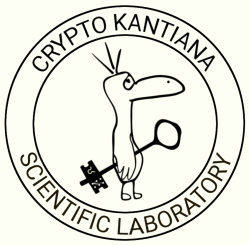
Криптосистемы на эллиптических кривых

Семён Новосёлов

БФУ им. И. Канта

Математическая школа НИЯУ МИФИ
Секция 1: Дискретная математика и ее приложения
04.12.2023



IKBFU

План

I. Классическая криптография
(на основе задачи дискретного логарифмирования)

II. Постквантовая криптография
(на основе задачи вычисления изогении)

I. Классическая криптография

1. Где используется?
2. Предварительные сведения
3. Схема обмена ключами
4. Схема подписи
5. Выбор кривой для криптографии

Где используется?

Классическая криптография на ЭК в реальном мире:

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

Где не используется?

Для **шифрования** лучше использовать симметричные схемы, используя эллиптические кривые (и в целом криптографию с открытым ключом) только для генерации общего секретного ключа.

Эллиптические кривые vs RSA

RSA

- криптография в кольце $\mathbb{Z}_N$
- задача факторизации
- сложность атаки $L_N(1/3)$
- размеры ключей $1024, 2048, 3072, 15360$

ЭК

- криптография в группе точек кривой над $\mathbb{F}_q$
- задача вычисления DLOG
- сложность атаки $q^{1/2}$
- размеры ключей $160, 224, 256, 512$

Дополнительно: случайная ЭК ведёт себя примерно как обычная группа.

- для группы G доказана[1] нижняя граница для сложности DLOG: $\Omega(\sqrt{\#G})$

[1] Shoup V. “Lower Bounds for Discrete Logarithms and Related Problems”. EUROCRYPT’97

Предварительные сведения

Эллиптическая кривая

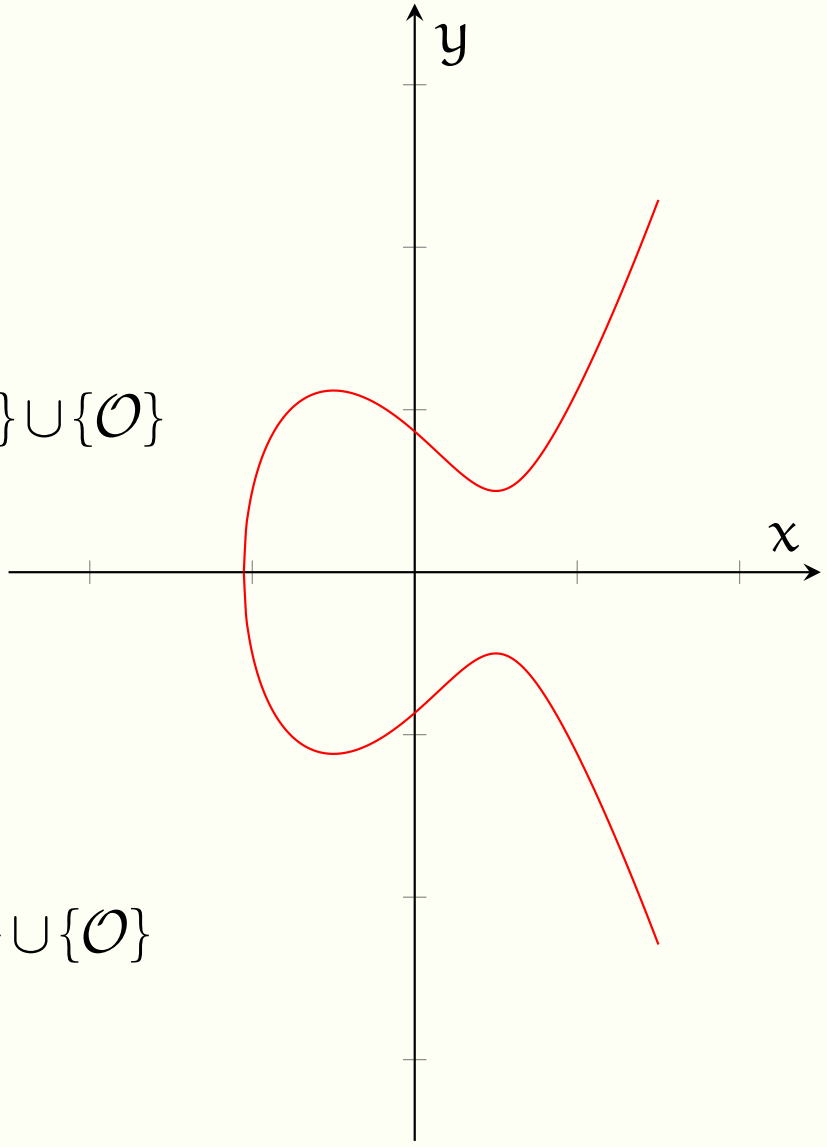
$$E/\mathbb{K} : y^2 = x^3 + ax + b$$

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

- $E(\mathbb{K})$ – группа
- $\mathcal{O}$ – нейтральный элемент

Расширение поля $\mathbb{L} \supseteq \mathbb{K}$

$$E(\mathbb{L}) = \{(x, y) \in \mathbb{L}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$



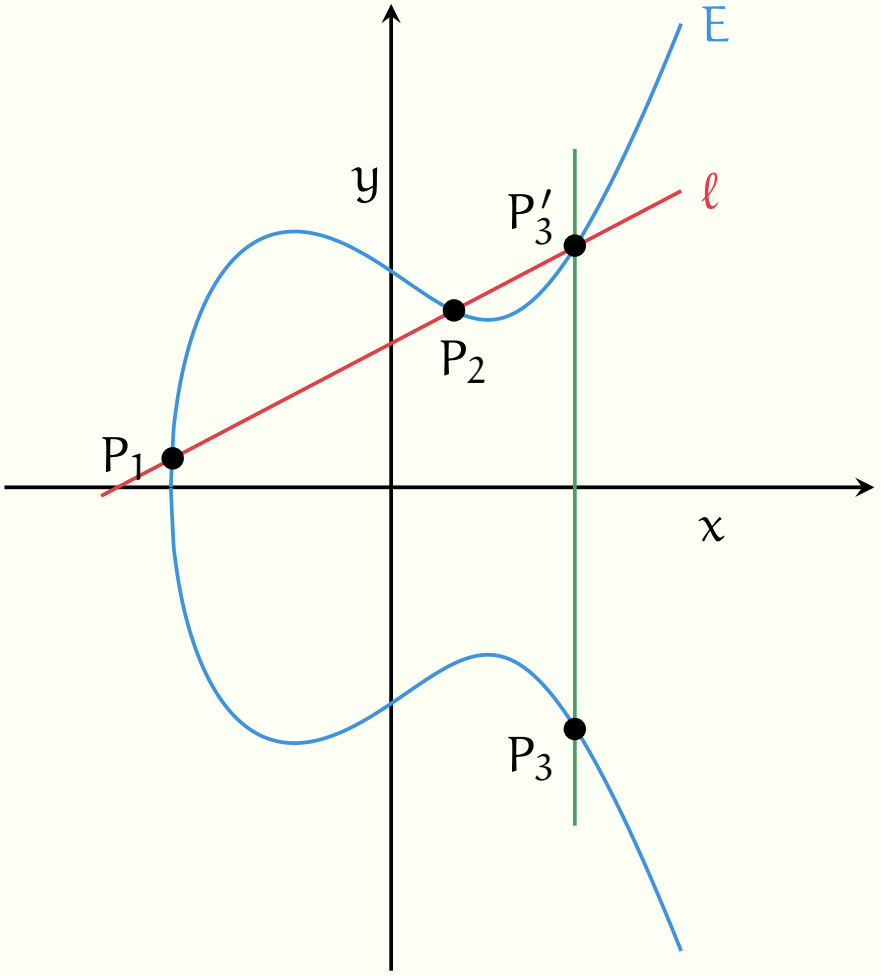
Групповой закон

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

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

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

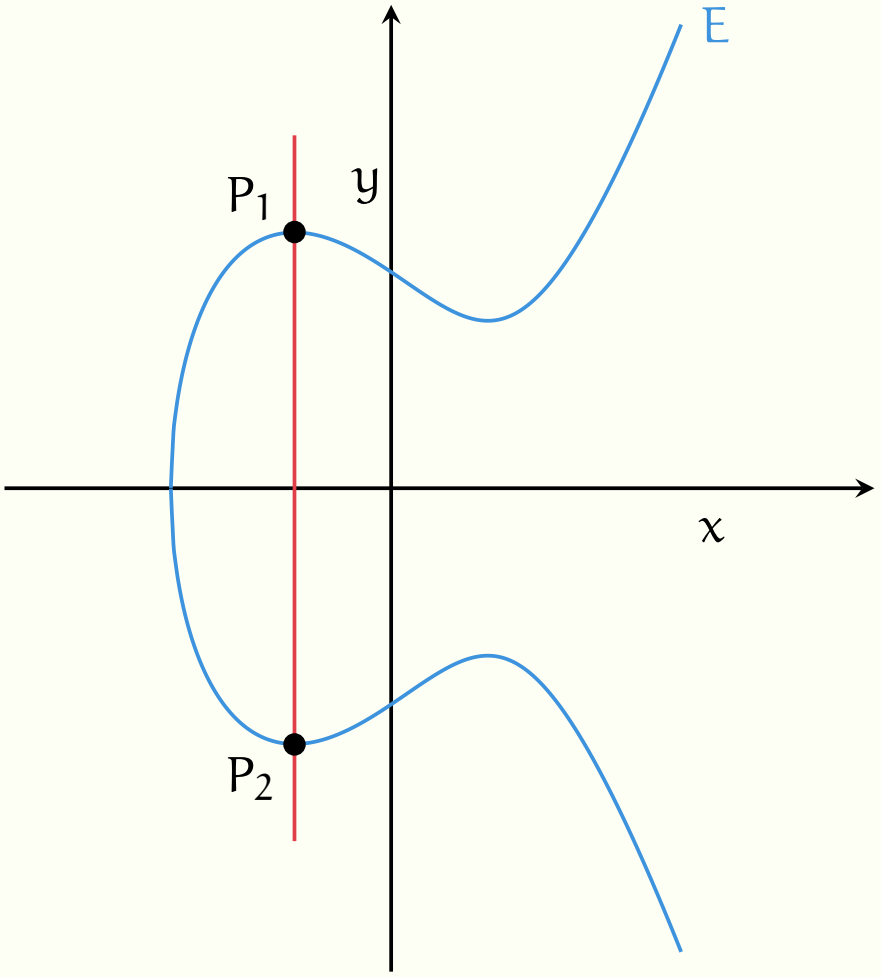
Групповой закон - 2

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

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

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

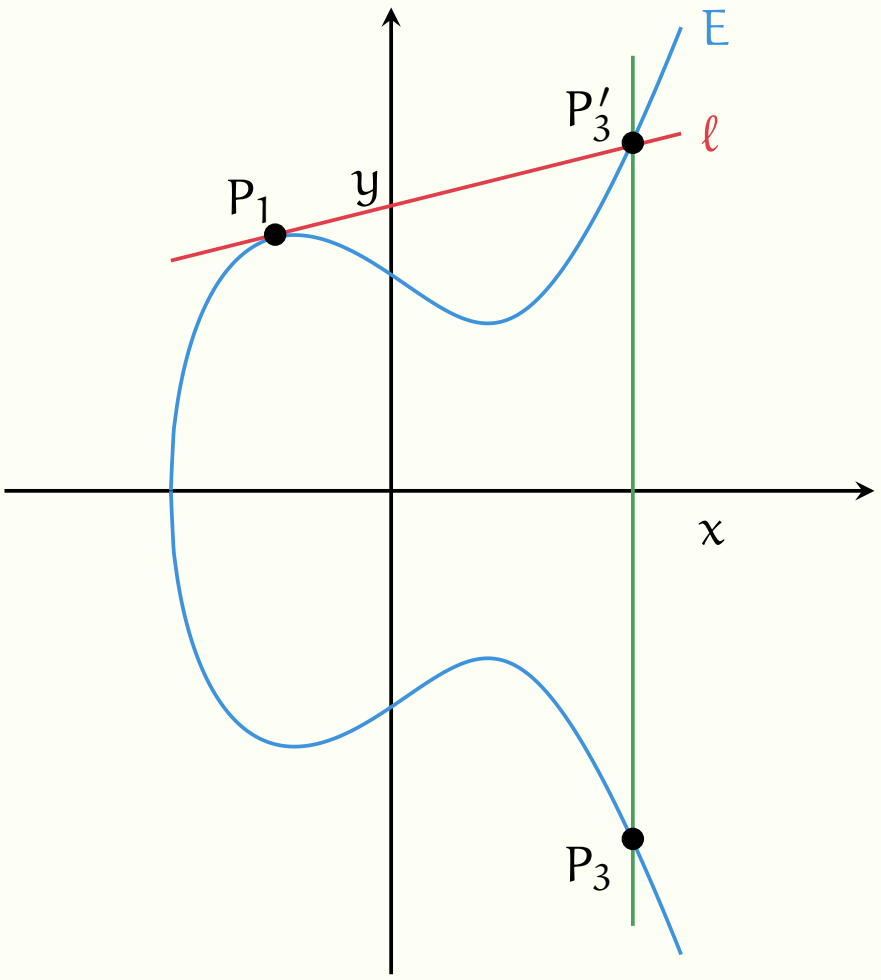
$$E/K : y^2 = x^3 + Ax + B$$

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

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



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: $O(\lg k)$

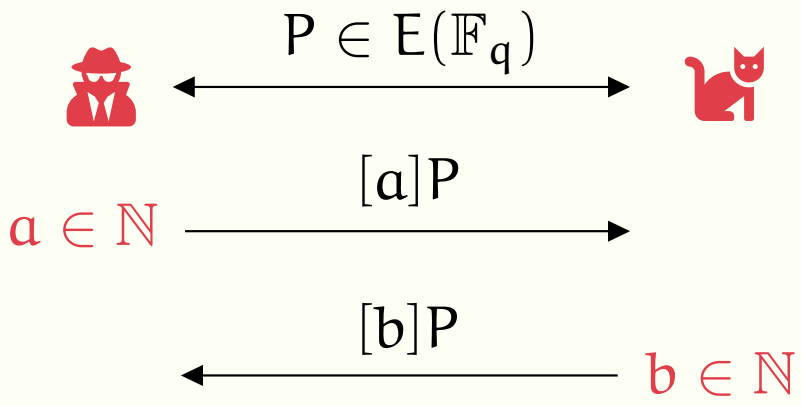
Схема обмена ключами

Задача: имеется два абонента, которые знают открытые ключи друг друга, сгенерировать общий секретный ключ, передавая сообщения по ***открытому*** каналу.

- секретный ключ может использоваться далее для шифрования сообщений при помощи быстрых симметричных шифров
- такие схемы широко используются в Интернете (протокол HTTPS = HTTP + TLS)

Протокол Диффи – Хеллмана

Выработка общего секретного ключа



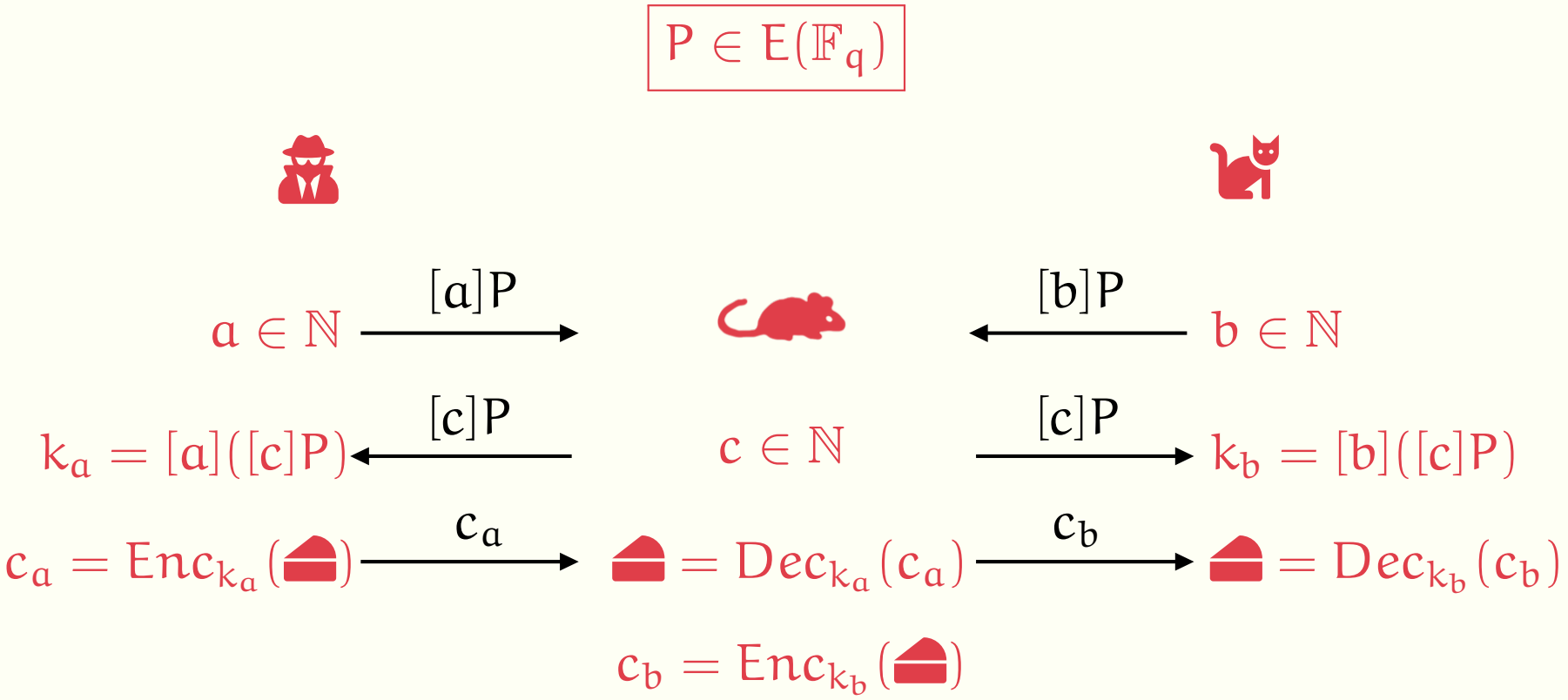
$$[ab]P = [a]([b]P)$$

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

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

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

Атака “человек посередине”[2]



[2] *(англ.)* man in the middle (MITM)

Цифровая подпись

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

Генерация ключей 🐱:

1. секретный ключ: $a \overset{🐟}{\in} [1, r]$
2. открытый ключ: $Q = [a]P$

Подпись сообщения ✉:

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

Проверка подписи 🐾 = (R, s):

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

Корректность:

$$S = [u_1]P + [u_2]Q = [s^{-1}✉]P + [s^{-1}x]Q =$$
$$= [s^{-1}]([✉]P + [xa]P) = [k]P = R$$

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

Выбор кривой для криптографии

Требования:

1. Безопасность:
   - для параметра безопасности λ сложность наилучшей известной атаки должна быть $\approx 2^{\lambda}$
   - на данный момент $\lambda \approx 128$.
2. Эффективность:
   - групповой закон должен вычисляться быстро.

Безопасность

$$E/\mathbb{F}_q : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- $N = \#E(\mathbb{F}_q)$, вычисляем с помощью SEA за $O(\log^4 q)$
- $N = O(q)$ (граница Хассе-Вейля)
- $G = \langle P \rangle$ для $P \in E(\mathbb{F}_q)$
- для эффективности: $\#G = \operatorname{ord} P \approx \#E(\mathbb{F}_q)$

DLOG: $Q = [\ell]P, \quad (P, Q) \mapsto \ell$

Каждая известная атака накладывает ограничения по безопасности на (N, q, ℓ).

Атака BSGS или $\rho-$методом Полларда

Алгоритм BSGS основан на парадоксе дней рождений.

Сложность: $\widetilde{O}(\sqrt{\#G}) = \widetilde{O}(\sqrt{q})$ по времени и по памяти.

- ρ-метод Полларда: сложность по памяти $O(\operatorname{polylog} q)$.

Вывод:

- для уровня безопасности $\lambda = 128$ требуется кривая с подгруппой G порядка $\approx 2^{256}$
- т.е. над полем $\mathbb{F}_q$ размера $q \approx 2^{256}$

Атака Полига-Хеллмана

Принцип: решить задачу DLOG в подгруппах G с помощью ρ-метода Полларда и восстановить искомый DLOG в G по КТО.

$$\#G = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} \implies G \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$$

т.е. $G \simeq G_1 \oplus \ldots \oplus G_m$, где $\#G_1 = p_1^{e_1}, \ldots, \#G = p_m^{e_m}$.

Сложность: $\widetilde{O}(\sum e_i(\log \#G + \sqrt{p_i}))$

$\Downarrow$

Вывод: для безопасности $\#G = cr$, где r – большое простое число, c – малое число.

Комбинируя условия двух атак получаем, что группа точек кривой должна как минимум:

- содержать подгруппу **простого** порядка размера 256-бит для уровня безопасности 128-бит.
- соответственно, размер поля $q \approx 2^{256}$.

Атака спуском Вейля

При $q = p^n$ можно определить ограничение Вейля:

$$W/\mathbb{F}_p := W_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\mathbb{F}_p) = E(\mathbb{F}_{p^n}).$$

- Это абелево многообразие размерности n, т.е. проективное многообразие, обладающее структурой группы.
- Поэтому DLOG на $E/\mathbb{F}_{p^n}$ можно свести к $W/\mathbb{F}_p$.
- Имеет смысл, если $W/\mathbb{F}_p$ – якобиан кривой рода $g \geq 3$
- Условия, при которых это происходит, не до конца ясны.

В общем случае, работать с абелевыми многообразиями сложнее, чем с эллиптическими кривыми.

Консервативный выбор размера поля для криптографии с учётом существования атаки спуском Вейля: $q = p$.

Атака с помощью билинейных спариваний

Пусть $r = \#G$, $G \subseteq E(\mathbb{F}_q)$ и $\mu_r = \{x \in \overline{\mathbb{F}}_q | x^r = 1\}$.
Атака использует следующее отображение на $E[r]$.

Теорема (спаривание Вейля)

$\exists$ отображение $e_n : E[r] \times E[r] \to \mu_r$ со свойствами:

1. $e_r(T, T) = 1$
2. $e_r(T, S) = e_r(S, T)^{-1}$
3. $e_r(S_1 + S_2, T) = e_r(S_1, T)e_r(S_2, T)$ *(билинейность)*
   $e_r(S, T_1 + T_2) = e_r(S, T_1)e_r(S, T_2)$
4. $e_r(S, T) = 1, \forall T \implies S = \mathcal{O}$ *(невырожденность)*
   $e_n(S, T) = 1, \forall S \implies T = \mathcal{O}$

Другие билинейные отображения: спаривание Тейта, эта-спаривание.

Степень вложения: минимальное целое k т.ч. $E[r] \subseteq E(\mathbb{F}_{q^k})$.

Атака на DLOG: $|\langle P \rangle| = r$, $Q = \ell P$.

1. Выбрать случайную точку R.
2. $\alpha = e_r(P, R)$
3. $\beta = e_r(Q, R)$ $\qquad (\beta = e_r(\ell P, R) = e_r(P, R)^\ell = \alpha^\ell)$
4. $\ell = \mathrm{DLOG}(\alpha, \beta)$ в $\mathbb{F}_{q^k}$

Конструктивное использование: ZCash, IBE, ~~SIKE~~.

- Сложность решения DLOG в $\mathbb{F}_{q^k}$ используя NFS (и его модификации): $L_{q^k}(1/3, c)$.
- Для уровня безопасности $\lambda = 128$ требуется поле размера 3072-бит [ECRYPT'18].

$$\Downarrow$$

Для стойкости к атаке с помощью билинейных спариваний необходимо: $k \geq 24$ $(3072/128)$.

- Т.к. $\mu_r \subseteq \mathbb{F}_{q^k} \iff q^k \equiv 1 \pmod{r}$. Достаточно проверить, что:

$$r \nmid q^k - 1,$$

для $k = 1, \ldots, 24$.

Аномальные кривые

Кривые с $\#E(\mathbb{F}_p) = p$ называются **аномальными**.

- Если $\#G = p$ для кривой $E/\mathbb{F}_p$, то $\exists$ гомоморфизм $E[p] \to \Omega^0_E(\mathbb{F}_p)$

Здесь $\Omega^0_E(\mathbb{F}_p)$ – $\mathbb{F}_p$-векторное пространство голоморфных дифференциалов, где DLOG решается время $O(\mathrm{polylog}(p))$

- Подробнее: [Galbraith'12, §26.4.1].
- Условия легко проверяются.

Атаки на кривые с автоморфизмами

Существуют модификации методов BSGS или ρ-метода Полларда, использующие автоморфизмы.

- **Идея:** при поиске DLOG перебирать вместо точек P классы эквивалентности $(\mathrm{P}, \psi(\mathrm{P}), \psi^2(\mathrm{P}), \ldots, \psi^{\alpha-1}(\mathrm{P}))$ для $\alpha = \operatorname{ord} \psi$.
- **Сложность:** для модифицированного ρ-метода Полларда – $\mathrm{O}(\sqrt{\frac{\pi}{2\alpha}}\sqrt{\#\mathrm{G}})$ [Galbraith'12, Th. 14.4.3]

- Может быть обобщено на эндоморфизмы, в случае если их можно эффективно вычислить.

Пример кривой:

$$E/\mathbb{F}_p : y^2 = x^3 + a_6,$$

- Автоморфизм: $(x, y) \mapsto (\zeta_3 x, y)$ для $p \equiv 1 \pmod 3$, $\alpha = 3$.
- Эффективная арифметика, т.к. $a_4 = 0$.
- Однако нужно учитывать ускорение DLOG.

Условия безопасности для $\lambda = 128$ относительно основных атак.

$$E/\mathbb{F}_q : y^2 = x^3 + a_4 x + a_6$$

1. $r = \#\langle P \rangle \subseteq E(\mathbb{F}_q)$ – простое число, $\#E(\mathbb{F}_q)/r$ – малое число (стойкость к методу Полига-Хеллмана)
2. $r \approx 2^{256}$ (стойкость к ρ-методу Полларда)
3. $q = p$ (стойкость к спуску Вейля)
4. $r \nmid q^k - 1$ для $k \leq 24$ (стойкость к атакам на спариваниях)
5. $r \neq p$ (кривая не аномальная)

Дополнительно

- Параметры кривой должны сопровождаться детальным описанием откуда они взялись.
  - сиды всех псевдослучайных функций
  - выбор псевдослучайных функций / хеш-функций (если $a_4 = hash(seed), a_6 = hash(seed)$)
- Условия только для DLOG, не гарантируется безопасное использование E в протоколах

Эффективность

Есть 3 основных формы кривой E.

1. Краткая форма Вейерштрасса:

$$y^2 = x^3 + ax + b$$

2. Кривые Монтгомери:

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

3. Кривые Эдвардса:

$$x^2 + y^2 = 1 + dx^2y^2$$

Сравнение операций

Кривая/Операция	$P + Q$	$2P$
Кривая Вейерштрасса (проект. коорд.)	$12M + 2S$	$5M + 2S$
Кривая Вейерштрасса (коорд. Якоби)	$11M + 5S$	$1M + 8S$
Кривая Эдвардса	$10M + 1S$	$3M + 4S$
Кривая Монтгомери	$6M + 2S$[3]	$4M$

[3] для $2P + Q$

Литература

- Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. 2000
- Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. 2006
- Washington L.C. Elliptic curves: number theory and cryptography. 2008
- Blake I., et al. Elliptic curves in cryptography. 1999.
- Cohen H., et al. Handbook of elliptic and hyperelliptic curve cryptography. 2005.
- Galbraith S. D. Mathematics of public key cryptography. 2012.

II. Постквантовая криптография

Задача вычисления DLOG решается на квантовом компьютере за **полиномиальное** время.

- для кривой над полем размера 256 бит требуется квантовый компьютер[4] с 2124 логическими кубитами
- из-за наличия шума может потребоваться существенно больше физических кубит
- квантовые компьютеры постоянно совершенствуются

$\Longrightarrow$ необходимо разработать криптосистемы, стойкие к атакам на квантовом компьютере.

[4] Häner T., Jaques S., et al. “Improved Quantum Circuits for Elliptic Curve Discrete Logarithms”. PQCrypto 2020

Криптография на изогениях

Альтернатива постквантовой криптографии на решётках и кодах.

- основана на сложности задачи вычисления изогении между двумя кривыми
- в настоящее время отрасль перестраивается
- так как в 2022 году появилась полиномиальная атака Кастрика-Декру на схему SIDH/SIKE, перевернувшая данную область
- многие схемы стали неактуальными
- однако базовые задачи остались трудными

Изогении

Неформально: “хорошие функции между эллиптическими кривыми“, которые можно описать в виде дробей из многочленов.

Пусть E_1, E_2 – эллиптические кривые.

- ненулевой гомоморфизм, задаваемый рациональными функциями

В явном виде:

$$\phi(x,y) = \left(\frac{f_1(x,y)}{f_2(x,y)}, \frac{g_1(x,y)}{g_2(x,y)}\right) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$$

Степень изогении: $\deg \phi = \max\{\deg p(x), \deg q(x)\}$.

Изогения называется **сепарабельной**, если производная $\frac{p}{q}$ по x не равна 0, и **несепарабельной** в противном случае.

Для сепарабельных изогений $\deg \phi = \#\ker\phi$.

Если $E_1 = E_2$, то ϕ – эндоморфизм.

Пример 1: Умножение на m

$$[m] : E \to E,$$

$$P \mapsto m \cdot P.$$

Задаётся многочленами деления.

$$E/\mathbb{Q} : y^2 = x^3 + x$$

$$[2]P = \left(\frac{(x^2-1)^2}{4(x^3+x)}, y\frac{x^6+5x^4-5x-1}{8(x^3+x)^2} \right)$$

$$\ker[2] = \{\mathcal{O}; (x_P, 0) : x_P^3 + x = 0\}$$

$$\#\ker[2] = 4 = \deg[2],$$

Для сепарабельных изогений степень совпадает с $\#ker$.

Пример 2: Эндоморфизм Фробениуса

$$\phi : E \to E,$$

$$(x, y) \mapsto (x^q, y^q),$$

$$\phi = (x^q, y(x^3 + ax + b)^{\frac{q-1}{2}})$$

$$\ker \phi = \mathcal{O}_E, \deg \phi = q$$

(изогения не сепарабельная)

Теорема Тейта о изогениях эллиптических кривых

Эллиптические кривые E_1, E_2 изогенны над $\mathbb{F}_q \iff$

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$$

Следствие: проверка кривых на изогенность имеет сложность $O(\log^4 q)$ при использовании SEA.

Формулы Vélu

Пусть $E/\mathbb{F}_q$ – эллиптическая кривая, G – подгруппа $E(\overline{\mathbb{F}}_q)$.

Тогда:

1. $\exists E'/\mathbb{F}_q$ и сепарабельная изогения $\phi : E \to E'$ определённая над $\mathbb{F}_q$ степени $\#G$ т.ч. $\ker \phi = G$.
2. если $\psi : E \to E''$ – другая сепарабельная изогения степени $\#G$ т.ч. $G = \ker \psi$, то $j(E') = j(E'')$.

Обозначение: $E/G := E'$ – фактор-кривая.

Важно! Не путать с фактор-группой.

Vélu описал явные формулы для E', ϕ.

$$E : y^2 = x^3 + ax + b$$

$$\phi(P) = \left(x_P + \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(x_{P+Q} - x_Q \right), y_P + \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(y_{P+Q} - y_Q \right) \right).$$

А изогенная кривая определяется как:

$$E/G : y^2 = x^3 + a'x + b',$$

где

$$a' = a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(3x_Q^2 + a \right),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(5x_Q^3 + 3ax_Q + b \right).$$

Пример 3: Сепарабельная изогения

$$E/\mathbb{F}_7 : y^2 = x^3 + 2x + 4$$

$$P = (3, 3), G = \langle P \rangle, \#G = 5$$

$$\phi : (x, y) \mapsto \left(\frac{x^5 + 4x^4 + 4x^3 + 5x^2 + 2x + 3}{x^4 + 4x^3 + 2x^2 + 3x + 1}, y \frac{x^6 - x^5 + 3x^3 + 3x^2 + 2x}{x^6 - x^5 + 2x^4 + 3x^3 - 2x^2 - x - 1} \right)$$

$$E/G : y^2 = x^3 + 6x + 4$$

Степень ϕ равна 5.

Ядра изогений

$$[\ell]P = P + \ldots + P \text{ } (\ell\text{-раз})$$

Группа-кручения

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}) \mid [\ell]P = \mathcal{O}\}$$

- все ядра изогений степени ℓ – подгруппы $E[\ell]$
- перебирая все подгруппы $G \subseteq E[\ell]$ можно построить с помощью формул Велу все изогении степени ℓ

Важно: ядра изогений не принадлежат базовому полю в общем случае.

Пример 4: Изогения с ядром над расширением

$$E/\mathbb{F}_7 : y^2 = x^3 + 2x + 4$$

$$\mathbb{F}_{7^4} = \mathbb{F}_7[\alpha] / \left\langle \alpha^4 + 5\alpha^2 + 4\alpha + 3 \right\rangle$$

$$P = (5\alpha^3 + \alpha^2 + 5\alpha + 2, 5\alpha^3 + 6\alpha^2 + 4\alpha + 2)$$

$$G = \langle P \rangle \subset E[5], \#G = 5$$

$$\phi : (x, y) \mapsto \left(\frac{x^5 - x^4 - 3x^3 - 3x^2 - x - 2}{x^4 - x^3 + x + 1}, y \frac{x^6 + 2x^5 - x^4 + x^3 - 2x^2 + 3x - 1}{x^6 + 2x^5 + 3x^4 + 2x^3 - 3x^2 + 2x - 1} \right)$$

$$E/G : y^2 = x^3 + 3x + 4$$

Степень ϕ равна 5. Изогения определена над $\mathbb{F}_7$ несмотря на то, что её ядро G определено над $\mathbb{F}_{7^4}$.

Сложность вычисления ϕ и E/G: $O(|G|)$.

Оптимизации:

- Castryck-Decru-Vercauteren, ”Radical isogenies”
- Bernstein-De Feo-Leroux-Smith: $O(\sqrt{|G|})$, `velusqrt.isogeny.org`

G – подгруппа большого порядка $\Longrightarrow$ вычисление E/G является трудной задачей.

Это делает невозможными вычисления с секретными изогениями “в лоб” в криптосистемах.

Выход: брать $|G| = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$ для малых ℓ_i и вычислять изогению как композицию изогений малых степеней.

Проблема нахождения изогении

Общая задача нахождения изогении

Даны две изогенные кривые E_1 и E_2.
Известно, что степень изогении равна ℓ.
Вычислить изогению между ними.

При известном ядре G задача решается за полиномиальное время (если $\#\mathrm{G}$ – гладкое).

Суперсингулярные кривые:

- наилучший алгоритм – поиск на основе парадокса дней рождений
- сложность: $\mathcal{O}(\mathrm{p}^6)$ (квант. алг.) и $\mathcal{O}(\mathrm{p}^4)$ (класс. алг.)

Обычные кривые:

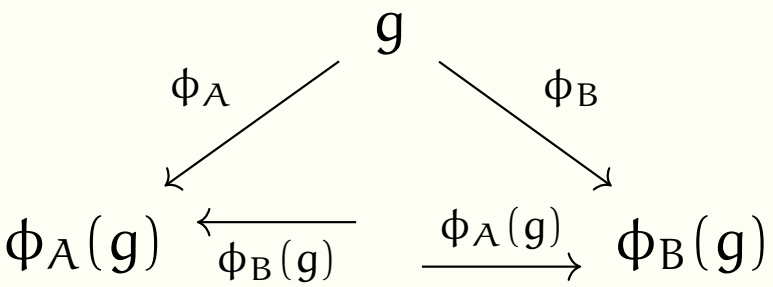
- квантовый субэкспоненциальный алгоритм

SIKE/SIDH

- Был одним из кандидатов на стандартизацию NIST
- Microsoft объявляла награду за взлом на $50,000 USD
- Для оптимизации в схему добавили дополнительную информацию об изогениях – значения секретной изогении в точках кручения.
- Что и привело в итоге к взлому данной системы.

“Стандартный” протокол DH в абстрактной группе

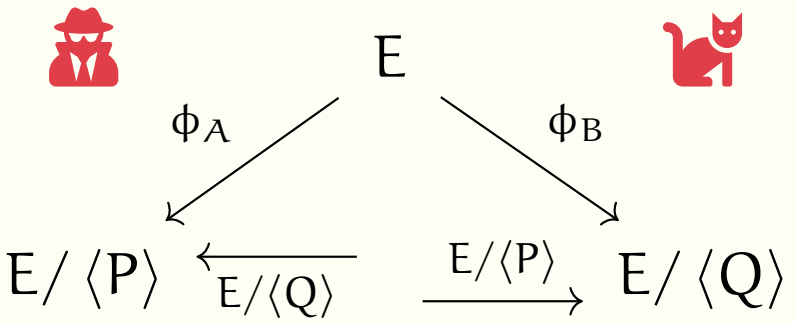
G – группа, $\langle g \rangle = G$, $\phi_A(x) = [A] \cdot x$ – гомоморфизм групп.



$$\phi_A(\phi_B(g)) = \phi_B(\phi_A(g)) = [AB] \cdot g$$

- изогении суперсингулярных кривых в качестве гомоморфизмов $\Rightarrow$ протокол SIDH (de Feo & Jao 2011)

SIDH (Supersingular Isogeny Diffie-Hellman)



Краткое описание:

1. Публичные параметры: E – суперсингулярная кривая.
2. выбирает секретное ядро $\langle P\rangle$, строит изогению и отсылает кривую $E/\langle P\rangle$
3. выбирает своё секретное ядро $\langle Q\rangle$, строит изогению и отсылает кривую $E/\langle Q\rangle$
4. Общий секретный ключ:
   $E/\langle P+Q\rangle = (E/\langle P\rangle)/\phi_A(Q) = (E/\langle Q\rangle)/\phi_B(P)$

Проблема: как посчитать $\phi_A(Q)$ и $\phi_B(P)$?

В SIDH для обхода данной проблемы публикуются значения секретных изогений в образующих групп кручения.

Детальное описание

Публичные параметры:

1. простое $p = \ell_A^{e_A} \ell_B^{e_B} \cdot c \pm 1$, где ℓ_A, ℓ_B – малые простые
2. E – суперсингулярная кривая над $\mathbb{F}_{p^2}$ т.ч. $\#E(\mathbb{F}_{p^2}) = (\ell_A^{e_A} \ell_B^{e_B} c)^2$
3. $\langle P_A, Q_A \rangle$ – базис $E[\ell_A^{e_A}]$, $\langle P_B, Q_B \rangle$ – базис $E[\ell_B^{e_B}]$

Секретные параметры:

$m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, изогения ϕ_A с ядром $\langle [m_A]P_A + [n_A]Q_A \rangle$

$m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, изогения ϕ_B с ядром $\langle [m_B]P_B + [n_B]Q_B \rangle$

Выработка общего ключа:

1.  $\Longrightarrow$  : $(E_A, \phi_A(P_B), \phi_A(Q_B))$
2.  $\Longrightarrow$  : $(E_B, \phi_B(P_A), \phi_B(Q_A))$
3.  : $E_{AB} := E_B / \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$
4.  : $E_{BA} := E_A / \langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle$
5. Общий секретный ключ: $j(E_{AB}) = j(E_{BA})$

Замечания

- сложность атаки (MITM): $O(\sqrt[4]{p})$ на классическом компьютере и $O(\sqrt[6]{p})$ для квантового компьютера
- гладкое число точек необходимо для быстрого вычисления изогений в точке
- можно выбрать E – обычную кривую с гладким числом точек $\Longrightarrow$ сложность атаки на квантовом компьютере становится субэкспоненциальной, т.к. кольцо эндоморфизмов – коммутативное.

SIKE. Параметры

1. $E : y^2 = x^3 + 6x^2 + x$
2. $p = 2^{e_A} 3^{e_B} + 1$
3. $\#E(\mathbb{F}_{p^2}) = 2^{e_A} 3^{e_B}$
4. $2^{e_A} \approx 3^{e_B}$

Атака Кастрика-Декру

- Castryck, Decru - An efficient key recovery attack on SIDH. 2022
- Maino, Martindale - An attack on SIDH with arbitrary starting curve. 2022
- Robert - Breaking SIDH in polynomial time. 2022

Выступление Castryck на ANTS XV:

- `https://www.youtube.com/watch?v=_eNv7An3Qj0`

Восстановление ключа

Пусть $G_B = \langle [m_B]P_B + [n_B]Q_B \rangle$ – секретное ядро  .

Задача восстановления ключа:

$$E, E/G_B, \phi_B(P_A), \phi_B(Q_A) \Longrightarrow \phi_B$$

Более того: $\phi_B = \phi_{e_B} \circ \ldots \circ \phi_2 \circ \phi_1$, где $\deg \phi_i = \ell_B$.

$$E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2 \xrightarrow{\phi_3} \ldots \xrightarrow{\phi_{e_B}} E/G_B$$

- в схемах на изогениях предполагается, что нельзя восстановить сначала ϕ_1, затем ϕ_2 и т.д.
- всего существует ℓ_B^2 вариантов выбора ϕ_i и перебор “в лоб” неэффективен.
- Кастрик и Декру предложили эффективный критерий для определения правильного варианта для ϕ_i на основе теоремы Кани’97.

Схемы стойкие к атаке

Замечание: если $\phi_B(P_A)$ и $\phi_B(Q_A)$ неизвестны (общая задача поиска изогении), то атака не работает.

Схемы не использующие точки кручения:

CSIDH, OSIDH, weakSIDH PoK, SeaSign, SQISign, CSI-FiSh

- issikebrokenyet.github.io

Схема CSIDH

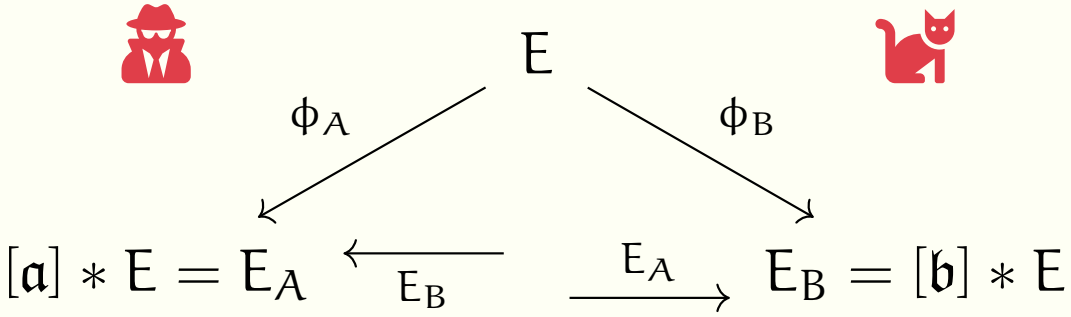
Предложена Castryck, Lange, Martindale, Panny и Renes.

- Основана на действии групп.
- Сложность классической атаки: $\mathcal{O}(\mathrm{p}^{1/4})$
- Сложность квантовой атаки: $\mathrm{L}(1/2)$

CSIDH: An Efficient Post-Quantum Commutative Group Action. ASIACRYPT 2018

`https://csidh.isogeny.org/`

Схема CSIDH - 2



Общий ключ: $E_{AB} = [\mathfrak{a}] * E_B = [\mathfrak{b}] * E_A = [\mathfrak{ab}] * E_0$

- $\mathfrak{a} \subset \mathrm{End}(E)$, кривая E_A и изогения вычисляются по формулам Велу, положив $G = \ker \mathfrak{a}$ (E_{AB}, E_B – аналогично)
- для формирования ключа требуется коммутативность
- из-за этого доступны квантовые субэксп. атаки

Схема CSIDH - 3

Публичные параметры схемы:

- простое $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, где $\ell_1, \ldots, \ell_n$ – малые простые.
- Суперсингулярная эллиптическая кривая $E_0 : y^2 = x^3 + x$ над полем $\mathbb{F}_p$.
- $\mathfrak{l}_i = (\ell_i, \pi_p - 1)$, $\mathfrak{l}_i^{-1} = (\ell_i, \pi_p + 1)$ – идеалы $\mathbb{Z}[\pi_p]$
- m – наименьшее положительное целое, такое, что $2m + 1 \geq \sqrt[n]{\#\,\mathrm{Cl}(\mathbb{Z}[\pi_p])}$.

Схема обмена ключами

Пользователь  :

1. выбирает секретный вектор $(e_1, \ldots, e_n) \in \{-m, \ldots, m\}^n$
2. определяет класс идеала $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \in \mathrm{Cl}(\mathbb{Z}[\pi_p])$
3. вычисляет свой открытый ключ $E_A = [\mathfrak{a}] * E_0$

Пользователь  :

1. выбирает секретный вектор $(f_1, \ldots, f_n) \in \{-m, \ldots, m\}^n$
2. определяет класс идеала $[\mathfrak{b}] = [\mathfrak{l}_1^{f_1} \cdots \mathfrak{l}_n^{f_n}] \in \mathrm{Cl}(\mathbb{Z}[\pi_p])$
3. вычисляет свой открытый ключ $E_B = [\mathfrak{b}] * E_0$

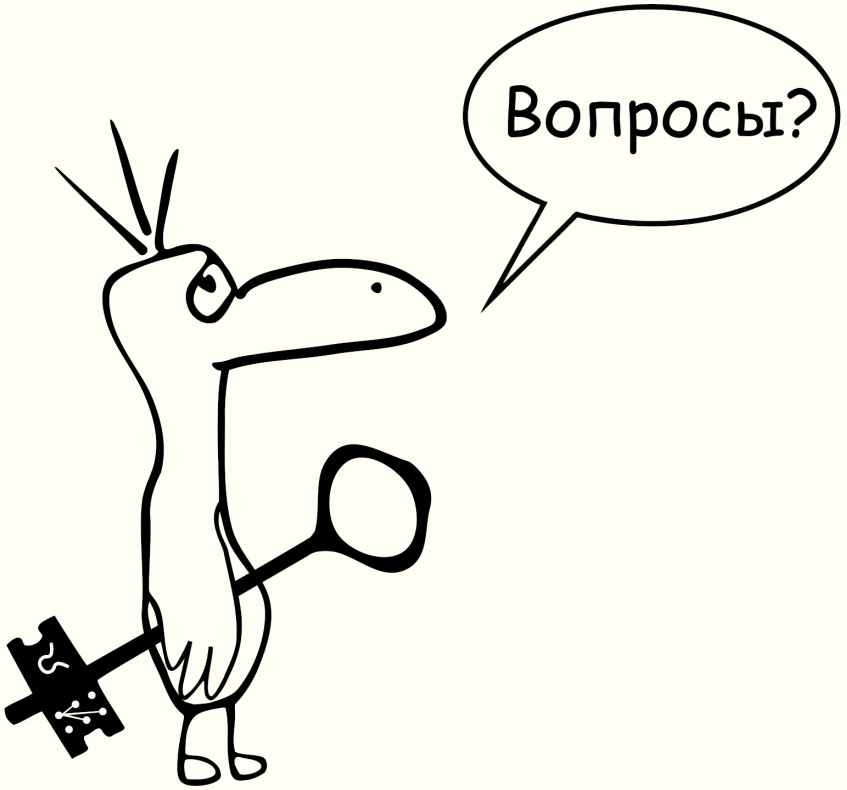
Общий ключ: $E_{AB} = [\mathfrak{a}] * E_B = [\mathfrak{b}] * E_A = [\mathfrak{ab}] * E_0$

Размеры ключей

Схема	Уровень стойкости	Открытый ключ	Закрытый ключ	Общий ключ
CRS	128/56	64	8	64
OSIDH	128/128	36	31	36
CSIDH-512	128/62	64	32	64

Таблица 1: Размеры ключей (в байтах) для актуальных схем обмена ключами на изогениях.

- CRS/CSIDH: субэкспоненциальные квантовые атаки
- OSIDH: экспоненциальные квантовые атаки



Контакты

snovoselov@kantiana.ru
crypto-kantiana.com/semyon.novoselov