ВЫЧИСЛЕНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ $EC(GF(3^n))$

1. Группа точек эллиптической кривой $EC(GF(3^n))$

На множестве $\mathcal{EF}$, состоящем из точек эллиптической кривой

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6,\ a_i \in GF(3^n)$$

и еще одного элемента — бесконечно удаленной точки $\mathcal{O}$ (формально не являющейся точкой кривой), можно определить операцию, обладающую свойствами операции абелевой группы. Принято получающуюся при этом группу рассматривать как аддитивную группу, а операцию называть операцией сложения и обозначать, как обычно, знаком $+$. Точка $\mathcal{O}$ выполняет роль нейтрального элемента (в аддитивной записи — нуля).

Полагаем, что $\mathcal{O} + \mathcal{O} = \mathcal{O}$ и для любой точки $(x, y) \in \mathcal{EF}$ выполняются равенства

$$(x, y) + \mathcal{O} = \mathcal{O} + (x, y) = (x, y).$$

Чтобы определить в общем случае операцию сложения абелевой группы, сначала покажем, что каждой точке (x, y) эллиптической кривой можно сопоставить в определенном смысле симметричную точку (далее будет пояснено, что такая точка и будет точкой $-(x, y)$, противоположной относительно точки (x, y) точкой в группе данной кривой). Заметим, что вместе с точкой (x, y) кривая имеет и точку

$$(x, \tilde{y}) = (x, -y). \tag{1}$$

В этом нетрудно убедиться непосредственным вычислением значений левой и правой частей уравнения кривой при $X = x$, $Y = -y$ и, учитывая, что при $X = x$ и $Y = y$ эти значения совпадают. Симметричность проявляется в том, что, как нетрудно проверить, по тому же правилу точке $(x, \tilde{y})$ соответствует исходная точка: $(x, \tilde{\tilde{y}}) = (x, -\tilde{y}) == (x, y)$, так что имеет место *инволютивный закон*: $(x, y) = (x, \tilde{\tilde{y}})$.

Будем считать, что $(x, y) + (x, \tilde{y}) = \mathcal{O}$, и обозначать $(x, \tilde{y}) = -(x, y)$. Как видим, множество $\mathcal{E}(\mathcal{F})$ удовлетворяет двум аксиомам группы (существует нулевой элемент и каждому элементу соответствует противоположный элемент).

Операция сложения определена для случаев, когда хотя бы одно слагаемое является точкой $\mathcal{O}$ или слагаемые (x_1, y_1), (x_2, y_2) таковы, что $x_1 = x_2$ и $y_2 = \tilde{y}_1$ или, что то же самое, $y_1 = \tilde{y}_2$.

Осталось определить сумму $(x_1, y_1) + (x_2, y_2)$ для остальных случаев, когда

$$x_1 \neq x_2 \tag{2}$$

или

$$x_1 = x_2 \text{ и } y_2 \neq \tilde{y}_1 \text{ (или, что то же, } y_1 \neq \tilde{y}_2). \tag{3}$$

Упражнение 1.1. Покажите, что в условиях (3) $y_2 = y_1$.

Пусть $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ две точки эллиптической кривой, удовлетворяющие условию (2), и ни одна из них не есть $\mathcal{O}$. Обозначим $\lambda(x_1, x_2, y_1, y_2) \neq 0$ элемент поля F, такой, что прямая на плоскости F^2

$$\mathcal{L} = \{(x, y)/y - y_1 = \lambda(P, Q)(x - x_1)\} \tag{4}$$

содержит эти две точки эллиптической кривой $\mathcal{EF}$.

Такой элемент легко вычислить:

$$\lambda(P, Q) = \lambda(x_1, x_2, y_1, y_2) = \frac{y_2 - y_1}{x_2 - x_1}. \tag{5}$$

Если же $P = Q = (x', y')$ (то есть имеет место условие (3)), то вместо прямой (4) будем использовать прямую

$$\mathcal{L}' = \{(x, y)/y - y' = \lambda'(P)(x - x')\}, \tag{6}$$

где

$$\lambda'(P) = -\left.\frac{\partial F(X, Y)/\partial X}{\partial F(X, Y)/\partial Y}\right|_{X=x', Y=y'} =$$
$$= -\left.\frac{(a_1 Y - 3X^2 - 2a_2 X - a_4)}{2Y + a_1 X + a_3}\right|_{X=x', Y=y'}. \tag{7}$$

Упражнение 1.2. Проверьте, что прямая (6) содержит точку $P = Q$, а знаменатель в выражении (7) не может быть нулевым.

Покажем, что кроме точек P и Q множество (4), как и множество (6), содержит еще одну точку R эллиптической кривой. В случае прямой (4) эта дополнительная точка может совпасть с точками P или Q, то есть одна из этих точек может быть кратным корнем уравнения (4). Такая точка называется *точкой инфлекции.*

Уравнения прямых (4) и (6) равносильны, соответственно, уравнениям $Y = \lambda X + \beta$, где $\lambda = \lambda(P, Q)$, $\beta = y_1 - \lambda x_1$ и $Y = \lambda' x + \beta'$, где $\lambda' = \lambda'(P)$, $\beta' = y_1 - \lambda' x_1$.

Точка $(x, \lambda x + \beta) \in \mathcal{L}$ (или точка $(x, \lambda' x + \beta') \in \mathcal{L}'$) лежит на эллиптической кривой только в том случае, когда

$$(\lambda x + \beta)^2 + a_1 x(\lambda x + \beta) + a_3(\lambda x + \beta) = x^3 + a_2 x^2 + a_4 x + a_6$$

(или, соответственно,

$$(\lambda' x + \beta')^2 + a_1 x(\lambda' x + \beta') + a_3(\lambda' x + \beta') = x^3 + a_2 x^2 + a_4 x + a_6)).$$

Отсюда следует, что кубическое уравнение

$$(\lambda X + \beta)^2 + a_1 X(\lambda X + \beta) + a_3(\lambda X + \beta) = X^3 + a_2 X^2 + a_4 X + a_6$$

(или, соответственно,

$$(\lambda' X + \beta')^2 + a_1 X(\lambda' X + \beta') + a_3(\lambda' X + \beta') = X^3 + a_2 X^2 + a_4 X + a_6)$$

имеет (с учетом кратности) три корня, среди них x_1 и x_2 (или дважды x), так как $(x_1, \lambda x_1 + \beta)$ и $(x_2, \lambda x_2 + \beta)$ (или $(x, \lambda' x + \beta')$) являются точками P и Q (точкой P) кривой.

Воспользовавшись теоремой Виета, согласно которой сумма корней нормированного многочлена равна взятому со знаком минус коэффициенту γ (или γ') при степени, предшествующей старшей степени, можем определить и третий корень $x_3 = \gamma - x_1 - x_2$ (или $x_3 = \gamma' - 2x$) кубического уравнения, а затем вторую координату $y_3 = y_1 + \lambda(x_3 - x_1)$ (или $y_3 = y + \lambda'(x_3 - x_1)$ третьей точки эллиптической кривой, принадлежащей прямой (4) (или (6)).

Это позволяет получить выражение для x_3 и, следовательно, для обеих координат третьей точки

$$R = (x_3, y_3) = (\gamma - x_1 - x_2,\ y_1 + \lambda(x_3 - x_1)) \tag{8}$$

эллиптической кривой на прямой (5) через координаты x_1, x_2, y_1, y_2.

Аналогично определяются координаты точки

$$R = (x_3, y_3) = (\gamma' - 2x,\ y + \lambda'(x_3 - x)) \tag{9}$$

на прямой (6).

Определение 1.1. При условиях (2) или (3) суммой двух (в случае (3) – совпадающих) точек эллиптической кривой объявляется точка

$$P + Q = -R = -(x_3, y_3) \tag{10}$$

или

$$P + P = 2P = -R = -(x_3, y_3), \tag{11}$$

где $R = (x_3, y_3)$ – третья точка (8) или (9), принадлежащая множеству (4) или (6) соответственно.

Заметим, что соблазнительно назвать суммой точек P, Q саму точку R. Но в этом случае определяемая операция не будет удовлетворять очевидному свойству $P + Q = R \rightarrow\ P = R - Q$ операции сложения.

Общая схема алгоритма сложения или удвоения для группы точек эллиптической кривой, а также конкретные формулы для вычисления координат третьей точки, когда ни одно из слагаемых не есть точка $\mathcal{O}$ и когда эти слагаемые не являются взаимно противоположными, рассматриваются в разд. 4.

Если кривая определена над полем $\mathcal{R}$ действительных чисел, множество $\mathcal{L}$ есть в самом деле прямая, проходящая через точки P и Q кривой и пересекающая ее в третьей точке R. Суммой является точка $-R$, противоположная точке R.

Эта точка R может оказаться точкой инфлекции и совпасть с одной из точек P или Q.

Прямая $\mathcal{L}'$ является касательной к кривой в точке $P = Q$. Тогда R – точка пересечения касательной с кривой, $2P$ – точка, противоположная к R точка $-R$.

Пример 1.1. На кривой $Y^2 = X^3 - 36X$ возьмем точки $P = (-3, 9)$, $Q = (-2, 8)$. Тогда при вычислении (используя формулы для кривых характеристики, не равной двум или трем, из подразд. 2.1) $P + Q$ находим $x_3 = 6,\ y_3 = 0$, а при вычислении $2P$ определяем $x_3 = 25/4, y_3 = -35/8$.

Упражнение 1.3. Докажите, что если $P = (x, 0)$, то $2P = 0$, $3P == P$, $4P = 0$ и т. д.

Заметим, что описанная операция коммутативна также в случаях (3) и (4), поскольку $\lambda(x_1, x_2, y_1, y_2) = \lambda(y_1, y_2, x_1, x_2)$ и $\lambda'(x, y) == \lambda'(y, x)$.

2 Алгоритмы сложения и удвоения точек

В соответствии с определением операции сложения в группе точек эллиптической кривой общая схема алгоритма сложения точек $P_1 = = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ представляется в виде алгоритма 2.1 на рис. 1.

Алгоритм 2.1

```
Вход: Коэффициенты эллиптической кривой,
точки P1 = (x1, y1) (или P1 = O) и P2 = (x2, y2) (или P2 = O).
Выход: P = P1 + P2.
Вычислить : если P1 = O, то P = P2,
            если P2 = O, то P = P1,
            если P2 = −P1, то P = O,
            если x1 ≠ x2, то P = −(x3, y3),
            иначе P = 2P1 = −(x3, y3).
Вернуть P.
```

Рис. 1. Общая схема алгоритма сложения и удвоения точек эллиптической кривой

Координаты точек $-(x_3, y_3)$ вычисляются по формулам в зависимости от вида эллиптической кривой.

Координаты точек $-(x_3, y_3)$ вычисляются по формулам, вытекающим из определения (1.1) (в зависимости от вида эллиптической кривой).

Для эллиптических кривых над полем $\mathcal{F}$ характеристики больше трех это формулы

– при $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$

$$P_1 + P_2 = -R = (x_3, -y_3) = (x_3, -y_1 + \lambda(x_1 - x_3)), \tag{12}$$

где

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_3 = \lambda^2 - x_1 - x_2;$$

– при $P_1 = P_2 = P = (x, y)$

$$2P = -R = (x_3, -y_3) = (x_3, -y + \lambda'(x - x_3)), \tag{13}$$

где

$$\lambda' = \frac{3x^2 + a}{2y},\ x_3 = (\lambda')^2 - 2x$$

(a – соответствующий коэффициент в (**??**)).

Для эллиптических кривых над полем характеристики три используются формулы

– при $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$

$$P_1 + P_2 = -R = (x_3, -y_3) = (x_3,\ -y_1 + \lambda(x_1 - x_3)), \tag{14}$$

где

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_3 = (\lambda^2 - a_2) - x_1 - x_2$$

(a_2 – коэффициент из формулы (**??**));

– при $P_1 = P_2 = P = (x, y)$

$$2P = -R = (x_3, -y_3) = (x_3, -y + \lambda'(x - x_3)). \tag{15}$$

.

3 . Скалярное умножение на эллиптических кривых

Алгоритмы умножения точки P эллиптической кривой на числовую константу k (алгоритмы вычисления $k \cdot P$), называются также алгоритмами скалярного умножения точки и являются основными в арифметике эллиптических кривых. С эффективными алгоритмами умножения на эллиптических кривых можно ознакомиться по соответствующим разделам учебного пособия [1] и монографии [2].

Рассмотрим умножение методом аддитивных цепочек.

Чтобы вычислить точку $k \cdot P$, разложим k в системе счисления по основанию 2^m, используя отрицательные цифры, и получим:

$$k = \sum_{i=0}^{\lfloor n/m \rfloor} a_i 2^{mi}.$$

Вычислим и запомним все кратные $a_i P$ (достаточно вычислить все нечетные кратные $P,\ 3P,\ \ldots,\ (2^{m-1} - 1)P$ с помощью поочередных удвоений и прибавлений P или даже только $P,\ 3P,\ \ldots,\ (2^{m-2} - -1)P$, если использовать разложение с отрицательными цифрами $\pm 1, \pm 3, \ldots, \pm(2^{m-2}-1)$). Затем вычислим kP по схеме Горнера:

$$kP = (\ldots(a_{s-1}2^m + a_{s-2})2^m + \ldots + a_1)2^m) + a_0)P =$$

$$= (\ldots(a'_{s-1}2^{m+l_{s-1}} + a'_{s-2})2^{m+l_{s-2}} + \ldots + a'_1)2^{m+l_1}) + a'_0 2^{l_0})P,$$

используя $s = \lfloor n/m \rfloor$ сложений-вычитаний с уже вычисленными точками и столько же умножений на 2^{m+l} при подходящем l.

4 . Особенности эллиптических кривых одного вида

Идея использовать поля характеристики три была предложена в работе

Barreto P.S.L.M., Kim H.Y., Lynn B., Scott M. Efficient algorithms for pairing-based cryptosystems, Crypto 2002, LNCS 2442(2002),pp,зз.354-368.

Конкретно, в этой работе рассматривались кривые

$$E_{3,b} : Y^2 = X^3 - X + b,\ b \in \{-1, 1\}$$

над полем $GF(3^m)$ при нечетном m. В частности, предлагалось использовать $m = 97$.

Правило сложения точек для этих кривых можно представить в следующем виде.

Если $P_i = (x_i, y_i)$, $P_1 \neq -P_2$, $P_3 = P_1 + P_2 = (x_3, y_3)$,
то $\lambda = 1/y_1$ при $x_1 = x_2$, и $\lambda = (y_2 - y_1)/(x_2 - x_1)$ при $x_1 \neq x_2$,
и $x_3 = \lambda^2 - (x_1 + x_2)$, $y_3 = y_1 + y_2 - \lambda^3$.

Упражнение 4.1. Докажите правило сложения для кривых $E_{3,b}$.
Указание. Учесть, что $2 \equiv -1 (\mathrm{mod}\ 3)$.

В той же работе сделано интересное наблюдение, что *утроение* точки на кривых $E_{3,b}$, $b \in \{1, 2\}$ можно выполнить столь же быстро, как и удвоение точки на суперсингулярных кривых над полями четной характеристики. А именно, если $P = (x, y)$, и $3P = (X, Y)$, то $X = (x^3)^3 - b$, $Y = -(y^3)^3$.

Упражнение 4.2. Докажите описанное правило утроения точки кривой $E_{3,b}$.

Это правило позволяет утраивать точки кривой $E_{3,b}$ над полем $GF(3^m)$ со сложностью $O(m)$, так как возведение в куб при использовании стандартного базиса с неприводимым малочленом над полем $GF(3)$ выполняется, очевидно, со сложностью $O(m)$, поскольку возведение в куб троичного многочлена согласно тождеству Фробениуса можно выполнить со сложностью $O(m)$, а приведение по модулю малочлена выполнятся со сложностью $O(m)$ аналогично случаю характеристики два. В нормальных же базисах возведение в куб и вовсе «бесплатно». Правда, умножение в них не так легко, но для него тоже можно применить оптимальные нормальные базисы, подобно случаю характеристики два.

Благодаря отмеченной особенности операции утроения точки, для ускорения скалярного умножения точек на кривой $E_{3,b}$ лучше использовать не бинарный, а тернарный метод, использующий разложение скалярного множителя n в троичной системе, причем удобно применять, как и в двоичном случае, уравновешенную троичную систему, в которой используются в качестве цифр нули и плюс-минус единицы.

Другой подход к ускорению скалярного умножения для этой кривой был указан в работе

Koblitz N. An elliptic curve implementation of the finite field digital signature algorithm, LNCS 1462 (1998),327-33.

Он основан на использовании проективных координат со следующим правилом сложения точек в смешанных координатах (данным в первой из указанных выше работ: если $P_1 = (X_1, Y_1, Z_1)$, $P_2 = (X_2, Y_2, 1)$, то $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$ можно вычислить следующим образом за девять умножений:

$$A = X_2Z_1 - X_1,\ B = Y_2Z_1 - Y_1,\ C = A^3,\ D = C - Z_1B^2,$$

$$X_3 = X_1C - AD,\ Y_3 = BD - Y_1C,\ Z_3 = Z_1C.$$

Упражнение 4.3. Докажите это правило.

Указание. Оно содержит девять умножений потому, что возведение в куб делается со сложностью почти такой же, как и сложение в этом поле.

Как и двоичном случае, переход к обычным координатам выполняется в конце вычислений по формуле $P = (X/Z, Y/Z)$, поэтому указанный метод требует только две операции деления в самом конце вычислений. Заметим, что утроение точки $P = (x, y, z)$ в смешанных координатах можно выполнить по формуле

$$Z = (Z^3)^3, X = (X^3)^3 - bZ, Y = -(Y^3)^3.$$

Действительно, переходя к обычным координатам, имеем известные формулы утроения

$$x_3 = X/Z = ((x/z)^3)^3 - b, y - 3 = Y/Z = -((y/z)^3)^3.$$

Поэтому использование проективных координат можно совместить с использованием уравновешенной троичной системы.

5 Контрольные вопросы

1. Запишите уравнение эллиптической кривой над полем $GF(3^n)$.

2. Какова характеристика поля $GF(3^n)$?

2. какая точка противоположна точке (x, y) эллиптической кривой $EG(GF(3^n))$?

3. Что является единицей группы точек эллиптической кривой?

4. Покажите,то применительно к эллиптическим кривым над полем характеристики три формула (7) эквивалентна формуле

$$\lambda'(P) = - \left. \frac{\partial F(X,Y)/\partial X}{\partial F(X,Y)/\partial Y} \right|_{X=x', Y=y'} = \\ = - \left. \frac{(a_1 Y + a_2 X - a_4)}{2Y + a_1 X + a_3} \right|_{X=x', Y=y'} . \tag{16}$$

4. Как определяется сумма взаимно противоположных точек эллиптической кривой?

5. Как определяется сумма $(x, y) + \mathcal{O}$ точек эллиптической кривой над полем $GF(3^n)$?.

6. Запишите формулу удвоения точки эллиптической кривой над полем $GF(3^n)$?. и дайте ее интерпретацию.

7. Запишите формулу для вычисления суммы двух различных, но не взаимно противоположных точек эллиптической кривой, ни одна из которых не является единицей группы точек эллиптической кривой над полем $GF(3^n)$?.

8. Дайте аддитивную интерпретацию алгоритма возведения в степень (см. раздел Вычисления в числовых кольцах и полях) применительно к операции скалярного умножения точки эллиптической кривой над полем $GF(3^n)$?.

9. Выполните упражнения 4.1,4.2 и 4.3.

Литература.

1. Болотов А.А., Гашков С.Б. , Фролов А.Б. Криптографические протоколы на эллиптических кривых: учебное пособие/ – М. : Издательский дом МЭИ, 2007. – 84 с.

2.Болотов А.А., Гашков С.Б. , Фролов А.Б., Часовских А.А. Криптографические протоколы на эллиптических кривых. – М.: Кокнига, 2006