ также являются их решениями. Именно эти пары мы получили в формулах (15) и (16). Однако, у точки $P = (a, b) \in T_2(p)$ существует всего два корня 2-й степени. Чтобы избавиться от двух лишних точек, используем 3-е уравнение системы (7). Сначала покажем, что (x_i, y_i), $i = \overline{1,4}$ также являются решениями системы

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

Действительно, из (6) следует, что

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

а из 2-го уравнения системы (7) получаем

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

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

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

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

откуда следует (20).

Поэтому выполняется ровно одно из равенств: либо $a = \dfrac{x^2-y^2}{1-dx^2y^2}$, либо $a = \dfrac{y^2-x^2}{1-dx^2y^2}$.

Поэтому из всех пар вида

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

которые являются решениями 1-го и 2-го уравнений системы (7), только две будут решениями 3-го уравнения этой системы. Исходя из вида левой части 3-го уравнения (7), делаем вывод, что это пары вида $R_1 = (x,y)$ и $R_2 = (-x,-y)$.

Именно эти точки R_1 и R_2 являются корнями второй степени 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 наших обозначениях $y^2 = \dfrac{(a+1)d \cdot Z^2 - a + 1}{2}$.

Доказательство**:** Так как $P=(a,b)\in T_2(E_p)$, то, 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 мы всегда можем 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 3-го 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 1-го уравнения системы (7) получаем

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

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 применением (27).

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

Алгоритм 1: Вычисление корня 2-ой степени из точки $P=(a,b)\in T_2(E_p)$.

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

1. Вычислить

$$V_1 = b^{-1}\left(1-\sqrt{1-b^2}\right),\ V_1 Z_1 = \frac{1}{b^2 d}\left(1-\sqrt{1-b^2}\right)\left(1-\sqrt{1-bd^2}\right),\ Z_1 = (bd)^{-1}\left(1-\sqrt{1-bd^2}\right)$$

(или $Z_1 = bd^{-1}\left(1+\sqrt{1-b^2 d}\right)$).

2. Если $V_1 Z_1 \notin Q_p$, то $Z_1 = (bd)^{-1}\left(1+\sqrt{1-bd^2}\right)$ (или $Z_1 = bd^{-1}\left(1+a^{-2}\sqrt{1-b^2}\right)$).

3. Вычислить $y = \sqrt{\dfrac{(a+1)dZ_1^2 - a + 1}{2}}$.

4. Вычислить $x = y^{-1} Z_1$.

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

Вычислительная сложность: Алгоритм использует 16 операций умножения (каждая порядка $(\log p)^2$ битовых операций), 6 операций вычисления обратного по модулю (каждая порядка $(\log p)^3$ битовых операций), 3 операции вычисления квадратичного корня по $mod\ p$ (каждая порядка $(\log p)^3$ битовых операций), а также 10 операций сложения и вычитания, время работы которых значительно меньше. Итак, вычислительную сложность алгоритма можно оценить как $O(\log^3 p)$.

3. КРИТЕРИЙ ДЕЛИМОСТИ ТОЧКИ НА 4

Теперь мы готовы сформулировать критерий делимости точки $P = (a, b)$ на 4.

Теорема 2: Пусть $P = (a, b) \in E_p$. Тогда, следующие условия равносильны:

1) $P \in T_4\left(E_p\right)$;

2) $$\begin{cases} 1-b^2 \in Q_p; \\ (a+1)\left(\sqrt{1-b^2}-1\right) \in Q_p. \end{cases} \qquad (29)$$

Доказательство:

Сначала докажем, что условие 1) равносильно совокупности систем

$$\begin{cases} 1-b^2 \in Q_p \\ \left(1-\sqrt{1-b^2}\right)\left(1-\sqrt{1-db^2}\right) \notin Q_p \\ -(a+1)\left(1-\sqrt{1-b^2 d}\right) \notin Q_p \end{cases} \tag{30}$$

и

$$\begin{cases} 1-b^2 \in Q_p \\ \left(1-\sqrt{1-b^2}\right)\left(1+\sqrt{1-db^2}\right) \notin Q_p \\ -(a+1)\left(1+\sqrt{1-b^2 d}\right) \notin Q_p \end{cases} \tag{31}$$

Потом докажем, что совокупность этих систем равносильна системе (29).

1. Необходимость.

Если $P \in T_4\left(E_p\right)$, то, очевидно, $P \in T_2\left(E_p\right)$, а значит $1-b^2 \in Q_p$, то есть выполняется 1-ое условие системы (29). Тогда существуют решения V_1, V_2 и Z_1, Z_2 уравнений (8) и (10), которые определяются формулами (9) и (11), соответственно.

Пусть $R=(x,y) \in E_p$, $2R=P$. Тогда, согласно (27), $y^2 = \dfrac{(a+1)dZ^2 - a + 1}{2}$, где Z – тот из корней (10), для которого $V_1 Z \in Q_p$. Пусть, для определенности, $V_1 = b^{-1}\left(1-\sqrt{1-b^2}\right)$. Если $Z = \dfrac{1}{bd}\left(1-\sqrt{1-b^2 d}\right)$, значит $b^{-1}\left(1-\sqrt{1-b^2}\right)\cdot\dfrac{1}{bd}\left(1-\sqrt{1-b^2 d}\right) \in Q_p$, что равносильно $\left(1-\sqrt{1-b^2}\right)\left(1-\sqrt{1-b^2 d}\right) \notin Q_p$, то есть выполняется 2-ое условие в (30). В этом случае, согласно (18), $1-y^2 = \dfrac{a+1}{2}\cdot\left(1-dZ^2\right) = -\dfrac{a+1}{b^2 d}\left(1-\sqrt{1-b^2 d}\right)$.

Так как $P \in T_4\left(E_p\right)$, то $R \in T_2\left(E_p\right)$, как следствие, $1-y^2 \in Q_p$, что эквивалентно условию $-(a+1)\left(1-\sqrt{1-b^2 d}\right) \notin Q_p$, то есть выполняется 3-е условие из (30).

Аналогично, если $Z=\frac{1}{bd}\left(1+\sqrt{1-b^2d}\right)$, то выполняются 2-ое и 3-е условия в (31). Необходимость доказана.

2. Достаточность.

Пусть выполняется одна из систем (30) или (31). Из 1-го условия этих систем и теоремы 1 получаем, что $P\in T_2\left(E_p\right)$, то есть $\exists R=(x,y)\in E_p : P=2R$. Теперь достаточно показать, что $R\in T_2\left(E_p\right)$, что, согласно теореме 1, эквивалентно выполнению условия $1-y^2\in Q_p$.

Согласно следствию 2 и (28),

$$1-y^2=\frac{(a+1)\left(1-dZ^2\right)}{2}, \tag{32}$$

где Z – один из корней (10), для которого $V_1Z\in Q_p$.

Если выполняется система (30), то, согласно второму условию этой системы, $Z=\frac{1}{bd}\left(1-\sqrt{1-b^2d}\right)$, тогда

$$1-y^2=\frac{a+1}{2}\left(1-dZ^2\right)=\frac{a+1}{2}\cdot\frac{-2}{b^2d}\left(1-\sqrt{1-b^2d}\right)=\frac{-(a+1)}{b^2d}\left(1-\sqrt{1-b^2d}\right)\in Q_p,$$

вследствие 3-го условия системы (30), учитывая, что $b^2\in Q_p, d\notin Q_p$.

Аналогично, если выполняется система (31), то $Z=\frac{1}{bd}\left(1+\sqrt{1-b^2d}\right)$, вследствие 2-го условия этой системы, а 3-е условие системы обеспечивает выполнение условия $1-y^2\in Q_p$.

Теперь докажем, что совокупность систем (30) и (31) равносильна системе (29).

Во-первых, заметим, что поскольку $\left(1-\sqrt{1-db^2}\right)\times\left(1+\sqrt{1-db^2}\right)=db^2\notin Q_p$, то либо выполняется второе условие системы (30), либо выполняется второе условие системы

(31). Аналогично, либо выполняется третье условие системы (30), либо выполняется третье условие системы (31). Если выполняется система (30) или (31), то, перемножив левые и правые части второго и третьего условий системы, получаем $-(a+1)\left(1-\sqrt{1-b^2}\right)=(a+1)\left(\sqrt{1-b^2}-1\right)\in Q_p$. А значит, если выполняется одна из систем (30) или (31), то выполняется и (29).

Аналогично, если выполняется (29), то $(a+1)\left(\sqrt{1-b^2}-1\right)\in Q_p$, следовательно, $(a+1)\left(\sqrt{1-b^2}-1\right)\left(1-\sqrt{1-db^2}\right)^2\in Q_p$, а, значит, левые части второго и третьего выражений системы (30) либо одновременно квадратичные вычеты (тогда выполняются условия системы (30)), либо одновременно квадратичные невычеты (тогда выполняются условия системы (31)).

Теорема доказана.

Замечание:

1) Алгоритмы получения корня 4-й степени из точки $P\in T_4\left(E_p\right)$ могут быть реализованы либо непосредственно, с использованием теоремы 2, либо последовательным двукратным применением алгоритма 1.

2) Если $\left|E_p\right|=4n$, где n – (большое) простое число, то для любой точки $P=(a,b)$ либо $1-b^2\in Q_p$, либо $1-a^2\in Q_p$.

Значит, либо $P=(a,b)\in T_2\left(E_p\right)$, либо $P'=(b,a)\in T_2\left(E_p\right)$.

4. СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ГЕНЕРАЦИИ БАЗОВОЙ ТОЧКИ КРИВОЙ ЭДВАРДСА.

Мы рассмотрим три алгоритма генерации базовой точки – «классический» (применяется, например, в алгоритме ДСТУ 4145-2002), алгоритм, который основывается на теореме 1, и алгоритм, который основывается на теореме 2. Проведём 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 $nP\neq O$, возвращаемся к шагу 1.

Выход: $P=(x,y)$ – базовая точка.

Время работы: Алгоритм использует примерно $\log p$ сложений точек. При каждом сложении точек выполняется 6 умножений ($6\log^2 p$ битовых операций), 6 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 успеха равно четырём).

Следующий алгоритм использует теорему 1.

Алгоритм 3:

Вход: эллиптическая кривая $E(F_p)$.

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

Выход: P – базовая точка.

Время работы: Алгоритм использует одно умножение и одно деление с остатком ($2\log^2 p$ битовых операций), одну проверку 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 использует теорему 2 и является, фактически, алгоритмом проверки делимости точки на 4. Действительно, любая точка $P \in T_4\left(E_p\right)$, такая, что $P \neq O$, где $O = (1,0)$, является базовой точкой кривой.

Алгоритм 4:

Вход: эллиптическая кривая $E\left(F_p\right)$.

1. Случайно выбрать точку $P = (a,b) \in E\left(F_p\right)$.

2. Если $1 - b^2 \notin E_p$, то $c \leftarrow a,\ a \leftarrow b,\ b \leftarrow a$.

3. Если $(a+1)\left(\sqrt{1-b^2} - 1\right) \notin Q_p$, то переходим к шагу 1.

Выход: P – базовая точка.

Время работы: Алгоритм использует 2 умножения и 2 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). Среднее количество шагов до успеха равно двум.

Поэтому время его работы составляет $12\log^3 p + 8\log^2 p$ битовых операций.

5. АЛГОРИТМЫ ВЫЧИСЛЕНИЯ КОРНЕЙ ДРУГИХ СТЕПЕНЕЙ

В этом разделе мы приведем алгоритмы вычисления корня степени n, $2n$, $4n$ и степени k, где $1 < k < 4n, (k,4n) = 1$. Заметим, что корни степени $2n$ та $4n$ 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 $4n$, то справедливыми будут следующие утверждения:

- ровно две точки кривой E_p делятся на $2n$ – это точка второго порядка $D=(-1,0)$ и точка первого порядка $O=(1,0)$;
- ровно одна точка кривой E_p делится на $4n$ – это точка $O=(1,0)$;
- ровно четыре точки кривой делятся на n – это точки $D=(1,0),\quad F=(0,1),\quad -F=(0,-1)$ и $O=(1,0)$;
- каждая точка кривой делится на k, где $1<k<4n$, $(k,4n)=1$.

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

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

Приведём теперь алгоритмы вычисления корней соответствующих степеней из точек кривой. Для них нам понадобится точка $G=(x,y)$, которая является образующим элементом группы E_p. Она может быть получена стандартным алгоритмом для нахождения образующего элемента группы, или как корень 4-й степени 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 $Z=O=(0,-1)$).

Выход: точка $S\in E_p$, такая, что $2nS=D$ (или $2nS=O$).

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

Вместо алгоритма вычисления корня степени $4n$, заметим, что корнем степени $4n$ из точки $O = (0,-1)$ является любая точка кривой.

Алгоритм 6. Вычисления корня степени k из точки кривой, где $1 < k < n$.

Вход: произвольная точка $Z \in E_p$.

Выход: точка $S \in E_p$ такая, что $kS = Z$.

1. Используя алгоритм Евклида вычислить $u, v \in Z$ такие, что $uk + vn = 1$.
2. Вычислить $u = u \bmod n$.
3. $S = uZ$.
4. Выход S.

ВЫВОДЫ

Наиболее существенными математическими результатами этой работы можно считать:

- критерий делимости точки на 4;
- критерий делимости точки на n и на произвольное число k, взаимно простое с n, где n – простое число, равное порядку циклической подгруппы группы точек кривой Едвардса.

Практическими результатами, которые основываются на перечисленных выше математических результатах, являются алгоритмы получения корня произвольной степени из точки кривой, а основным практическим результатом – новые алгоритмы генерации базовой точки кривой Эдвардса. Также приведен сравнительный анализ новых и классических алгоритмов генерации базовой точки.

- Алгоритмы 3 и 4 имеют одинаковую сложность в смысле «О-большое» (то есть учитывая лишь степень полинома, без коэффициента) и значительно быстрее алгоритма 2.
- Если использовать более точные оценки, то в порядке снижения быстродействия алгоритмы располагаются следующим образом:
    - Алгоритм 3
    - Алгоритм 4
    - Алгоритм 2
- Преимущества алгоритма 4:
    - Не используется арифметика на кривой, лишь операции в поле.
    - Этот алгоритм появился недавно, поэтому, возможно, в дальнейших исследованиях его можно оптимизировать.

СПИСОК ЛИТЕРАТУРЫ

1. Edwards H.M. A normal form for elliptic curves. / H.M. Edwards // Bulletin of the AMS 44(3) – 2007 – С. 393–422.
2. Bernstein D.J. Faster addition and doubling on elliptic curves. / D.J. Bernstein, T. Lange // ASIACRYPT 2007. Volume 4833 of LNCS., Springer – 2007 – С. 29–50.
3. Bernstein D.J. Twisted Edwards curves. / D.J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters // AFRICACRYPT 2008. Volume 5023 of LNCS., Springer – 2008 – С. 389–405.
4. Huseyin Hisil Twisted Edwards Curves Revisited / Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, Dawson Ed. // ASIACRYPT. – 5350. – New York: Springer, 2008. – С. 326-343.
5. Бессалов А.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. / А.В. Бессалов, Л.В. Ковальчук // Кибернетика и системный анализ, том 51 №2 – 2015 – С. 3-12.
6. Ковальчук Л.В. Рекурентні алгоритми обчислення кореню довільного степеню у кільці лишків. / Л.В. Ковальчук, О.Ю. Беспалов, П.В. Огнєв // Правове, нормативне та метрологічне забезпечення захисту інформації в Україні, випуск 25 – 2013 – С. 58-66.

7. Бессалов А.В. Новые свойства кривой Эдвардса над простым полем / А.В. Бессалов, О.В. Цыганкова. Радиотехника №180, 2015. – С.137-143.
8. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер // «Мир», Том 1 – 1988 – 273 стр.