Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Эллиптические кривые

Эллиптическая криптография

- **Эллиптические кривые** над конечными полями представляют собой пример **конечных структур**, широко используемых для построения криптографических алгоритмов.
- **Эллиптическая криптография** — раздел современной криптографии, который изучает криптографические методы и алгоритмы, построенные на основе математического аппарата эллиптических кривых.

Понятие эллиптической кривой

- Пусть F – произвольное поле. Эллиптической кривой E над полем F называется гладкая кривая, задаваемая уравнением вида

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in F$$

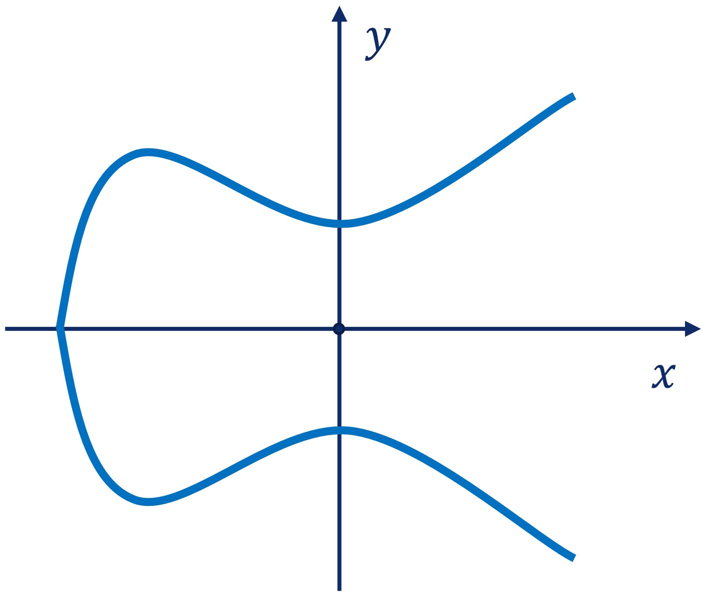
- Множество точек эллиптической кривой $E(F)$ включает все точки, удовлетворяющие данному уравнению, и «бесконечно удаленную» точку 0.
- Если $\mathrm{char}\, F \neq 2$ и $\mathrm{char}\, F \neq 3$, то уравнение эллиптической кривой над полем F имеет вид, называемый нормальной формой Вейерштрасса

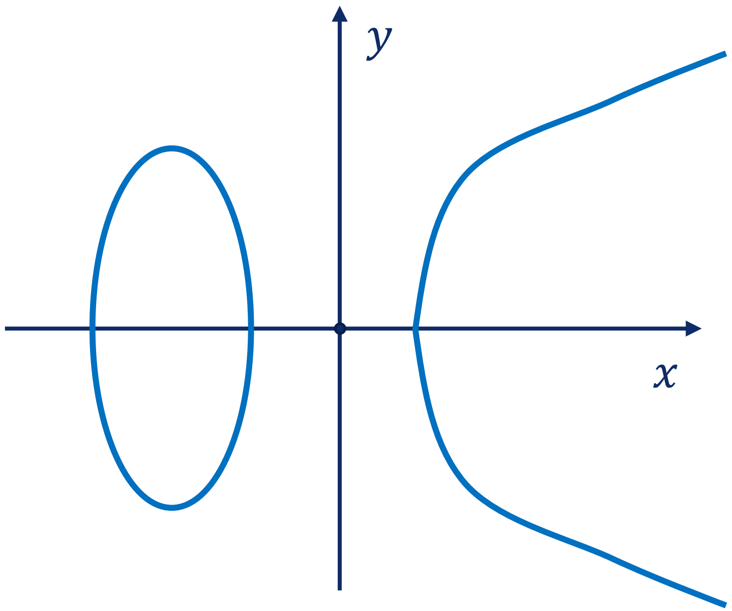
$$y^2 = x^3 + ax + b, a, b \in F$$

- Условие гладкости эллиптической кривой:

$$\Delta = -4a^3 - 27b^2 \neq 0.$$

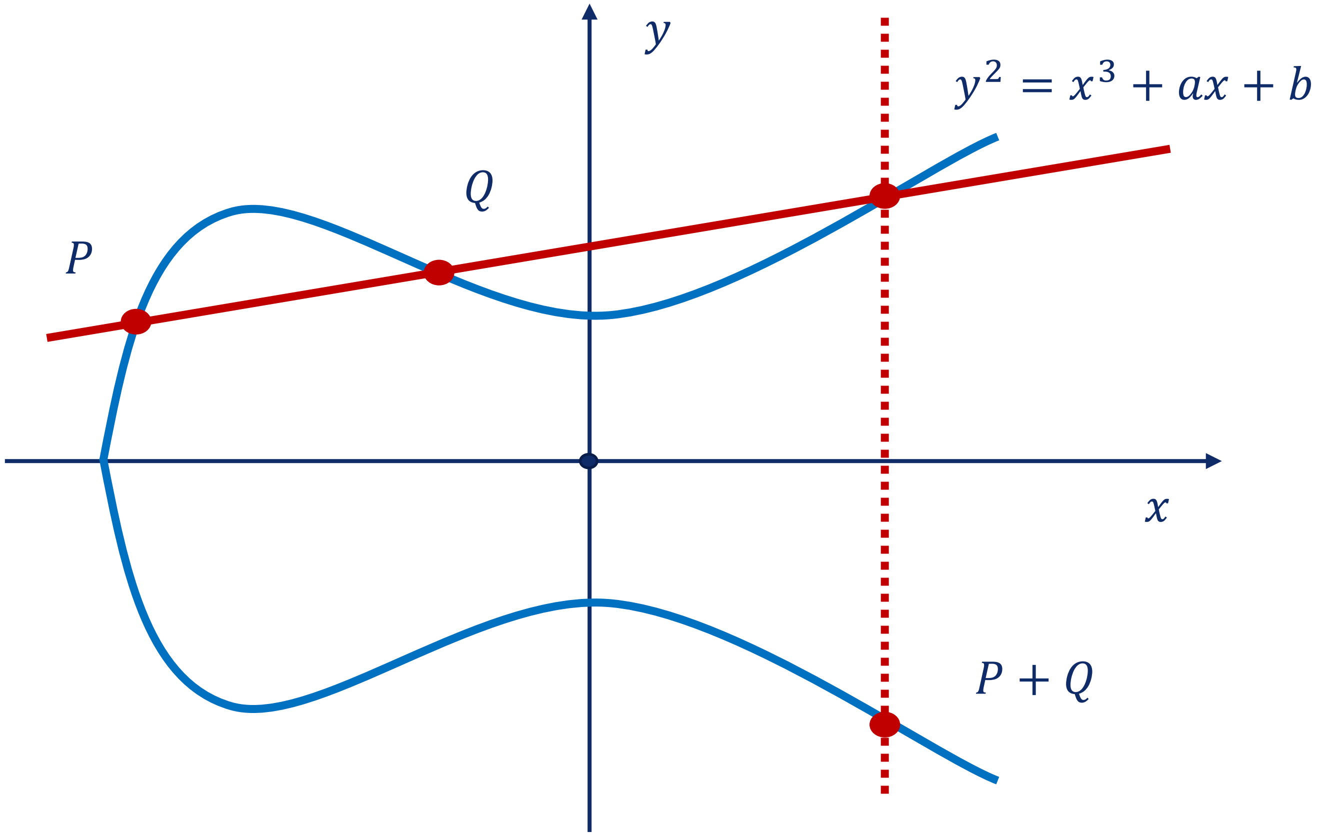
Эллиптические кривые над полем $\mathbb{R}$





Операция сложения точек эллиптической кривой

- Две точки:
  - $P = (x_1, y_1)$,
  - $Q = (x_2, y_2)$.
- Сумма:
  - $P + Q = (x_3, y_3)$.



Операция сложения точек эллиптической кривой

- Рассмотрим случай $P \neq Q$ и $x_1 \neq x_2$ и составим систему уравнений:

$$\begin{cases} y = \alpha x + \beta \\ y^2 = x^3 + ax + b \end{cases}, \Rightarrow (\alpha x + \beta)^2 = x^3 + ax + b, \Rightarrow x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + \left(b - \beta^2\right) = 0$$

- По теореме Виета для кубического уравнения $Ax^3 + Bx^2 + Cx + D = 0$ справедливо:

$$x_1 + x_2 + x_3 = -\frac{B}{A}, \Rightarrow x_3 = -\frac{B}{A} - x_1 - x_2, \Rightarrow x_3 = \alpha^2 - x_1 - x_2$$

- Уравнение секущей, проходящей через точки $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, имеет вид:

$$y = \alpha x + \beta = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x + \left(y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1\right) = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$$

- Чтобы найти значение y_3, нужно подставить значение x_3 в уравнение прямой и поменять знак.

Операция сложения точек эллиптической кривой

- В случае $P = Q = (x_1, y_1)$ необходимо составить уравнение касательной с помощью дифференцирования функции $f(x)$, заданной уравнением $y^2 = x^3 + ax + b$ в неявном виде. Для этого следует продифференцировать обе части данного уравнения и выразить производную y':

$$y^2 = x^3 + ax + b, \Rightarrow 2yy' = 3x^2 + a, \Rightarrow y' = \frac{3x^2 + a}{2y}$$

- Полученное выражение определяет угловой коэффициент уравнения касательной к эллиптической кривой в точке $P = (x_1, y_1)$:

$$\alpha = \frac{3x_1^2 + a}{2y_1}, \Rightarrow \beta = y_1 - \frac{3x_1^2 + a}{2y_1}x_1, \Rightarrow y = \left(\frac{3x_1^2 + a}{2y_1}\right)x + \left(y_1 - \frac{3x_1^2 + a}{2y_1}x_1\right) = \frac{3x_1^2 + a}{2y_1}(x - x_1) + y_1$$

- Чтобы найти значение y_3, нужно подставить значение x_3 в уравнение прямой и поменять знак.

Операция сложения точек эллиптической кривой

- Случай $P \neq Q$ и $x_1 \neq x_2$
  - $$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \end{cases}$$
- Случай $P \neq Q$ и $x_1 = x_2$
  - $P + Q = 0.$
- Случай $P = Q$, $P + Q = 2P$
  - $$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases}$$
- Множество точек эллиптической кривой над полем вместе с бесконечно удаленной точкой ноль образует **абелеву группу** относительно операции сложения.
- **Теорема Хассе.** $\left| |E_{a,b}(F_p)| - (p+1) \right| \leq 2\sqrt{p}.$

Пример построения группы точек эллиптической кривой

- Конечное поле: $F_7 = \{0,1,2,3,4,5,6\} = \{-3,-2,-1,0,1,2,3\} = \{0,\pm1,\pm2,\pm3\}.$
- Уравнение: $y^2 = x^3 + 3x + 1.$
- Условие гладкости: $-4 \cdot 3^3 - 27 \cdot 1^2 = -135 \neq 0 \pmod 7.$

x	-3	-2	-1	0	1	2	3
y^2	0	1	4	1	5	1	2

- $E_{3,1}(F_7) =$

P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
0	$(-3,0)$	$(-2,-1)$	$(-2,1)$	$(-1,-2)$	$(-1,2)$	$(0,-1)$	$(0,1)$	$(2,-1)$	$(2,1)$	$(3,-3)$	$(3,3)$

Пример исследования точек эллиптической кривой

- Точка $P = (2,1)$.
- $2P = P + P = (-2,1)$:

  – $\begin{cases} x_3 = \left(\frac{3\cdot 2^2+3}{2\cdot 1}\right)^2 - 2\cdot 2 = -2, \\ y_3 = \left(\frac{3\cdot 2^2+3}{2\cdot 1}\right)(2-(-2)) - 1 = 1. \end{cases}$

- $3P = P + 2P = (0,-1)$:

  – $\begin{cases} x_3 = \left(\frac{1-1}{-2-2}\right)^2 - 2 - (-2) = 0, \\ y_3 = \left(\frac{1-1}{-2-2}\right)(2-0) - 1 = -1. \end{cases}$

- $4P = 2P + 2P = (-1,2)$.

  – $\begin{cases} x_3 = \left(\frac{3\cdot(-2)^2+3}{2\cdot 1}\right)^2 - 2\cdot(-2) = -1, \\ y_3 = \left(\frac{3\cdot(-2)^2+3}{2\cdot 1}\right)(-2-(-1)) - 1 = 2. \end{cases}$

- $5P = P + 4P = (3,-3)$.

  – $\begin{cases} x_3 = \left(\frac{2-1}{-1-2}\right)^2 - 2 - (-1) = 3, \\ y_3 = \left(\frac{2-1}{-1-2}\right)(2-3) - 1 = -3. \end{cases}$

Пример исследования точек эллиптической кривой

- Полученные значения позволяют сделать следующие выводы:
  - $2P \neq 0, \Rightarrow O(P) > 2;$
  - $3P \neq 0, \Rightarrow O(P) > 3;$
  - $4P \neq 0, \Rightarrow O(P) > 4;$
  - $3P \neq -3P, \Rightarrow 6P \neq 0, \Rightarrow O(P) > 6$
- Отсюда $O(P) = 12$ и $E_{3,1}(F_7) = \langle(2,1)\rangle$.

- Прочие точки можно найти на основании равенства $12P = 0$:
  - $12P = P + 11P, \Rightarrow 11P = -P = (2,-1);$
  - $12P = 2P + 10P, \Rightarrow 10P = -2P = (-2,-1);$
  - $12P = 3P + 9P, \Rightarrow 9P = -3P = (0,1);$
  - $12P = 4P + 8P, \Rightarrow 8P = -4P = (-1,-2);$
  - $12P = 5P + 7P, \Rightarrow 7P = -5P = (3,3);$
  - $12P = 6P + 6P, \Rightarrow 6P = -6P = (-3,0).$

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru