Лекция # 9

Изогении. Протокол обмена ключами, ~~основанный~~ SIKE.

I. Изогении

Опр-е E_1, E_2 – эллиптические кривые

Изогения $\varphi: E_1 \to E_2$ – морфизм, т.ч. $\varphi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$.

("морфизм", означает, что φ задаётся рац. ~~функциями~~ многочленами, т.е.

$$\varphi(x,y) = \left(\frac{f_1(x,y)}{f_2(x,y)}, \frac{g_1(x,y)}{g_2(x,y)} \right) \overset{\text{док-во в wash.}}{=\!=} \left(\frac{p(x)}{q(x)}, y \cdot r(x) \right)$$

изогения – гомоморфизм групп

Степень изогении – степень φ, т.е. $\deg \varphi = \max\{\deg p(x), \deg q(x)\}$.

Если $E_1 = E_2$, φ – эндоморфизм.

Примеры: 1. "умножение на m" – описывается многочленами деления

$$[m]: E \to E$$
$$P \mapsto m \cdot P$$

$E: y^2 = x^3 + x$ над $\mathbb{Q}$

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

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

$\#\ker [2] = 4 = \deg [2]$ ← совпадение не случайно (для сепарабельных изогений $\#\ker \varphi = \deg \varphi$)

2. Frobenius: $E_1: y_1^2 = x^3 + Ax + B$

$$E_2: y^2 = x^3 + A^p x_3 + B^p$$

$\varphi(x_1, y_1) = (x_1^p, y_1^p)$ – изогения н/д E_1, E_2

$$\varphi = \left(x^p, (x^3 + Ax + B)^{\frac{p-1}{2}} \right)$$

$\ker \varphi = \mathcal{O}_E$, $\deg \varphi = p$ (несепарабельная изогения)

Факт 1 (теорема Тэйта об изогениях)

E_1, E_2 изогенны над $\mathbb{F}_q$ $\iff$ $\#E_1(\mathbb{F}_q) = \#E(\mathbb{F}_q)$

(т.е. рац. мн-ны определены над $\mathbb{F}_q$)

т.е. $\exists$ эффективный метод определения изогенных эл кривых

ФАКТ 2 (Vélu)

(Док-во Galbraith и. Mathematics of Public Key Cryptography", Chap. 25)

∃ E – эллиптическая кривая над $\mathbb{F}_q$

G – конечная подгруппа $E(\overline{\mathbb{F}_q})$

Тогда ∃ эллиптическая кривая E' над $\mathbb{F}_q$ и сепарабельная изогения $\varphi: E \to E'$, определённая над $\mathbb{F}_q$, степени $\#G$, т.ч. $\boxed{\ker \varphi = G}$

Кроме того, если $\psi: E \to E''$ – другая сепарабельная изогения степени $\#G$, с $\ker \psi = G$, то $j(E') = j(E'')$ (т.е. E', E'' – изоморфны).

⇒ образ E корректно определён до изоморфизма.

Обозначение: $E' \cong E/G$ (!) E/G – НЕ фактор-группа, это кривая, отличная от (но изогенная) E

Vélu описал явные ф-лы для E', φ

ФАКТ 3 (Док-во в L. De Feo "Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies")

∃ $E: y^2 = x^3 + ax + b$ – эллиптическая кривая над полем K,

$G \subset E(K)$ – конечная подгруппа;

сепарабельная изогения $\varphi: E \to E'$ с ядром G может быть записана

$$\varphi(P) = \left[\overbrace{x(P)}^{x\text{-коорд. точки } P} + \sum_{Q \in G \setminus \{O\}} \left(x(P+Q) - x(Q) \right), \right.$$

$$\left. \overbrace{y(P)}^{y\text{-коор. точки } P} + \sum_{Q \in G \setminus \{O\}} \left(y(P+Q) - y(Q) \right), \right.$$

А изогениая кривая E/G задаётся ур-ием $y^2 = x^3 + a'x + b'$, где

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

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

Сложность вычисления E/G: $O(|G|)$.

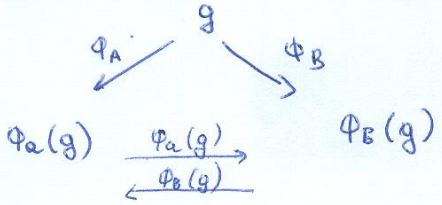
Если G – подгруппа большого порядка, вычисление E/G является трудной задачей.

II SIDH – Supersingular Isogeny Diffie-Hellman

1. "Стандартный" протокол обмена ключами DH в абстрактной группе G:

G - группа, $\langle g \rangle = G$

$\varphi_A(X) = [a] \cdot X$ - групповой гомоморфизм

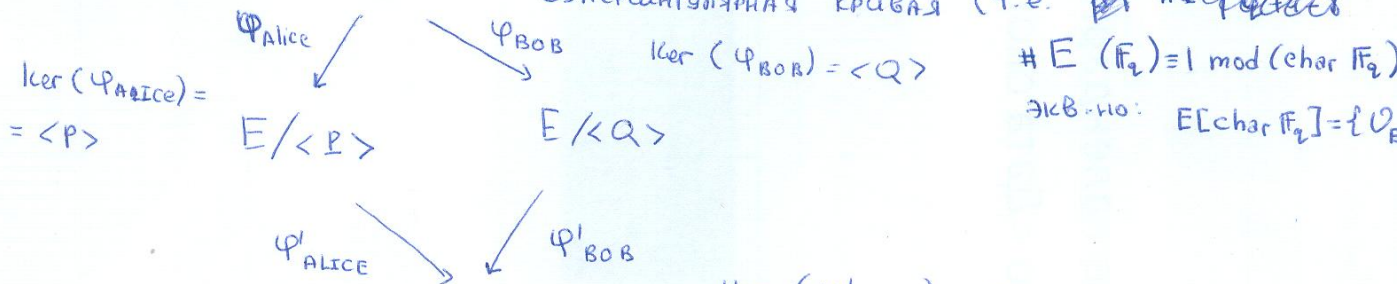


$$\varphi_a(\varphi_b(g)) = \varphi_b(\varphi_a(g)) = [ab] \cdot g$$

2. В качестве группового ~~закона~~ гомоморфизма можно взять изогении

$\Rightarrow$ Протокол SIKE (De Feo & Jao 2011)

E ← эллиптическая кривая (пар-р системы)
суперсингулярная кривая (т.е. ~~$\#E(\mathbb{F}_q) = q+1$~~)



$\#E(\mathbb{F}_q) \equiv 1 \bmod (\mathrm{char}\ \mathbb{F}_q)$

эквивалентно: $E[\mathrm{char}\ \mathbb{F}_q] = \{\mathcal{O}_E\}$

$\ker(\varphi'_{ALICE}) = \langle \varphi_{Bob}(P) \rangle$

$\ker(\varphi'_{BOB}) = \langle \varphi_{Alice}(Q) \rangle$

ДЕТАЛЬНЕЕ: $E[\ell_A] \simeq (\mathbb{Z}/\ell_A\mathbb{Z}) \otimes (\mathbb{Z}/\ell_A\mathbb{Z})$ - группа точек ℓ_A-кручения

~~(E, выберем~~ S_A, R_A $E[\ell_B] \simeq (\mathbb{Z}/\ell_B) \otimes (\mathbb{Z}/\ell_B\mathbb{Z})$ — — // — — ℓ_B-кручения

~~Alice~~ ~~Bob~~

$E[\ell_A] = \langle R_A, S_A \rangle$ - образующие

$E[\ell_B] = \langle R_B, S_B \rangle$

(!) В лабораторной #8 даны подгруппы $E[\ell_A]$, $E[\ell_B]$ с одной образующей

Alice (E, R_A, S_A, R_B, S_B) **Bob**

1. $a \xleftarrow{R} [0, \ell_A]$

$T_a = R_A + a S_A \in E[\ell_A]$

$\varphi_A: E \to E/\langle T_a \rangle$ (по ф-ле Вёлу)

$\varphi_A(R_B), \varphi_A(S_B), E/\langle T_a \rangle$

$\varphi_B(R_A), \varphi_B(S_A), E/\langle T_b \rangle$

2. $T'_a = \varphi_B(R_a) + a \cdot \varphi_B(S_A)$

$= \varphi_B(R_a + a \cdot S_A) = \varphi_B(T_a)$

1. $b \xleftarrow{R} (0, \ell_B)$

$T_b = R_b + b \cdot S_B \in E[\ell_B]$

$\varphi_B: E \to E/\langle T_b \rangle$

2. $T'_b = \varphi_A(R_B) + b \cdot \varphi_B(S_B)$

$= \varphi_A(R_B + b S_B) = \varphi_A(T_b)$

Alice

3. $T_a' = \varphi_B(R_A) + a \cdot \varphi_B(S_A)$

$= \varphi_B(R_A + a \cdot S_A) = \varphi_B(T_a)$

$\varphi_a' : E/\langle T_b \rangle \to (E/\langle T_b \rangle)/\langle T_a' \rangle := E_{A,B}$

имеем одну кривой +
строим группу, порождённую T_a'
$\Rightarrow$ ф-лы Vélu.

Bob

3. $T_b' = \varphi_A(R_B) + b \circ \varphi_A(S_b)$

$= \varphi_A(R_B + b S_B) = \varphi_A(T_b)$

$\varphi_b' : E/\langle T_a \rangle \to E/\langle T_a \rangle/\langle T_b' \rangle := E_{A,B}$

$$E_{A,B} := \underbrace{\varphi_a' \circ \varphi_B(E)}_{\text{Alice}} = \underbrace{\varphi_b' \circ \varphi_a(E)}_{\text{Bob}} = E/\langle T_a, T_b \rangle$$

Ур-ия кривых, полученные (A) и (B) могут быть не идентичными, т.е. обязательно изоморфными $\Leftrightarrow$ j-инвариант одинаков

$\Rightarrow j(E_{A,B})$ – общий секретный ключ.