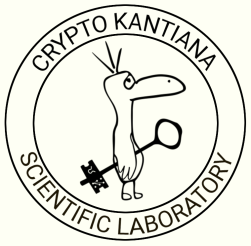
Эллиптические кривые

Лекция 10. Изогении

Семён Новосёлов

БФУ им. И. Канта

2022



Мотивация

- Постквантовая криптография на изогениях
- Схемы CSIDH, ~~SIKE~~, weakSIDH, SeaSign

План

1. Определение и примеры изогений
2. SIKE/SIDH
3. Атака Castryck-Decru (общая схема)
4. “Оставшиеся в живых” схемы (след. лекция)

I. 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 изогению можно задать следующими рац. функциями (для кривых в краткой форме):

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

Такая форма называется стандартной.

Степень изогении: $\deg \phi = \max\{\deg p(x), \deg q(x)\}$.
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. Не путать с фактор-группой.

Vélu описал явные формулы для E', ϕ. Для $E : y^2 = x^3 + ax + b$ имеем

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

А изогенная кривая E/G задаётся уравнением $y^2 = x^3 + a'x + b'$, где

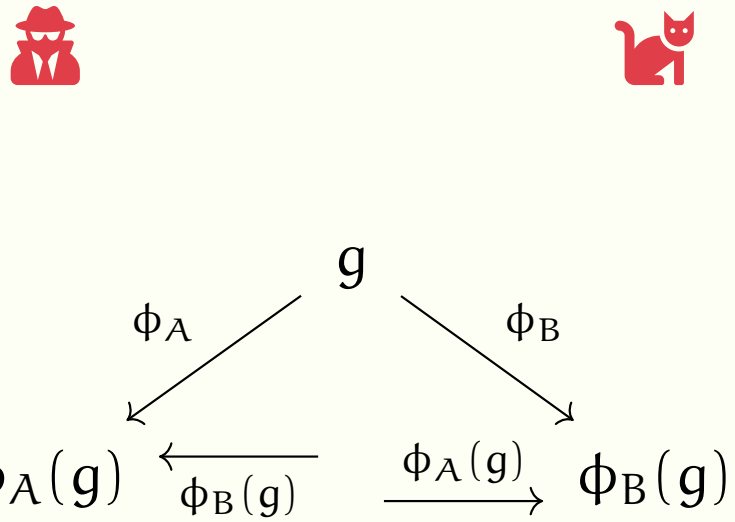
$$a' = a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(3x_Q^2 + a \right),$$

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

- Сложность вычисления E/G: $O(|G|)$.
- Если G – подгруппа большого порядка вычисление E/G является трудной задачей.
- Выход: брать $|G| = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$ для малых ℓ_i
- Оптимизации:
  - Castryck-Decru-Vercauteren, ”Radical isogenies”
  - Bernstein-De Feo-Leroux-Smith: $O(\sqrt{|G|})$, `velusqrt.isogeny.org`

1. “Стандартный” протокол DH в абстрактной группе

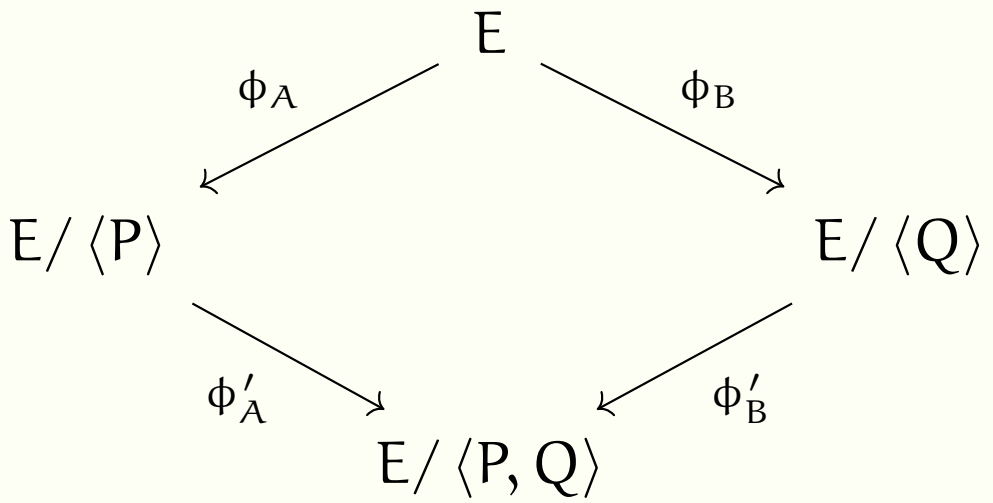
G – группа, $\langle g \rangle = G$, $\phi_A(x) = [A] \cdot x$ – гомоморфизм групп.



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

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

2. 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:
   $E/\langle P, Q\rangle = (E/\langle P\rangle)/\phi_A(Q) = (E/\langle Q\rangle)/\phi_B(P)$

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 Castryck-Decru

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

Данные статьи – предварительные версии статей и нечитаемы.

Выступление Castryck на ANTS XV:
`https://www.youtube.com/watch?v=_eNv7An3Qj0`

Восстановление ключа

Пусть $B = \langle [m_b] P_B + [n_B] Q_B \rangle$.

Задача восстановления ключа:

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

- Атака Decru-Castryck использует группу

$$\langle (P_A, \phi_B(P_A)), (Q_A, \phi_B(Q_A)) \rangle \subseteq E \times E/B$$

  и соответствующую этой группе фактор-изогению из $E \times E/B$ (используя аналогии формул Велу для размерности 2).
- В большинстве случаев фактор-изогения будет вести в якобиан кривой рода 2.
- В редких случаях – в произведение эллиптических кривых.
- Детектирование последнего редкого случая позволяет выявить правильное направление движения при поиске пути в графе изогений.

Детектирование разложимого случая

Тройка (ϕ, G_1, G_2) – “алмазная” изогенная конфигурация степени N, если:

1. $\phi : E \to E'$ – изогения
2. $G_1, G_2 \subseteq \ker \phi$
3. $\deg \phi = \#G_1 \cdot \#G_2$, $N = \#G_1 + \#G_2$, $G_1 \cap G_2 = \{0\}$

Теорема Кани (неформально). (N, N)-подгруппа $E \times E'$ разложимая $\iff$ она получена из некоторой “алмазной” изогенной конфигурации степени N.

Атака

Изогения $\phi_B : E \to E/B$ степени 3^{e_B} восстанавливается методом поиска алмазной конфигурации степени 2^{e_A}.

- строится изогения $\gamma : E \to C$ степени $2^{e_A} - 3^{e_B}$, т.ч. $(\phi_B \circ \widehat{\gamma}, \ker \widehat{\gamma}, \gamma(B))$ – алмазная конфигурация степени 2^{e_A}
- $P_C = \gamma(P_A), Q_C = \gamma(Q_A)$
- по теореме Кани подгруппа $\langle (P_C, \phi_B(P_A)), (Q_C, \phi_B(Q_A)) \rangle \subseteq C \times E/B$ – разложимая

Основная идея: Если бы точки $\phi_B(P_A)$ и $\phi_B(Q_A)$ не были бы образами точек относительно (какой-либо) изогении степени 3^{e_B}, то с большой вероятностью группа не была бы разложимой

Имеем $\phi_B = \phi_1 \circ \phi_2 \circ \ldots \circ \phi_{e_B}$, где ϕ_i изогении степени 3.

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

Будем восстанавливать изогению ϕ_B по шагам.

1. Выбираем изогению $\phi'_1 : E \to E'_1$
   (т.к. $\deg \phi'_1 = 3$, таких изогений немного)
2. Строим $\gamma : E'_1 \to C$ степени $2^{e_A} - 3^{e_B - 1}$
   (γ можно построить используя эндоморфизмы кривой малой степени)
3. $P'_1 = \phi'_1(P_A)$, $Q'_1 = \phi'_1(Q_A)$
4. $P_C = \gamma(P'_1)$, $Q_C = \gamma(Q'_1)$
5. Проверяем, что подгруппа

   $$(P_C, \phi_B(P_A)), (Q_C, \phi_B(Q_A)) \subseteq C \times E/B$$

   разложимая
6. Если разложимая, то $\phi_1 = \phi'_1$ и $E'_1 = E_1$

Схемы стойкие к атаке

Схемы не использующие точки кручения.

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

- issikebrokenyet.github.io

Литература

- W. Castryck и T. Decru.
  An efficient key recovery attack on SIDH. 2022.
- SIKE – Supersingular Isogeny Key Encapsulation. 2020.
  URL: https://sike.org/.

Контакты

snovoselov@kantiana.ru