

Эллиптические кривые

Лекция 13. Криптоанализ схем на изогениях

Семён Новосёлов

БФУ им. И. Канта

2025



Граф изогений

Граф с вершинами – j -инвариантами эллиптических кривых и рёбрами – изогениями.

Обозначение: $X(K, \ell)$, где K – поле, ℓ – степень изогении.

Задача поиска изогении

Общая задача нахождения изогении

Даны две изогенные кривые E_1 и E_2 .
Вычислить изогению между ними.

Теорема Тейта: $E_1 \sim E_2 \iff \#E_1 = \#E_2$

$\implies$ легко проверить существование изогении.

Методы поиска изогений

- на основе парадокса дней рождений
- сведение задачи к вычислению $\text{End}(E)$

Методы на основе парадокса дней рождений

- модификация алгоритмов BSGS/Полларда/vOW
- исп. случайные блуждания в графе изогений

Сложность для суперсингулярных кривых:

- $\tilde{O}(p^{1/2})$ по времени/памяти в худшем случае или
- $\tilde{O}(p^{3/4})$ по времени в среднем для алгоритма с малой памятью (vOW)

Число изогенных суперсингулярных кривых $\approx \frac{p}{12}$.

Как задавать случайные блуждания?

- через ядра изогений – подгруппы $E[\ell]$
- через модулярные многочлены

Модулярный многочлен – это многочлен $\Phi_\ell \in \mathbb{Z}[X, Y]$ т.ч.
 $\Phi_\ell(j(E_1), j(E_2)) = 0 \iff \exists$ изогения степени ℓ между E_1 и E_2 .

$\implies$ находясь в вершине $j(E)$, находим корни $\Phi_\ell(j(E), Y)$ и берём случайный.

Суперсингулярная задача поиска изогении

Эллиптическая кривая $E/\mathbb{F}_q$, $q = p^n$ – **суперсингулярная**, если $p \mid t = \#E(\mathbb{F}_q) - q - 1$.

Факт: $j(E) \in \mathbb{F}_{p^2}$ [Silverman, Th. 3.1.(a).iii]

$\implies$ суперсингулярный граф изогений определён над $\mathbb{F}_{p^2}$

Также над $\mathbb{F}_{p^2}$ он связан для любой степени изогении ℓ .

Алгоритм Delfs-Galbraith

Пусть E_1, E_2 определены над $\mathbb{F}_{p^2}$.

Идея:

- найти изогении $\phi_1 : E_1 \rightarrow E'_1/\mathbb{F}_p$ и $\phi_2 : E_2 \rightarrow E'_2/\mathbb{F}_p$,
- найти изогению $\phi' : E'_1 \rightarrow E'_2$ в графе изогений над $\mathbb{F}_p$
- вернуть $\phi : E_1 \rightarrow E_2$ как $\phi = \hat{\phi}_2 \circ \phi' \circ \phi_1$

Граф изогений $X(\mathbb{F}_p, \ell)$ меньше, чем $X(\mathbb{F}_{p^2}, \ell)$ – состоит из $\tilde{O}(\sqrt{p})$ вершин, но он не связный и надо брать несколько ℓ .
 $\Rightarrow$ сложность поиска ϕ' равна $\tilde{O}(p^{\frac{1}{4}})$

Общая **сложность** алгоритма Delfs-Galbraith: $\tilde{O}(p^{1/2})$,
доминирующие шаги – нахождение ϕ_1, ϕ_2 .

Сведение задачи к вычислению $\text{End}(E)$

- Задачи поиска изогении и вычисления $\text{End}(E)$ эквивалентны [Wesolowski'21] (одна за полиномиальное время сводится к другой).
- Один эндоморфизм $\implies$ всё кольцо за полиномиальное время [Page-Wesolowski'23]
- Детектирование эндоморфизмов малых степеней возможно с помощью нахождения классового многочлена Гильберта
 $\implies$ алгоритм нахождения изогений [Love-Boneh'19]

Квантовые атаки – сложность

- суперсингулярные кривые: $\tilde{O}(p^{1/2}) \Rightarrow \tilde{O}(p^{1/4})$
- обычных кривые: $L(1/2)$

Литература

-  Silverman J.H. "The Arithmetic of Elliptic Curves", 2ed (2009)
-  Delfs C., Galbraith S.D. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$ ". 2016. DCC. <https://arxiv.org/pdf/1310.7789>
-  Wesolowski B. "The supersingular isogeny path and endomorphism ring problems are equivalent" (2021)
<https://ieeexplore.ieee.org/document/9719728>
-  Page A., Wesolowski B. "The supersingular Endomorphism Ring and One Endomorphism problems are equivalent" (2023)
<https://eprint.iacr.org/2023/1399>
-  Love J., Boneh D. - Supersingular Curves With Small Non-integer Endomorphisms (2019) <https://arxiv.org/pdf/1910.03180>

Контакты

snovoselov@kantiana.ru