Эллиптические кривые

Лекция 1. Введение

Семён Новосёлов

БФУ им. И. Канта

2023

Мотивация

Криптография:

- классическая – дискретный логарифм (ECDH, ECDSA)
- постквантовая – схемы на изогениях (~~SIKE~~, CSIDH, SQISign)

База для построения множества схем и протоколов.

Примеры использования

Классическая криптография в реальном мире:

- **https** (TLS): цифровая подпись
- **WireGuard VPN** в составе ядра Linux: Curve25519, обмен ключами
- **SSH**: кривая Эдвардса Ed25519
- **Bitcoin/Ethereum**: кривая Secp256k1, цифровая подпись

Постквантовая криптография – перспективы

SIKE/SIDH: обмен ключами

- был кандидатом на стандартизацию в Round 3 NIST

SIKE Cryptographic Challenge

- github.com/microsoft/SIKE-challenges/
- 5000 USD или 50 000 USD за взлом

- взломан Castryck и Decru, используя информацию о точках кручения в протоколе
- замена: **weakSIDH**, **CSIDH**

Есть также подписи: **OSIDH**, **SQISign**.

* Castryck W., Decru T. An efficient key recovery attack on SIDH. `https://eprint.iacr.org/2022/975`
* `https://issikebrokenyet.github.io/`

План курса

1. Введение
2. Групповой закон на эллиптической кривой
3. Точки n-кручения
4. Алгоритмы подсчета $\mathbb{F}_q$-рациональных точек кривой
5. Алгоритм факторизации на эллиптических кривых
6. Тест на простоту Goldwasser-Kilian
7. Выбор эллиптической кривой для криптографии
8. Криптографические схемы на изогениях

Порядок работы

Формат: лекции **+** сдача лабораторных работ

- после лекций выкладываются лабораторные работы
- срок сдачи: **2** недели
- за пределами срока сдачи работы принимаются с низким приоритетом и в количестве не более **2** за пару

Экзамен: сдать **85%** лабораторных и **курсовую**

- оценка – среднее по оценкам за сдачу лабораторных

Определение

Уравнение Вейерштрасса **в аффинных координатах**:

$$f : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

Уравнение над полем K – **гладкое**, если во множестве его решений над $\overline{K}$ нет сингулярных точек.

Эллиптическая кривая задаётся как

$$E(K) = \{(x, y) \in K \times K : f(x, y) = 0\} \cup \{\mathcal{O}\}$$

для гладкого f.

- $\mathcal{O}$ – точка в бесконечности.
- K – некоторое поле, чаще всего $K = \mathbb{F}_q$.

Проективные координаты

Уравнение Вейерштрасса в проективных координатах:

$$F : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (2)$$

где $a_i \in K$.

- сингулярное: $\exists P \in \mathbb{P}^2(K) : \frac{dF}{dX}(P) = \frac{dF}{dY}(P) = \frac{dF}{dZ}(P) = 0$.
- гладкое (или несингулярное) в противном случае.

Эллиптическая кривая E – множество точек $\mathbb{P}^2(K)$, удовлетворяющих гладкой кривой (2).

- Точка в бесконечности: $\exists! \mathcal{O} = (0 : 1 : 0)$.
- Проективные координаты позволяют избежать деления в арифметике за счёт доп. умножений.

Дискриминант

Как проверить, что уравнение Вейерштрасса задаёт эллиптическую кривую? Обозначим

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1 a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24d_4 \end{aligned} \tag{3}$$

Тогда **дискриминант** уравнения (1) определяется как

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6.$$

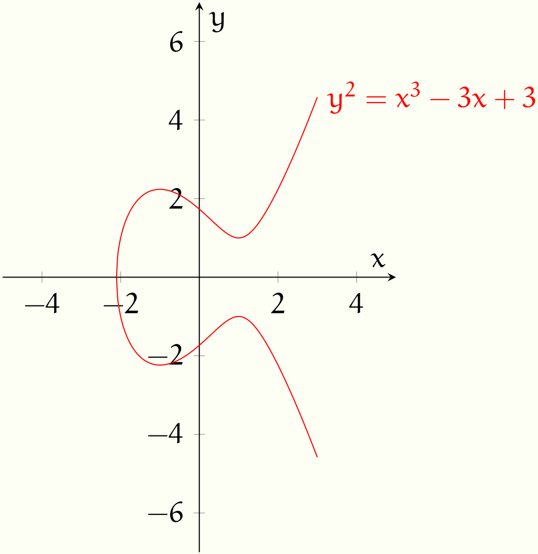
Классификация уравнений Вейерштрасса

Теорема [Silverman, Thm. 1.4]

1. $\Delta \neq 0 \iff$ кривая гладкая ($\implies$ задаёт эллиптическую кривую)
2. $\Delta = 0, c_4 \neq 0 \iff$ кривая обладает узлом (node)
3. $\Delta = c_4 = 0 \iff$ кривая обладает точкой перегиба (cusp)

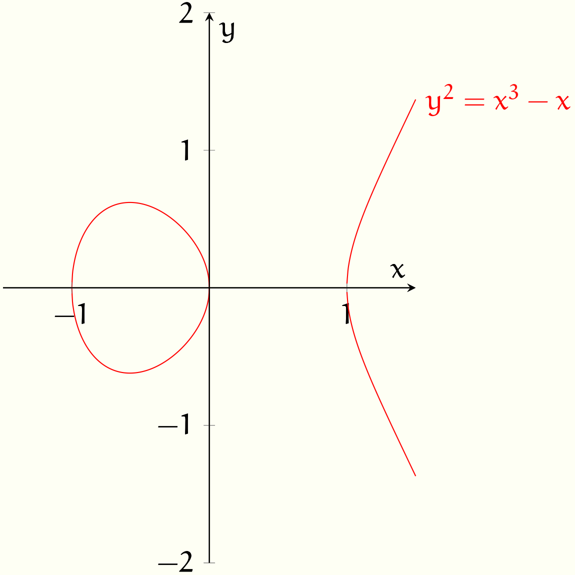
Классификация уравнений Вейерштрасса - 2

$\Delta < 0$



Классификация уравнений Вейерштрасса - 3

$\Delta > 0$



Изоморфизмы эллиптических кривых

Пусть $E_1/K, E_2/K$ – эллиптические кривые с уравнениями:

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 &: y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \end{aligned} \tag{4}$$

$E_1/K, E_2/K$ **изоморфны**, если они изоморфны как проективные многообразия.

Теорема

$E_1 \simeq E_2 \iff \exists u, r, s, t \in K, u \neq 0$ такие, что замена

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{5}$$

преобразует кривую E_1 в E_2.

Изоморфизм кривых задаёт отношение эквивалентности.

Изоморфизмы – зачем нужно?

Позволяют подбирать форму кривой под нужные свойства в арифметике. Например:

- с меньшим кол-вом коэффициентов: ускорение вычислений
- с константным временем выполнения группового закона: противодействие атакам по побочным каналам

Краткие формы

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

$\mathrm{char}\, K \neq 2$: Изоморфизм

$$(x, y) \mapsto \left(x, \frac{1}{2}(y - a_1x - a_3)\right)$$

преобразует E/K к виду:

$$E/K : y^2 = 4x^3 + d_2x^2 + 2d_4 + d_6. \tag{6}$$

$\mathrm{char}\, K \neq 2, 3$: Изоморфизм

$$(x, y) \mapsto \left(\frac{x - 3d_2}{36}, \frac{y}{216}\right)$$

Преобразует (6) к виду:

$$E/K : y^2 = x^3 + ax + b \tag{7}$$

$$a = -27c_4$$

$$b = -56(d_2^3 + 36d_2d_4 - 216d_6)$$

Краткие формы - 2

В последнем случае,

$$\Delta = -16(4a^3 + 27b^2)$$

$\mathrm{char} K = 2$**:**

$$a_1 \neq 0 \implies (x, y) \mapsto \left(a_1^2 x + \frac{a_3}{a_1};\ a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3}\right)$$

$$E/K : y^2 + xy = x^3 + a_2' x^2 + a_6' \qquad (8)$$

$$a_1 \neq 0 \implies (x, y) \mapsto (x + a_2, y)$$

$$E/K : y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad (9)$$

Определение изоморфности кривых

j-инвариант эллиптической кривой E:

$$j(E) = \frac{c_4^3}{\Delta}$$

или для краткой формы $j(E) = -1728\frac{4a^3}{\Delta}$.

Теорема

$$E_1 \simeq E_2 \text{ над } \overline{K} \iff j(E_1) = j(E_2)$$

Определение изоморфности кривых над полем K: проверка условий теоремы. Если выполняется – составление и решение системы уравнений используя (5).

Литература

1. Washington L.C. ”Elliptic curves number theory and cryptography”
2. Menezes A. ”Elliptic curve public key cryptosystems”
3. Hankerson D., Menezes A., Vanstone S. ”Guide to elliptic curve cryptography”
4. Blake I., Seroussi G., Smart N. ”Elliptic Curves in Cryptography”
5. Silverman J.H. ”The Arithmetic of Elliptic Curves”

Контакты

snovoselov@kantiana.ru

Страница курса:

crypto-kantiana.com/semyon.novoselov/teaching/elliptic_curves_2023

Темы курсовых

1. Криптоанализ схем на изогениях (несколько тем)
2. Схема цифровой подписи SQISign
3. Атака Кастрика-Декру
4. crypto-kantiana.com/thesis_topics.html