Эллиптические кривые

Лекция 10. Изогении. Протокол обмена ключами

Семён Новосёлов
на основе курса Елены Киршановой

БФУ им. И. Канта

2020

IKBFU

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

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

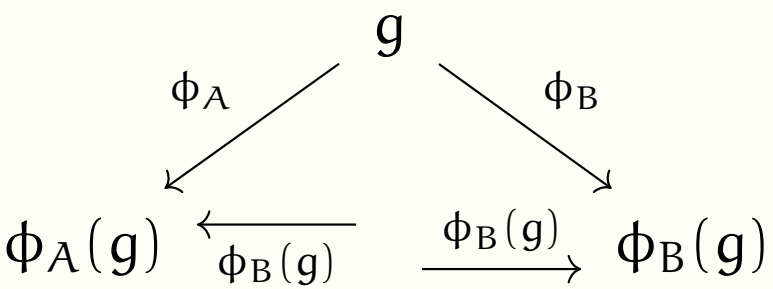
$$b' = b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} \left(5x_Q^3 + 3ax + 2b \right).$$

- Сложность вычисления E/G: $O(|G|)$.
- Если G – подгруппа большого порядка вычисление E/G является трудной задачей.

1. “Стандартный” протокол DH в абстрактной группе

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

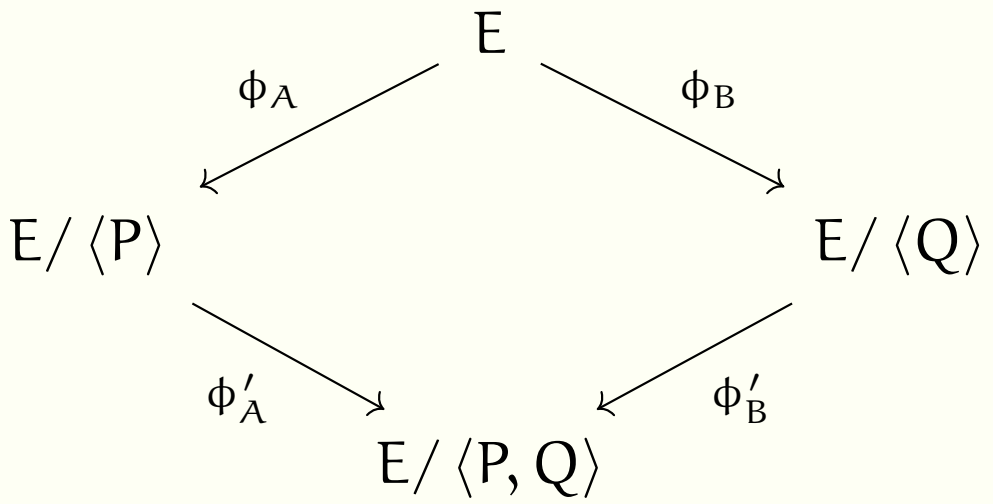
Alice **Bob**



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

- 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. Alice выбирает секретное ядро $\langle P\rangle$, строит изогению и отсылает Bob кривую $E/\langle P\rangle$
3. Bob выбирает своё секретное ядро $\langle Q\rangle$, строит изогению и отсылает Alice 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 $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$, где ℓ_A, ℓ_B – малые простые
2. E – суперсингулярная кривая над $\mathbb{F}_{p^2}$ т.ч. $\#E(\mathbb{F}_{p^2}) = (\ell_A^{e_A} \ell_B^{e_B} f)^2$
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:

1. **Alice:** $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, изогения ϕ_A с ядром $\langle [m_A]P_A + [n_A]Q_A \rangle$
2. **Bob:** $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, изогения ϕ_B с ядром $\langle [m_B]P_B + [n_B]Q_B \rangle$

Выработка общего ключа:

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

Замечания

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

Литература

- H. Cohen и др. *Handbook of elliptic and hyperelliptic curve cryptography*. 2005.
- C. Costello. *Supersingular Isogeny Key Exchange for Beginners*. 2019.
- S. D. Galbraith. *Mathematics of public key cryptography*. 2012.
- D. Jao и L. De Feo. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. 2011.
- *SIKE – Supersingular Isogeny Key Encapsulation*. 2020. URL: `https://sike.org/`.

Контакты

snovoselov@kantiana.ru