КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 7

Математические основы криптографии: построение и исследование эллиптических кривых

Данный материал демонстрирует разбор задания, посвященного построению и исследованию группы точек эллиптической кривой над конечным полем.

Эллиптической кривой над конечным полем вычетов по модулю простого числа $p > 3$ называется множество точек $(x, y) \in F_p \times F_p$, удовлетворяющих уравнению $y^2 = x^3 + ax + b$, где $a,\ b \in F_p$ и $-4a^3 - 27b^2 \neq 0 \pmod p$, дополненное бесконечно удаленной точкой 0, не имеющей численного выражения. Данное множество точек, обозначаемое $E_{a,b}(F_p)$, представляет собой абелеву группу относительно операции сложения точек.

Операция сложения точек эллиптической кривой задается следующим образом. Чтобы сложить точки P и Q, необходимо провести через них прямую, которая в общем случае будет проходить еще через одну точку эллиптической кривой. Эту третью точку необходимо симметрично отразить относительно оси абсцисс, полученный результат и будет представлять собой сумму $P + Q$.

Зная координаты двух исходных точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, достаточно легко вывести формулы для нахождения координат третьей точки $C = (x_3, y_3) = P + Q$. При этом необходимо учесть три случая.

Первый случай. Складываются две одинаковые точки $P = (x_1, y_1)$ и $P = (x_1, y_1)$. При выводе координат результирующей точки необходимо воспользоваться уравнением касательной к эллиптической кривой. Формулы для нахождения координат точки $C = (x_3, y_3) = P + P$ имеют вид

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases} \quad (1)$$

Второй случай. Складываются две разные точки, $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, причем $x_1 \neq x_2$. При выводе координат результирующей точки необходимо воспользоваться уравнением секущей к эллиптической кривой. Формулы для нахождения координат точки $C = (x_3, y_3) = P + Q$ имеют вид

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \end{cases} \quad (2)$$

Третий случай. Складываются две разные точки, $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, причем $x_1 = x_2,\ y_1 = y_2$. Такие точки являются взаимно обратными элементами группы $E_{a,b}(F_p)$,

то есть $Q = -P$, поэтому их сумма дает нейтральный элемент группы, то есть бесконечно удаленную точку 0.

Выполнение задания включает построение и исследование группы точек эллиптической кривой $E_{a,b}(F_p)$.

В простейшем случае, чтобы построить всю группу точек эллиптической кривой, можно использовать полный перебор, подставляя все возможные значения элементов из F_p в качестве x в уравнение эллиптической кривой и определяя, можно ли извлечь квадрат из полученного значения. При положительном исходе в группу $E_{a,b}(F_p)$ необходимо добавить две точки вида $\left(x; \pm\sqrt{y^2} \pmod p\right)$ или одну точку, если $y^2 \pmod p = 0$. Кроме того, в группу $E_{a,b}(F_p)$ необходимо включить бесконечно удаленную точку 0.

Чтобы исследовать построенную группу $E_{a,b}(F_p)$, необходимо выполнить следующее:

- найти порядок всех элементов группы $E_{a,b}(F_p)$;

- установить, является ли группа $E_{a,b}(F_p)$ циклической, и при положительном исходе найти все ее образующие элементы;

- найти все циклические подгруппы группы $E_{a,b}(F_p)$;

- составить диаграмму, описывающую внутреннее устройство группы $E_{a,b}(F_p)$.

При выполнении данного задания необходимо опираться на свойства абстрактных циклических групп и навыки, приобретенные при исследовании подобных групп.

Пример.

Построить и исследовать группу точек эллиптической кривой $E_{-2,1}(F_7)$.

Решение.

Сначала проверим, что данные в примере параметры эллиптической кривой действительно удовлетворяют условию гладкости. Из задания следует, что $a = -2$, $b = 1$. Подставим данные значения в выражение для нахождения дискриминанта кубического многочлена $x^3 - 2x + 1$:

$-4a^3 - 27b^2 = -4 \cdot (-2)^3 - 27 \cdot 1^2 = 5 \neq 0 \pmod 7$.

Полученное значение отлично от нуля, значит уравнение $y^2 = x^3 - 2x + 1$, заданное над полем F_7, действительно является уравнением эллиптической кривой.

Теперь запишем простое конечное поле F_7, служащее основой для построения данной эллиптической кривой, с использованием положительных и отрицательных вычетов, каждый раз выбирая наименьшее по абсолютной величине значение:

$F_7 = \{0, 1, 2, 3, 4, 5, 6\} = \{-3, -2, -1, 0, 1, 2, 3\} = \{0, \pm1, \pm2, \pm3\}$.

Такой вид поля позволит упростить последующие расчеты.

Чтобы построить всю группу точек эллиптической кривой, используем полный перебор, подставляя все возможные значения $x \in F_7$ в уравнение эллиптической кривой и определяя, можно ли извлечь квадратный корень из полученного значения.

Поскольку возможность извлечения квадратного корня из данного значения по модулю не всегда очевидна, можно предварительно возвести все элементы поля F_7. это даст список значений, из которых может быть извлечен квадратный корень, вместе со значениями самих корней.

$0^2 = 0$,

$(\pm1)^2 = 1$,

$(\pm2)^2 = 4$,

$(\pm 3)^2 = 9 = 2 \pmod 7$.

Таким образом, в поле F_7 квадратный корень может быть извлечен из следующих значений: 0, 1, 2, 4. Следовательно, из всех прочих значений квадратный корень извлечь нельзя: 3, 5, 7.

Теперь последовательно подставим значения $x \in F_7$ в уравнение эллиптической кривой.

Возьмем $x = -3$. Получим $y^2 = (-3)^3 - 2(-3) + 1 = -20 = 1 \pmod 7$. Уравнение $y^2 = 1$ является разрешимым. Из 1 может быть извлечен квадратный корень, равный ± 1. Следовательно, группе точек эллиптической кривой $E_{-2,1}(F_7)$ принадлежат следующие две точки: $(-3, -1)$ и $(-3, 1)$.

Возьмем $x = -2$. Получим $y^2 = (-2)^3 - 2(-2) + 1 = 4 = \pmod 7$. Следовательно, $(-2, -2), (-2, 2) \in E_{-2,1}(F_7)$.

Возьмем $x = -1$. Получим $y^2 = (-1)^3 - 2(-1) + 1 = 2 = \pmod 7$. Следовательно, $(-1, -3), (-1, 3) \in E_{-2,1}(F_7)$.

Возьмем $x = 0$. Получим $y^2 = (0)^3 - 2(0) + 1 = 1 \pmod 7$. Следовательно, $(0, -1), (0, 1) \in E_{-2,1}(F_7)$.

Возьмем $x = 1$. Получим $y^2 = 1^3 - 2 \cdot 1 + 1 = 0 \pmod 7$. Следовательно, $(1, 0) \in E_{-2,1}(F_7)$.

Возьмем $x = 2$. Получим $y^2 = 2^3 - 2 \cdot 2 + 1 = 5 \pmod 7$. Из 5 нельзя извлечь квадратный корень по модулю 7.

Возьмем $x = 3$. Получим $y^2 = 3^3 - 2 \cdot 3 + 1 = 1 \pmod 7$. Следовательно, $(3, -1), (3, 1) \in E_{-2,1}(F_7)$.

Таким образом, уравнению эллиптической кривой $y^2 = x^3 - 2x + 1$ над полем F_7 соответствуют 11 точек. Кроме того, данной эллиптической кривой принадлежит удаленная точка 0, не имеющая численного выражения.

Запишем полученную группу точек.

$$E_{-2,1}(F_7) = \{0, (-3, -1), (-3, 1), (-2, -2), (-2, 2), (-1, -3), (-1, 3), (0, -1), (0, 1), (1, 0), (3, -1), (3, 1)\}.$$

Теперь необходимо определить, является ли данная группа циклической. Для этого нужно найти порядок всех элементов группы $E_{-2,1}(F_7)$ и установить, есть ли среди них элементы, порядок которых равен 12. Если данная группа является циклической, то таких элементов должно быть ровно четыре по количеству чисел, меньших числа 12 и взаимно простых с ним.

Возьмем точку $P = (-3, -1)$ и определим ее порядок. Для этого будем последовательно получать целочисленные кратные данной точки вида $2P = P + P$, $3P = 2P + P$, ..., до тех пор, пока не получим точку 0.

Начнем с точки $2P$. Чтобы ее найти, нужно воспользоваться группой формул (1). Вычислим $x_3 = \left(\frac{3 \cdot (-3)^2 - 2}{2 \cdot (-1)}\right)^2 - 2 \cdot (-3) = 3$, затем $y_3 = \left(\frac{3 \cdot (-3)^2 - 2}{2 \cdot (-1)}\right)(-3 - 3) - (-1) = -1$. Следовательно, $2P = (3, -1)$.

Чтобы найти точку $3P = 2P + P = (3, -1) + (-3, -1)$, нужно воспользоваться группой формул (2). Вычислим $x_3 = \left(\frac{-1-(-1)}{-3-3}\right)^2 - 3 - (-3) = 0$, затем $y_3 = \left(\frac{-1-(-1)}{-3-3}\right)(3 - 0) - (-1) = 1$. Следовательно, $3P = (0, 1)$.

Точку $4P$ можно найти двумя способами. Либо представить ее как $4P = 2P + 2P$ и воспользоваться группой формул (1), либо представить ее как $4P = 3P + P$ и воспользоваться группой формул (2). Аналогичным образом можно работать с последующими точками, представляя различными суммами уже вычисленных точек.

Опустим дальнейшие вычисления и приведем значения последующих целочисленных кратных точки $P = (-3, -1)$.

$4P = (-2, -2)$.

$5P = (-1, 3)$.

$6P = (1, 0)$.

$7P = (-1, -3)$.

$8P = (-2, -2)$.

$9P = (0, -1)$.

$10P = (3, 1)$.

$11P = (-3,1)$.

$12P = 0$.

Таким образом, точка $P = (-3, -1)$ имеет порядок, равный 12, порождает все точки группы $E_{-2,1}(F_7)$ и, соответственно, является образующим данной группы.

Определим порядок всех прочих точек группы $E_{-2,1}(F_7)$, основываясь на проделанных расчетах.

$O\big(P = (-3, -1)\big) = 12$,

$O\big(2P = (3, -1)\big) = 6$,

$O\big(3P = (0, 1)\big) = 4$,

$O\big(4P = (-2, -2)\big) = 3$,

$O\big(5P = (-1, 3)\big) = 12$,

$O\big(6P = (1, 0)\big) = 2$,

$O\big(7P = (-1, -3)\big) = 12$,

$O\big(8P = (-2, -2)\big) = 3$,

$O\big(9P = (0, -1)\big) = 4$,

$O\big(10P = (3, 1)\big) = 6$,

$O\big(11P = (-3,1)\big) = 12$.

Теперь можем выделить все циклические подгруппы группы $E_{-2,1}(F_7)$ и описать ее внутреннее устройство.

$E_{-2,1}(F_7) = \langle P = (-3, -1)\rangle = \langle 5P = (-1, 3)\rangle = \langle 7P = (-1, -3)\rangle = \langle 11P = (-3,1)\rangle$.

$H_1 = \langle 2P = (3, -1)\rangle = \langle 10P = (3, 1)\rangle = \{0, 2P, 4P, 6P, 8P, 10P\}$, $H_1 \leq E_{-2,1}(F_7)$.

$H_2 = \langle 3P = (0, 1)\rangle = \langle 9P = (0, -1)\rangle = \{0, 3P, 6P, 9P\}$, $H_2 \leq E_{-2,1}(F_7)$.

$H_3 = \langle 4P = (-2, -2)\rangle = \langle 8P = (-2, -2)\rangle = \{0, 4P, 8P\}$, $H_3 \leq H_1 \leq E_{-2,1}(F_7)$.

$H_4 = \langle 6P = (1, 0)\rangle = \{0, 2P\}$, $H_4 \leq H_3 \leq H_1 \leq E_{-2,1}(F_7)$.