Эллиптические кривые

Лекция 2. Групповой закон

Семён Новосёлов
на основе курса Елены Киршановой

БФУ им. И. Канта

2020

IKBFU

Групповой закон

$$E/K : y^2 = x^3 + Ax + B$$

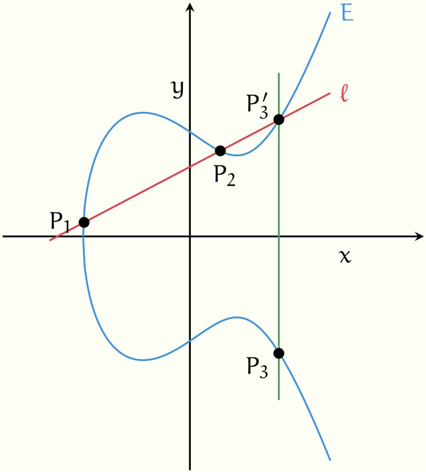
$$P_1 = (x_1, y_1) \in E$$
$$P_2 = (x_2, y_2) \in E$$
$$P_3 = P_1 + P_2 = (x_3, y_3)$$

Случай $x_1 \neq x_2$:

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Сложность

I + 3M в K



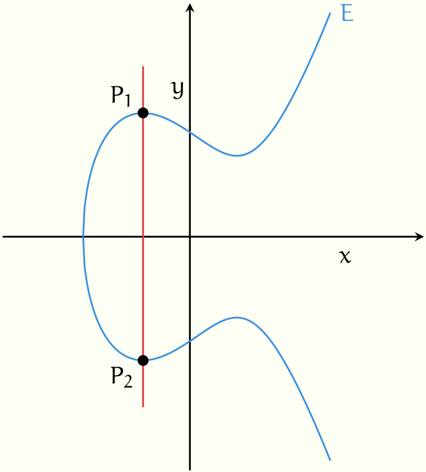
Групповой закон - 2

$$E/K : y^2 = x^3 + Ax + B$$

$$P_1 = (x_1, y_1) \in E$$
$$P_2 = (x_2, y_2) \in E$$
$$P_3 = P_1 + P_2 = (x_3, y_3)$$

Случай $x_1 = x_2$, $y_1 \neq y_2$ или $P_1 = P_2, y_1 = 0$:

$$P_1 + P_2 = \mathcal{O}$$



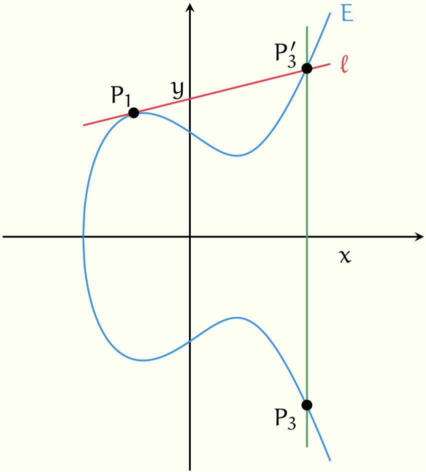
Групповой закон - 3

$$E/K : y^2 = x^3 + Ax + B$$

$$P_1 = (x_1, y_1) \in E$$
$$P_2 = (x_2, y_2) \in E$$
$$P_3 = P_1 + P_2 = (x_3, y_3)$$

Случай $P_1 = P_2$, $y_1 \neq 0$:

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = \frac{3x_1^2 + A}{2y_1}$$



Сложность

I + 4M в K

Групповой закон - 4

Теорема

1. $P_1 + P_2 = P_2 + P_1$ *(коммутативность)*
2. $P + \mathcal{O} = P \ \forall P \in E$ *(∃ нейтральный элемент)*
3. $\forall P \in E \ \exists P' \in E : P + P' = \mathcal{O}$ *(∃ обратный элемент)*
4. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ *(ассоциативность)*

- $-P = (x, -y)$ для кривой в краткой форме

Вывод:

$E(K)$ – аддитивная абелева группа

$E(\mathbb{Q})$ – конечно-порожденная группа

$E(\mathbb{F}_q)$ – конечная группа $\Rightarrow$ криптография на DLOG

Быстрое умножение точки на число

$$P \to [k] \cdot P = \underbrace{P + P + \ldots + P}_{k\text{-раз}}$$

Сложность

$k - 1$ сложений (наивно)

Бинарный метод:

$$k = \sum_{j=0}^{\ell-1} k_j 2^j, \quad k_j \in \{0, 1\}$$

1. $Q \leftarrow \mathcal{O}$
2. **for** $j = \ell - 1$ **to** 0 **by** -1:
   $Q \leftarrow [2]\,Q$
   if $k_j = 1$:
   $Q \leftarrow Q + P$
3. **return** Q

Сложность

удвоений: $O(\lg k)$
сложений: $\omega t(k) \sim O(\lg k)$
(ωt – вес Хэмминга k)
всего: $O\,(\lg k)$

Протокол Диффи – Хеллмана

Выработка общего секретного ключа

 $\xleftrightarrow{\quad P \in E(\mathbb{F}_q) \quad}$ 

$a \in \mathbb{N} \xrightarrow{\qquad [a]P \qquad}$

$\xleftarrow{\qquad [b]P \qquad} b \in \mathbb{N}$

$\boxed{[ab]P = [a]([b]P)}$ $\qquad$ $\boxed{[ab]P = [b]([a]P)}$

- Безопасность основана на сложности нахождения **DLOG**:

$$(P, [n]P) \mapsto n$$

Оптимизация: проективные координаты

$$E : Y^2Z = X^3 + AxZ^2 + BZ^3$$

$$P_3 = P_1 + P_2$$
$$u = Y_2Z_1 - Y_1Z_2$$
$$v = X_2Z_1 - X_1Z_2$$
$$X_3 = v(\underbrace{u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2}_{w}),$$
$$Y_3 = u(X_1v^2Z_2 - w) - v^3Z_2Y_1$$
$$Z_3 = v^3Z_1Z_2$$

Сложность

12M (проективные) **vs** I + 3M (аффинные)

Оптимизация: особые формы кривой

Кривые Монтгомери:

$$By^2 = x^3 + Ax^2 + x$$

Сложность
удвоение+сложение: 6M + 4S

Curve25519: $B = 1, A = 486662, q = p = 2^{255} - 19.$
Также: кривые Эдвардса, в форме Якоби и др.

Литература

- I. Blake и др. *Elliptic curves in cryptography*. 1999.
- A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. 1993.
- L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.

Контакты

snovoselov@kantiana.ru