Эллиптические кривые

Лекция 11. Изогении II

Семён Новосёлов

БФУ им. И. Канта

2023

Актуальные схемы на изогениях

Обмен ключами:

- CSIDH, ~~SIKE~~, CRS, OSIDH

Подписи:

- SQISign, weakSIDH

issikebrokenyet.github.io

Схема CSIDH

Предложена Castryck, Lange, Martindale, Panny и Renes.

- Основана на действии групп.
- 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

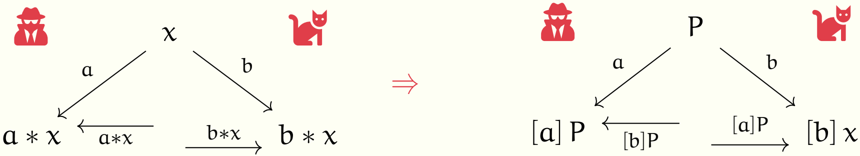
$$\begin{tikzcd}
 & x \arrow[dl, "a"'] \arrow[dr, "b"] & \\
a * x & & b * x \arrow[ll, shift right, "a*x"'] \\
 & &
\end{tikzcd}$$

$$\begin{tikzcd}
a * x \arrow[r, "b*x"] & b * x
\end{tikzcd}$$

- $x \in X$ – 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

$$\begin{tikzcd}
 & x \arrow[dl, "a"'] \arrow[dr, "b"] & \\
a * x \arrow[rr, leftarrow, shift left, "a*x"'] & & b * x \arrow[ll, leftarrow, shift left, "b*x"']
\end{tikzcd}$$

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 $\bmod \operatorname{End}(E)$

$*$: действие изогении на кривую

- формулы Велу + соотношение Дойринга для связи эндоморфизмов с изогениями

Постквантовая схема CSIDH

$$\begin{tikzcd}
 & E \arrow[dl, "\phi_A"'] \arrow[dr, "\phi_B"] & \\
{[\mathfrak{a}] * E = E_A} & & {E_B = [\mathfrak{b}] * E} \arrow[ll, shift right, "E_B"'] \\
{} \arrow[rr, "E_A"] & & {}
\end{tikzcd}$$

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

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

Кольца эндоморфизмов эллиптических кривых

Кольцо эндоморфизмов $\mathrm{End}(E)$ 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 $2m + 1 \geq \sqrt[n]{\# \operatorname{Cl}(\mathbb{Z}[\pi_p])}$.

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

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

Литература

- Castryck, Lange, Martindale, Panny, Renes.
  CSIDH: An Efficient Post-Quantum Commutative Group Action. ASIACRYPT 2018
  `https://csidh.isogeny.org/`
- Deuring M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.
  1941

Контакты

snovoselov@kantiana.ru