БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель С. Новоселов Осень 2025

Лекция 1. Введение

Эллиптические кривые используются в криптографии как основа для построения множества криптографических примитивов, схем и протоколов, таких как цифровых подписи и схемы обмена ключами.

В настоящее время в криптографии выделяется два направления: классическая криптография и посквантовая. К классической криптографии относятся криптографические схемы, построенные на основе сложности задач дискретного логарифмирования, факторизации целых чисел и других. Однако, данные задачи могут быть взломаны на квантовом компьютере за полиномиальное время. В связи с этим появилось новое направление криптографических исследований – постквантовая криптография требует от схем стойкость к атакам на квантовом компьютере.

Среди распространённых классических схем на эллиптических кривых имеются схема подписи (ECDSA) и обмен ключами по протоколу Диффи-Хэлмана на эллиптических кривых (ECDH).

Из перспективных постквантновых схем на эллиптических кривых можно отметить схемы, построенные на сложности задачи вычисления изогении между эллиптическими кривыми – цифровую подпись SQISign и схему обмена ключами CSIDH.

Классическая криптография в настоящее время широко используется на практике в большом числе приложений.

1. Обмен ключами и цифровые подписи в протоколе HTTPS (TLS), который используется для шифрования данных при доступе к ресурсам в интернете (см. Рис. 1).
2. В составе протоколов для построения VPN: обмен ключами в протоколе WireGuard, встроенном в ядро Linux, осуществляется на базе эллиптической кривой Curve25519.
3. Кривые Эдвардса Ed25519 можно использовать для цифровой подписи в протоколе SSH.
4. Bitcoin/Ethereum используют кривую Secp256k1 для цифровой подписи транзакций.

Хотя на практике современные квантовые компьютеры в настоящее время не могут взломать классические криптосистемы на эллиптических кривых, предполагается, что такие компьютеры могут быть созданы в течении 10 лет.

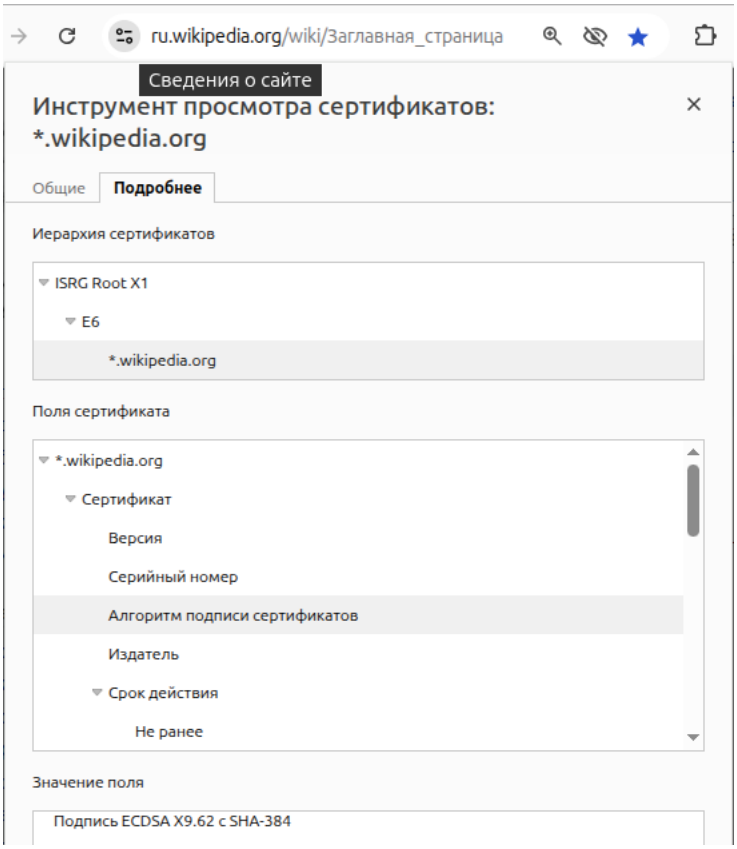
Полный отказ от классической криптографии (ECDSA, ECDH, FFDH, RSA) рекомендован NIST начиная с 2035 года. А с 2030 года классические схемы объявлены устаревшими. Это значит, что начиная с этих дат будет прекращена поддержка классической криптографии в популярных протоколах сети Интернет (TLS, https, ssh).

В качестве замены предлагаются различные схемы постквантовой криптографии. В эллиптической криптографии, это SQISign вместо ECDSA, CSIDH вместо ECDH. Однако, в настоящее время схемы на изогениях не утверждены в качестве стандартов.

1 План курса

1. Введение
2. Групповой закон на эллиптической кривой
3. Точки n-кручения

Рис. 1: Пример. Wikipedia использует сертификат на основе ECDSA



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

Заметим, что и классическая криптография и постквантовая криптография имеют одну и ту же теоретическую базу. И всё, что используется в классической криптографии на эллиптических кривых, используется и в постквантновой. Поэтому мы начинаем с классической криптографии и потом переходим к постквантовой.

2 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

3 Основные определения

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 $K = \mathbb{F}_q$.

Уравнение Вейерштрасса в проективных координатах:

$$F : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2}$$

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.

3.1 Дискриминант

Как проверить, что уравнение Вейерштрасса задаёт эллиптическую кривую? Для решения задачи используется дискриминант кривой. Обозначим

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24d_4 \end{aligned} \tag{3}$$

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

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6.$$

Данные формулы можно получить применив общую теорию дискриминантов [2, Ch. 13] к уравнению Вейерштрасса.

Theorem 3.1 ([5], Prop. 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)*

Рис. 2: Случай $\Delta < 0$

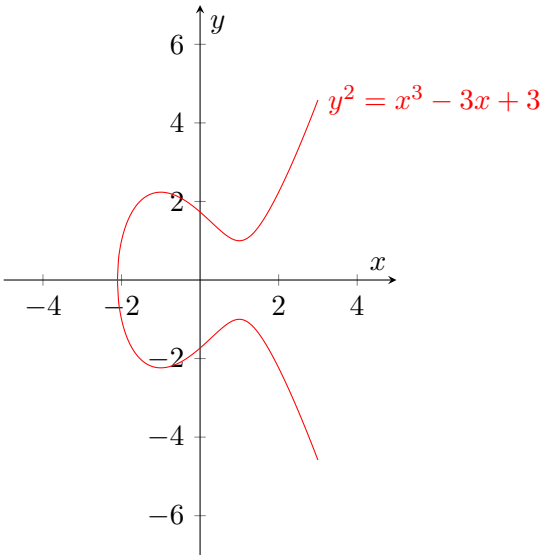
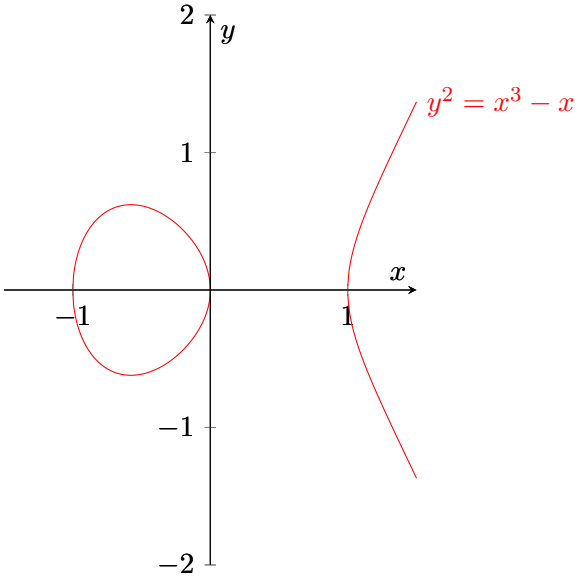


Рис. 3: Случай $\Delta > 0$



3.2 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, т.е. $\exists$ морфизмы $\phi : E_1/K \to E_2/K, \psi : E_2/K \to E_1/K$ (определённые над K), такие что $\psi \circ \phi = id_{E_1}, \phi \circ \psi = id_{E_2}$.

Theorem 3.2. *$E_1 \simeq E_2 \iff \exists u, r, s, t \in K, u \neq 0$ такие, что замена*

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

преобразует кривую E_1 в E_2.

Изоморфизм кривых задаёт отношение эквивалентности.

Зачем нужны изоморфизмы на практике? Они позволяют подбирать форму кривой под нужные свойства в арифметике. Например:

- с меньшим количеством коэффициентов: ускорение вычислений;
- с константным временем выполнения группового закона: противодействие атакам по побочным каналам.

3.3 Краткие формы

$$E/K : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1}$$

$\operatorname{char} K \neq 2$**:** Изоморфизм

$$(x, y) \mapsto \left(x, \frac{1}{2}(y - a_1 x - a_3) \right)$$

преобразует E/K к виду:

$$E/K : y^2 = 4x^3 + d_2 x^2 + 2d_4 + d_6. \tag{6}$$

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

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

Преобразует (6) к виду:

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

$$a = -27c_4$$
$$b = -56(d_2^3 + 36 d_2 d_4 - 216 d_6)$$

В последнем случае,

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

$charK = 2$**:**

$$a_1 \neq 0 \implies (x, y) \mapsto \left(a_1^2 x + \frac{a_3}{a_1};\ a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$
$$E/K : y^2 + xy = x^3 + a_2' x^2 + a_6' \tag{8}$$

$$a_1 \neq 0 \implies (x, y) \mapsto (x + a_2, y)$$
$$E/K : y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{9}$$

3.4 Определение изоморфности кривых

j-инвариант эллиптической кривой E:

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

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

Theorem 3.3. *$E_1 \simeq E_2$ над $\overline{K}$ $\iff$ $j(E_1) = j(E_2)$.*

Теорема даёт необходимые условия изоморфности, но не достаточности, так как кривые могут быть изоморфны над алгебраическим замыканием поля, но неизоморфными над базовым полем.

Таким образом определение изоморфности кривых над полем K состоит в проверке условий теоремы, а затем, если условия теоремы выполняются, то составлении и решении системы уравнений, используя (5).

Список литературы

[1] I. Blake и др. *Elliptic curves in cryptography*. 1999.

[2] I. M. Gelfand, M. M. Kapranov и A. V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Springer, 1994.

[3] D. Hankerson, A. J. Menezes и S. Vanstone. *Guide to elliptic curve cryptography*. 2006.

[4] A. J. Menezes. *Elliptic Curve Public Key Cryptosystems*. 1993.

[5] J. H. Silverman. *The arithmetic of elliptic curves*. 2-е изд. 2009.

[6] L. C. Washington. *Elliptic curves: number theory and cryptography*. 2008.