

Эллиптические кривые

Лекция 2. Групповой закон

Семён Новосёлов

БФУ им. И. Канта

2024



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 $x_1 \neq x_2$:

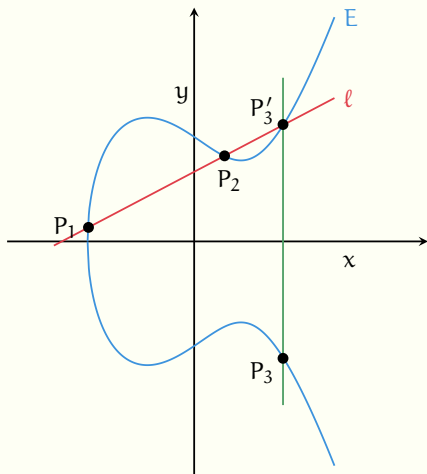
$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

СЛОЖНОСТЬ

$I + 3M$ в K



Групповой закон - 2

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

$$P_1 = (x_1, y_1) \in E$$

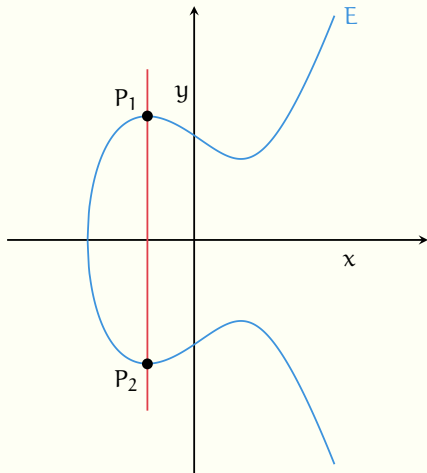
$$P_2 = (x_2, y_2) \in E$$

$$P_3 = P_1 + P_2 = (x_3, y_3)$$

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 $P_1 = P_2, y_1 \neq 0$:

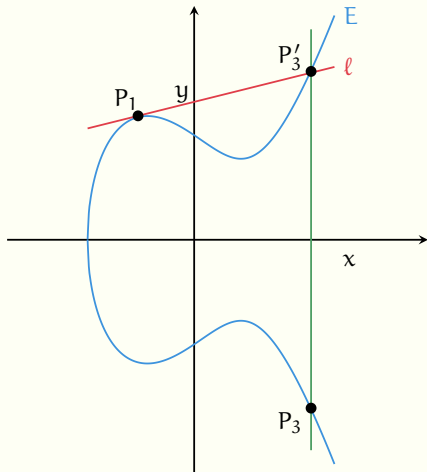
$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

$$m = \frac{3x_1^2 + A}{2y_1}$$

СЛОЖНОСТЬ

I + 4M в K



Групповой закон - 4

Теорема

- 1 $P_1 + P_2 = P_2 + P_1$ (коммутативность)
- 2 $P + \mathcal{O} = P \forall P \in E$ (\exists нейтральный элемент)
- 3 $\forall P \in E \exists P' \in E : P + P' = \mathcal{O}$ (\exists 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

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

Бинарный метод:

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

- 1 $Q \leftarrow O$
- 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

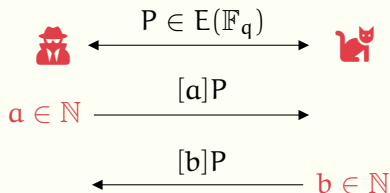
$k - 1$ сложений (наивно)

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



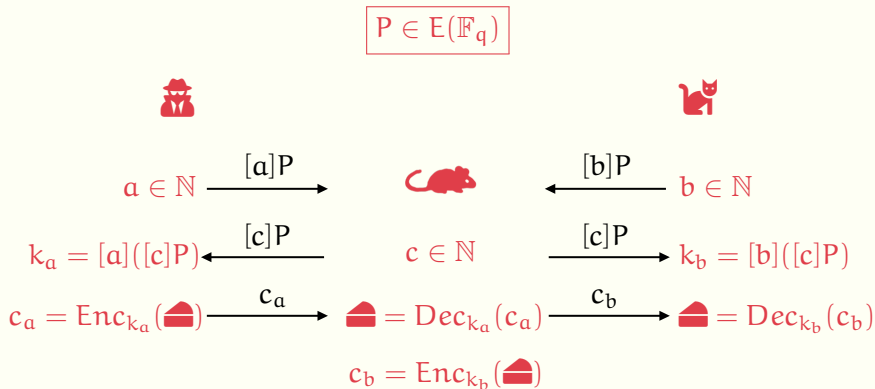
$$[ab]P = [a]([b]P)$$

$$[ab]P = [b]([a]P)$$

- Безопасность основана на сложности нахождения **DLOG** (как минимум):

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

Атака “человек посередине”¹



¹(англ.) man in the middle (MITM)

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** 1 + 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.

Цифровая подпись

Общие параметры: кривая E над \mathbb{F}_q , $P \in E(\mathbb{F}_q)$, $r = \text{ord}(P)$.

Генерация ключей 🐱:

- 1 🔑 секретный ключ: $a \in [1, r]$
- 2 📩 открытый ключ: $Q = [a]P$

Подпись сообщения 📩:

- 1 🐱 выбирает $k \in [1, r]$ и вычисляет $R = [k]P = (x, y)$
- 2 📩 вычисляет $s = k^{-1}(\text{📩} + ax) \bmod r$
- 3 🐾 = (R, s)

Проверка подписи 🐾 = (R, s):

- 1 🏠 вычисляет $u_1 = s^{-1} \text{☑} \bmod r$ и $u_2 = s^{-1} x \bmod r$
- 2 $S = [u_1]P + [u_2]Q$
- 3 проверяет равенство $S = R$.

Корректность:

$$\begin{aligned} S &= [u_1]P + [u_2]Q = [s^{-1} \text{☑}]P + [s^{-1} x]Q = \\ &= [s^{-1}]([\text{☑}]P + [x a]P) = [k]P = R \end{aligned}$$

- используется повсеместно в составе протокола TLS
- для безопасности схемы требуется ряд ограничений на параметры
- ECDSA / ГОСТ 34.10-2018

Литература

- Washington L.C. "Elliptic curves number theory and cryptography"
- Menezes A. "Elliptic curve public key cryptosystems"
- Blake I., Seroussi G., Smart N. "Elliptic Curves in Cryptography"

Контакты

snovoselov@kantiana.ru

Страница курса:

crypto-kantiana.com/semyon.novoselov/teaching/elliptic_curves_2024