

# Эллиптические кривые

## Лекция 10. Изогении

Семён Новосёлов

БФУ им. И. Канта

2023



# Мотивация

Постквантовая криптография на изогениях.

- схемы CSIDH, SIKE, weakSIDH, SeaSign
- в 2022 году появилась полиномиальная атака Кастрика-Декру на схему SIDH/SIKE, перевернувшая данную область
- многие схемы стали неактуальными
- однако базовые задачи остались трудными

# План

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

# 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  $\phi$  – эндоморфизм.

## Пример 1: Умножение на $m$

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

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

Задаётся многочленами деления.

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

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

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

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

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

## Пример 2: Эндоморфизм Фробениуса

$$\phi : E \rightarrow E,$$

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

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

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

(изогения не сепарбельная)

# 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  $\phi : E \rightarrow E'$  определённая над  $\mathbb{F}_q$  степени  $\#G$  т.ч.  $\ker \phi = G$ .
- 2 если  $\psi : E \rightarrow E''$  – 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  $E'$ ,  $\phi$ .

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

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

А изогенная кривая определяется как:

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

где

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

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

## 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  $\phi$  равна 5.

# Ядра изогений

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

## Группа-кручения

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

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

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

## Пример 4: Изогения с ядром над расширением

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

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

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

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

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

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

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

Сложность вычисления  $\phi$  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  $\implies$  вычисление  $E/G$  является трудной задачей.

Это делает невозможными вычисления с секретными изогениями "в лоб" в криптосистемах.

**Выход:** брать  $|G| = \ell_1^{e_1} \cdot \dots \cdot \ell_r^{e_r}$  для малых  $\ell_i$  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  $\ell$ .  
Вычислить изогению между ними.

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

Суперсингулярные кривые:

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

Обычные кривые:

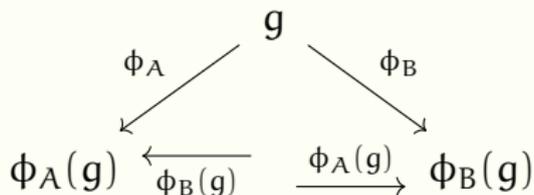
- квантовый субэкспоненциальный алгоритм

## 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

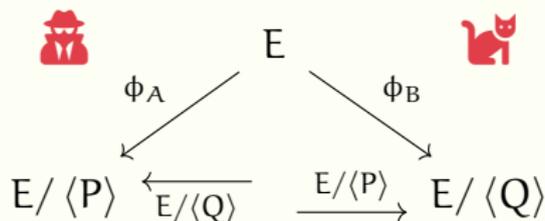
$G$  – группа,  $\langle g \rangle = G$ ,  $\phi_A(x) = [A] \cdot x$  – гомоморфизм групп.



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

- 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 отправляет  кривую  $E/\langle P \rangle$
- 3  выбирает своё секретное ядро  $\langle Q \rangle$ , строит изогению и отправляет  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  $\ell_A, \ell_B$  – 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  $\phi_A$  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  $\phi_B$  с ядром  $\langle [m_B]P_B + [n_B]Q_B \rangle$

## Выработка общего ключа:

- 1   $\implies$  :  $(E_A, \phi_A(P_B), \phi_A(Q_B))$
- 2   $\implies$  :  $(E_B, \phi_B(P_A), \phi_B(Q_A))$
- 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  $\implies$  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 Кастрыка-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](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:**

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

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

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

- в схемах на изогениях предполагается, что нельзя восстановить сначала  $\phi_1$ , затем  $\phi_2$  и т.д.
- всего существует  $\ell_B^2$  вариантов выбора  $\phi_i$  и перебор “в лоб” неэффективен.
- Кастрик и Декру предложили эффективный критерий для определения правильного варианта для  $\phi_i$ .

# Склейка эллиптических кривых

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

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

Может быть два случая:

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

# Атака

Рассмотрим процесс восстановления  $\phi_1$ .

$$\begin{array}{ccccccc} E & \xrightarrow{\phi_1} & E_1 & \xrightarrow{\phi_2} & E_2 & \xrightarrow{\phi_3} & E_3 \longrightarrow \dots \xrightarrow{\phi_{e_B}} E/G_B \\ & \searrow \phi_1^? & & & & & \\ & & C & \xleftarrow{\gamma} & E_1^? & & \end{array}$$

- 1 Выбрать  $\phi_1^? : E \rightarrow E_1^?$  – один из  $\ell_B^2$  вариантов для  $\phi_1$
- 2 Построить (любую) вспомогательную изогению  $\gamma : E_1^? \rightarrow C$  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  $\phi_1$ .

$$\begin{array}{ccccccc} E & \xrightarrow{\phi_1} & E_1 & \xrightarrow{\phi_2} & E_2 & \xrightarrow{\phi_3} & E_3 \longrightarrow \dots \xrightarrow{\phi_{e_V}} E/G_V \\ & \searrow \phi_1^? & & & & & \\ & & C & \xleftarrow{\gamma} & E_1^? & & \end{array}$$

## Откуда это взялось?

- Подгонка под условия теоремы Кани'97 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](https://github.com/issikebrokenyet)

# Литература

-  Castryck W., Decru T. An efficient key recovery attack on SIDH. 2022.
-  SIKE – Supersingular Isogeny Key Encapsulation. 2020.  
<https://sike.org/>
-  Выступление Castryck на ANTS XV:  
[https://www.youtube.com/watch?v=\\_eNv7An3Qj0](https://www.youtube.com/watch?v=_eNv7An3Qj0)

Контакты

snovoselov@kantiana.ru