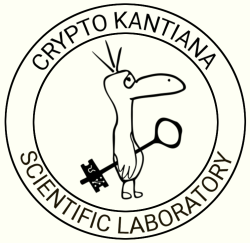
Криптосистемы на изогениях эллиптических кривых

Семён Новосёлов

06.12.2024



Мотивация

Постквантовая криптография.

- малые размеры ключей
- медленная скорость работы
- схемы CSIDH, ~~SIKE~~, weakSIDH, SeaSign, SQISign

Содержание

I. Предварительные сведения

Эллиптическая кривая

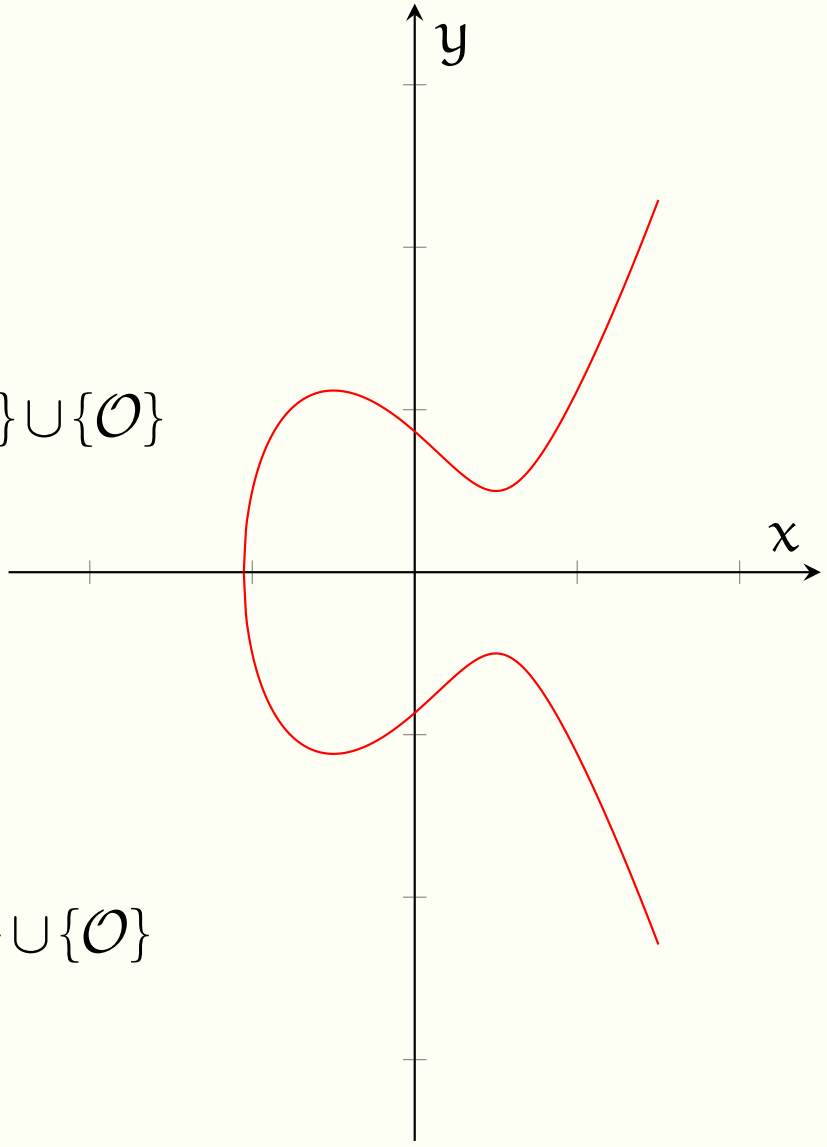
$$E/\mathbb{K} : y^2 = x^3 + ax + b$$

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

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

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

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



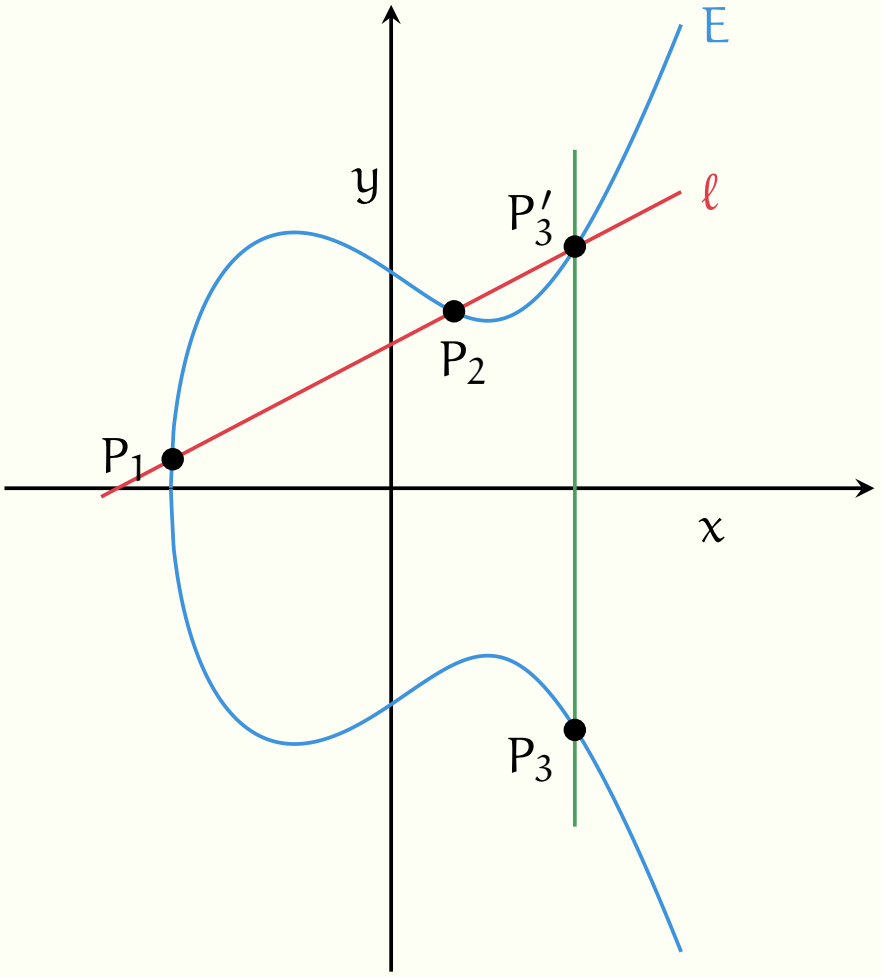
Групповой закон

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

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

Случай $x_1 \neq x_2$**:**

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



Изогении

Пусть E_1, E_2 – эллиптические кривые.

- В общем случае абелевых многообразий, **изогения** – гомоморфизм с конечным ядром, сюръективный над замыканием поля.
- Для эллиптических кривых определение упрощается: **изогения** – ненулевой гомоморфизм.

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

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

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

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

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

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

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

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:

- сложность: экспоненциальная

Обычные кривые:

- квантовый субэкспоненциальный алгоритм

II. Схема CSIDH

Предложена Castryck, Lange, Martindale, Panny и Renes.

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

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

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

Схемы на действиях групп

Схема CSIDH и многие другие схемы строятся на принципе действия группы на множество.

Определение

Пусть G – группа, X – множество. Тогда G **действует** на X, если:

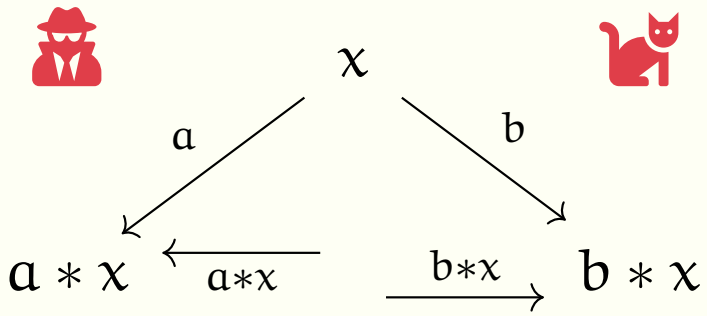
1. $\exists$ отображение $* : G \times X \to X$
2. $\forall g_1, g_2 \in G$ и $x \in X$:

$$g_1 * (g_2 * x) = (g_1 g_2) * x$$

Требования для построения криптосистем:

- восстановление g по известному $g * x$ должно быть сложной задачей (обобщение задачи **DLOG**)

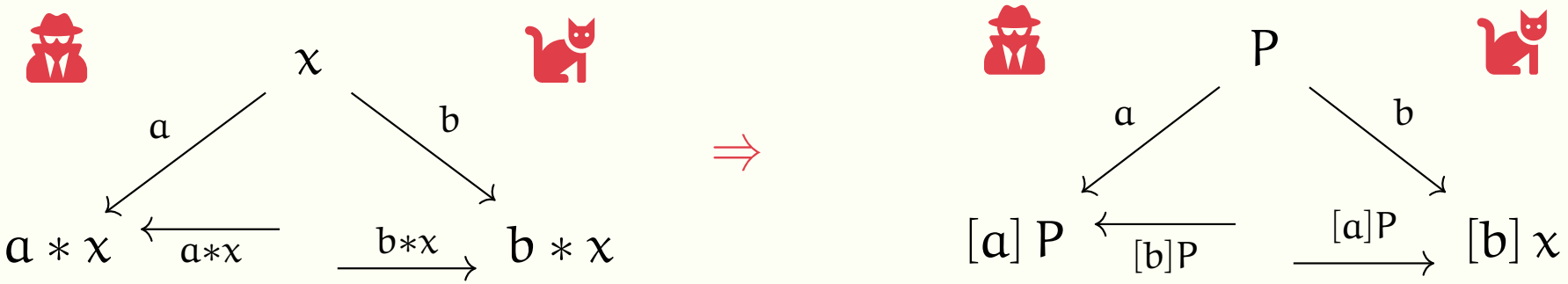
Протокол Диффи-Хеллмана на действиях групп



- $x \in X$ – публичный параметр
- $a, b \in G$ – секретные ключи абонентов
- общий секретный ключ:

$$(ab) * x = a * (b * x) = b * (a * x)$$

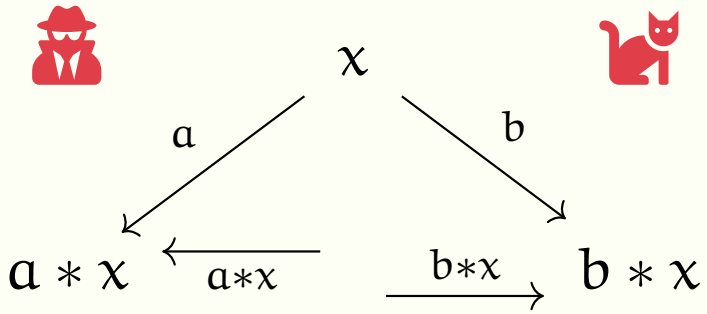
Пример. Классическая схема на ЭК



- $X = E(\mathbb{F}_p), x = P \in E(\mathbb{F}_p)$
- $G = \mathbb{Z}_r^\times$, где $r = \#\langle P \rangle$
- $a, b \in \mathbb{Z}_r^\times$
- $*$ – скалярное умножение точки на число

Аналогично описывается схема Диффи-Хеллмана на конечных полях.

Постквантовая схема CSIDH



Идейно:

$X = SS_p$

- множество суперсингулярных кривых над $\mathbb{F}_p$

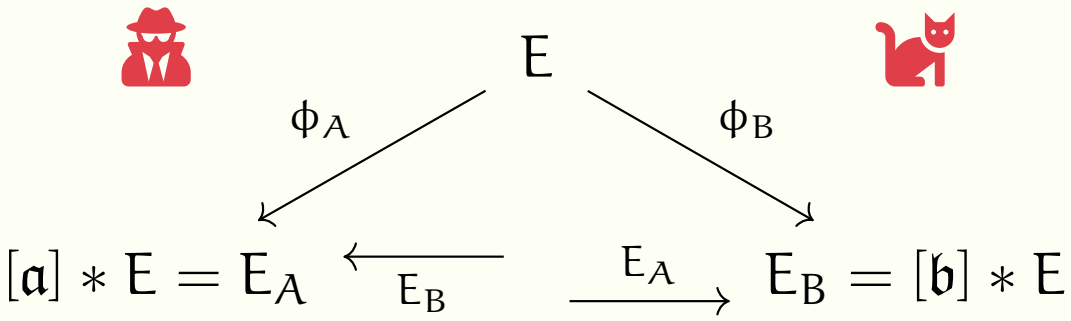
G = “изогении с точностью до эндоморфизмов”

- эндоморфизмы образуют петли и циклы в графе изогений, поэтому изогении можно редуцировать $\bmod \mathrm{End}(E)$

$*$: действие изогении на кривую

- формулы Велу + соотношение Дойринга для связи эндоморфизмов с изогениями

Постквантовая схема CSIDH



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

- для формирования ключа требуется коммутативность
- из-за этого доступны квантовые субэксп. атаки

Кольца эндоморфизмов эллиптических кривых

Кольцо эндоморфизмов $\mathrm{End}(\mathrm{E})$ эллиптической кривой E над конечным полем $\mathbb{F}_q$ изоморфно[1]:

- порядку в квадратичном мнимом поле (**обычные кривые**)
- максимальному порядку в алгебре кватернионов (**суперсингулярные кривые**)

Порядок – конечно порожденное над $\mathbb{Z}$ подкольцо (кольца целых в первом случае или алгебры кватернионов во втором).

Т.е. подкольцо $\mathcal{O}$ вида $\mathcal{O} = \omega_1\mathbb{Z} \times \ldots \times \omega_k\mathbb{Z}$ для некоторых ω_i из базового кольца.

[1] Deuring M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. 1941

Соответствие Дойринга

Эквивалентность между изогениями эллиптических кривых и идеалами кольца эндоморфизмов.

Идеалы по определению замкнуты относительно умножения на элементы кольца (эндоморфизмы).

- реализация идеи “работы с изогениями с точностью до эндоморфизма”
- главные идеалы соответствуют эндоморфизмам
- группа классов $\mathrm{CL}_{\mathcal{O}}$: фактор-группа группы идеалов по главным идеалам (эндоморфизмам)

Соответствие Дойринга в явном виде

Пусть $\mathfrak{a}$ – идеал порядка $\mathcal{O}$, который изоморфен кольцу эндоморфизмов кривой E или его подкольцу. Определим **$\mathfrak{a}$-кручение** как

$$E[\mathfrak{a}] = \left\{ P \in E(\overline{\mathbb{F}}_q) : \alpha(P) = P_\infty \ \forall \alpha \in I \right\}.$$

Тогда идеалу $\mathfrak{a}$ сопоставим изогению $\phi_\mathfrak{a}$ с ядром $E[\mathfrak{a}]$.

В обратную сторону: пусть ϕ-изогения, тогда соответствующий ей идеал равен

$$\mathfrak{a}_\phi = \{ \alpha \in \mathcal{O} : \alpha(P) = P_\infty \ \forall P \in \ker(\phi) \}.$$

CSIDH

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

III. Криптоанализ

1. Атаки на основе парадокса дней рождений
2. Использование кольца эндоморфизмов
3. Восстановление изогений по значениям в точках

Атаки на основе парадокса дней рождений

- Поиск по полному графу изогений над $\mathbb{F}_{p^2}$: $\mathcal{O}(\sqrt{p})$

[DelfsGalbraith13]:

- сводим задачу к графу изогений над $\mathbb{F}_p$
- для целевых кривых выполняются случайные блуждания, пока не получатся кривые над $\mathbb{F}_p$
- между кривыми над $\mathbb{F}_p$ задача решается за время $\mathcal{O}(p^{1/4})$

Использование кольца эндоморфизмов

Задача вычисления изогении эквивалентна нахождению колец эндоморфизмов кривых **[Wesoloswki21]**.

Сложность вычисления кольца эндморфизмов:
[Eisentrager+20]: $\mathcal{O}(\sqrt{\mathrm{p}})$ (классическая)
[Biasse+14]: $\mathcal{O}(\mathrm{p}^{1/4})$ (квантовая)

[Wesolowski+23]: знание одного нецелого эндоморфизма позволяет найти всё кольцо за (квантовое) субкэкспоненциальное время

[LoveBoneh20]: детектирование эндоморфизмов малой степени и построение изогении на их основе

Восстановление изогений по значениям в точках

Как правило, если известны несколько значений функции в точках, то восстановить её полностью не просто.

- для изогений – это **не верно**.

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:

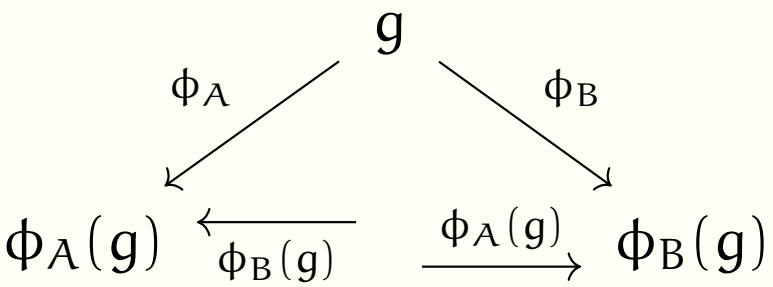
- `https://www.youtube.com/watch?v=_eNv7An3Qj0`

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

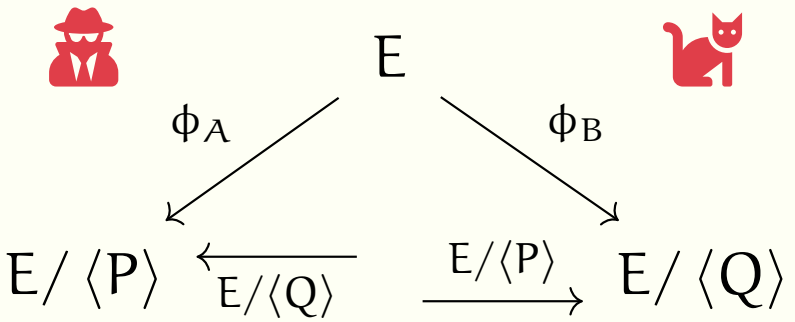
G – группа, $\langle g \rangle = G$, $\phi_A(x) = [A] \cdot x$ – гомоморфизм групп.



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

- 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. $2^{e_A} \approx 3^{e_B}$

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.

Склейка эллиптических кривых

Пусть E и F – две (суперсингулярные) эллиптические кривые. Тогда:

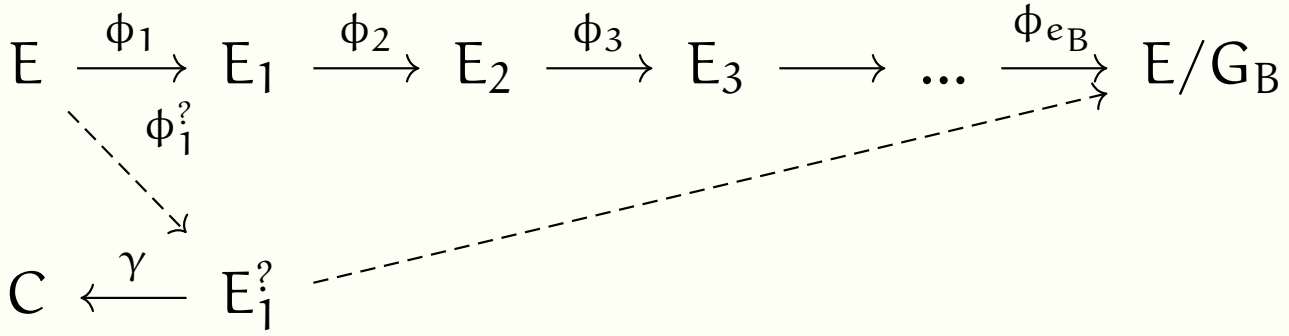
- $\mathrm{E} \times \mathrm{F}$ – абелева поверхность ($\dim = 2$)
- для подгруппы $\mathrm{H} \subseteq \mathrm{E} \times \mathrm{F}$ можно определить фактор-поверхность $\mathrm{A}' = (\mathrm{E} \times \mathrm{F})/\mathrm{H}$ по аналогам формул Велу.

Может быть два случая:

1. $\mathrm{A}' \simeq \mathrm{Jac}_\mathrm{C}$ с вероятностью $\approx 1 - 1/\mathrm{p}$ (H – **неразложимая**)
2. $\mathrm{A}' \simeq \mathrm{E}' \times \mathrm{F}'$ с вероятностью $\approx 1/\mathrm{p}$ (H – **разложимая**)

Атака

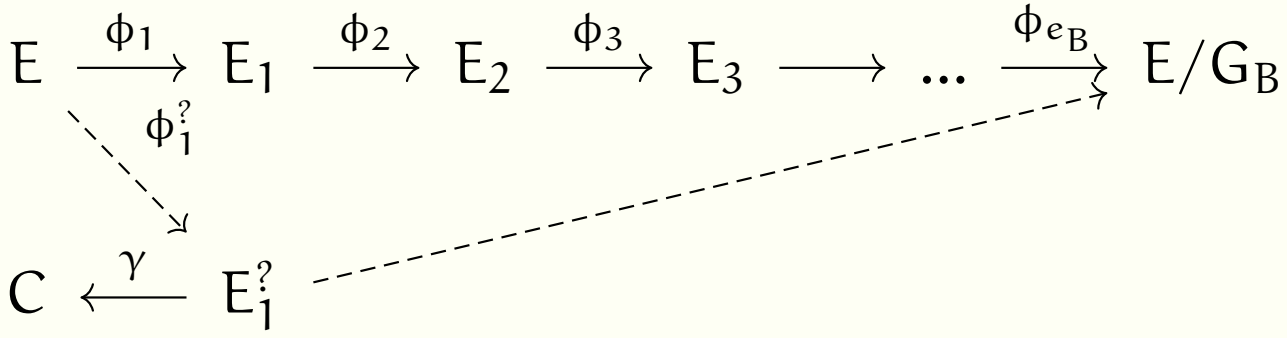
Рассмотрим процесс восстановления ϕ_1.



1. Выбрать $\phi_1^? : E \to E_1^?$ – один из ℓ_B^2 вариантов для ϕ_1
2. Построить (любую) вспомогательную изогению $\gamma : E_1^? \to C$ степени $\ell_A^{e_A} - \ell_B^{e_B - 1}$
3. $P_C = \gamma(\phi_1^?(P_A))$, $Q_C = \gamma(\phi_1^?(Q_A))$
4. Если подгруппа $H = \langle (P_C, \phi_B(P_A)), (Q_C, \phi_B(Q_A)) \rangle \subseteq C \times E/G_B$ – разложима, то $\phi_1^? = \phi_1$, $E_1^? = E_1$
5. В противном случае выбрать другую $\phi_1^?$

Атака

Рассмотрим процесс восстановления ϕ_1.



Откуда это взялось?

- Подгонка под условия теоремы [Кани97] с классификацией разложимых подгрупп.
- При $\phi_1^? = \phi_1$ всегда выполняется теорема Кани и группа H разложима
- При $\phi_1^? \neq \phi_1$ группа будет неразложима с вероятностью $\approx (1 - 1/p)$

Схемы стойкие к атаке

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

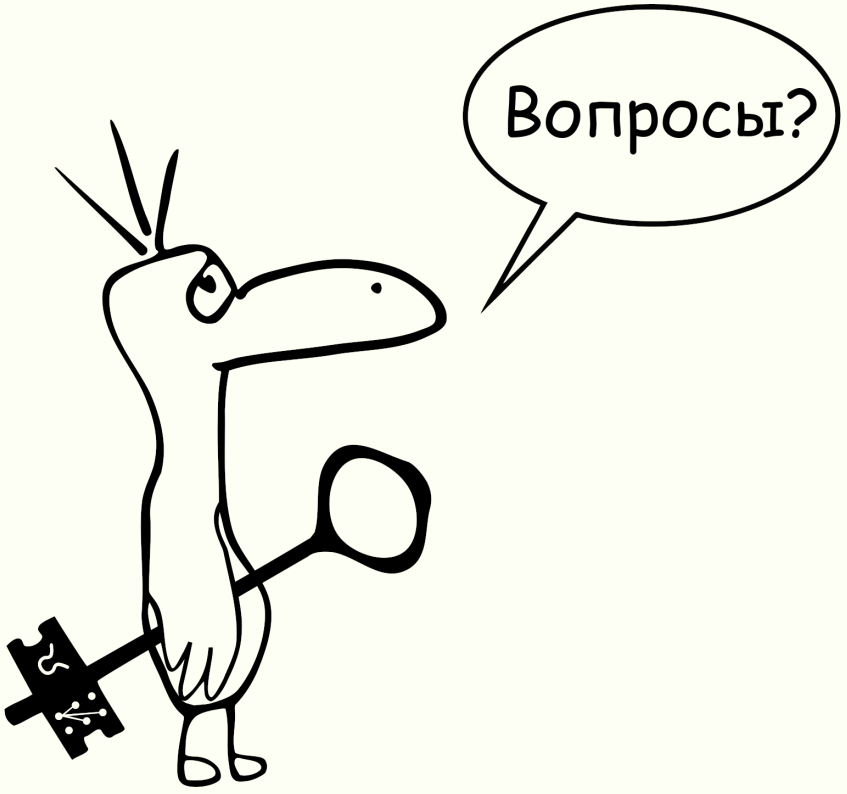
Схемы не использующие точки кручения:

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

issikebrokenyet.github.io

Вывод: для вычисления секретной изогении достаточно её значений в двух точках.

- атака Кастрика-Декру перевернула всю область
- многие схемы стали неактуальными
- однако базовые задачи остались трудными
- на основе атаки получили более быстрые подписи (SQIsignHD)



Контакты

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