Форзиция: протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых

С. Гребнев [1], П. Ключарёв [2], А. Коренева [3],
Д. Кошелев [4], О. Тараскин [5], А. Тулебаев[3]

[1]QApp [2]МГТУ им. Н.Э. Баумана [3]Код безопасности [4]ИнфоТеКС
[5]Waves

RusCrypto’2021, Москва

Изогении

Isogeny-based cryptography

The youngest class of post-quantum cryptography methods; initiated in the early 2000s. An isogeny is a function that maps points of an elliptic curve to points of another elliptic curve and that satisfies specific mathematical properties. You can then draw a graph whose nodes are elliptic curves and whose edges are isogenies between them, and walk through this graph in a pseudorandom way. After throwing a lot of cool math at the study of these objects—graph theory, quaternion algebras, and so on—you end up with hard computational problems that you can use for crypto applications.

J.-P. Aumasson, Crypto Dictionary (2021)

Изогении

Изогения — это рациональное отображение между двумя эллиптическими кривыми, являющееся гомоморфизмом. Если существует такого рода отображение между двумя кривыми, то они называются **изогенными**.

Theorem 1.

(Serre-Tate) Две кривые изогенны над конечным полем K iff они имеют одинаковое кол-во точек.

Сложность вычисления изогении степени l (т.е. с ядром мощностью l) есть $O(l)$ операций в поле $GF(p^2)$ (при помощи **формул Велю**).
При этом для вычисления изогении гладкой степени можно воспользоваться ее декомпозицией на изогении малых степеней.

Суперсингулярные кривые

Эллиптическая кривая, определенная над K с характеристикой p – **суперсингулярна**, если #E $\equiv 1 \pmod{p}$.

Theorem 2.

(Deuring) E суперсингулярна, тогда

1. E изоморфна кривой, определенной над GF(p^2)
2. каждый эндоморфизм E определен над GF(p^2)

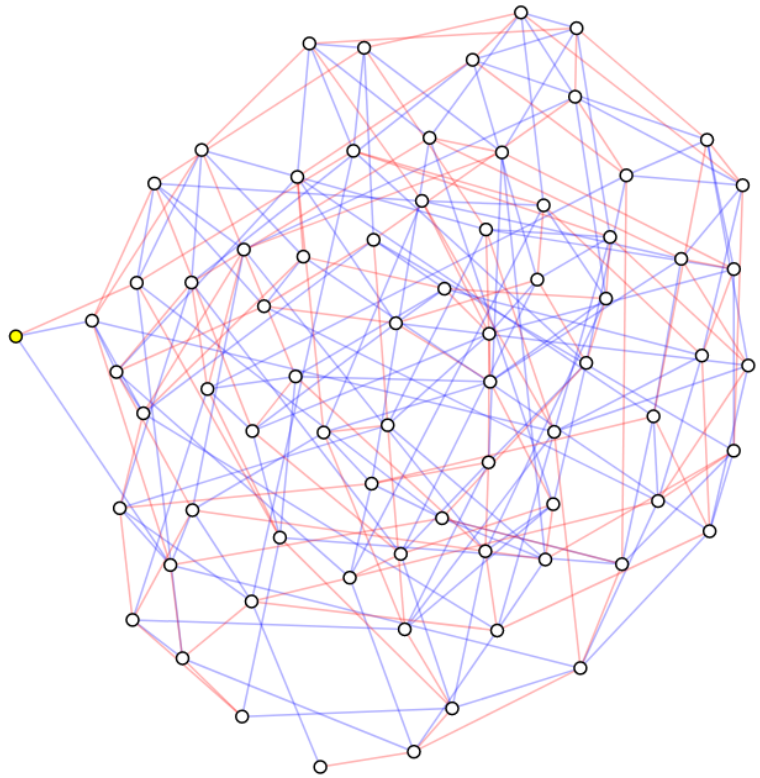
Суперсингулярные кривые

Графом изогений называется граф, множеством вершин которого является множество классов изоморфизма эллиптических кривых. Две различных вершины этого графа соединены ребром тогда и только тогда, когда представители соответствующих классов изоморфизма изогенны. Если ограничиться только изогениями степени l, то получим **граф l-изогений**. Граф изогений простой степени $l \neq p$ для суперсингулярных эллиптических кривых:

- $(l+1)$-регулярный
- содержит единственный связный компонент, состоящий из всех суперсингулярных кривых.
- **экспандер** (конечный ненаправленный мультиграф, в котором любое подмножество вершин, не являясь «слишком большим», имеет «сильную» связность).

Граф изогений

Пример: $p = 2^5 \cdot 3^3 - 1 = 863$;
73 суперсингулярных j-инварианта.
2-изогении, 3-изогении, $E_0 : y^2 = x^3 + x$.



(c) `https://isogenies.enricflorit.com/visualizations/graph.html`

Протокол SIDH

Возьмем простое число p вида $p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$, где l_A, l_B – маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$, поле $GF(p^2)$. Построим суперсингулярную кривую $E(GF(p^2))$, мощность группы точек кривой которой равна $(l_A^{e_A} l_B^{e_B})^2$. По построению $E[l_A^{e_A}]$ содержит $l_A^{e_A - 1}(l_A + 1)$ циклических подгрупп порядка $l_A^{e_A}$, каждая из которых определяет собственную изогению (т.е. ядром которой она является), аналогичное замечание верно и для $E[l_B^{e_B}]$.

Протокол SIDH

В основе протокола лежит следующая коммутативная диаграмма:

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E/\langle P\rangle \\ {\scriptstyle\psi}\downarrow & & \downarrow \\ E/\langle Q\rangle & \longrightarrow & E/\langle P,Q\rangle \end{array} \tag{1}$$

где φ, ψ – случайные пути в графах изогений степеней $l_A^{e_A}$, $l_B^{e_B}$ соответственно. Стойкость протокола основана на сложности нахождения пути, соединяющего две вершины в графе.

Протокол SIDH

Вариант схемы Диффи-Хеллмана, реализованный над диаграммой (1). Идея его состоит в том, чтобы абонент A выбирал φ, а B выбрал ψ.
Фиксируем открытые параметры протокола:
$p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$, где l_A, l_B – маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$, суперсингулярную эллиптическую кривую $E_0(GF(p^2))$ и базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$, которые порождают, соответственно, $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$, т.е. $\langle P_A, Q_A\rangle = E_0[l_A^{e_A}]$ и $\langle P_B, Q_B\rangle = E_0[l_B^{e_B}]$.
Абонент A выбирает случайный элемент $n_A \in_R \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ и строит изогению $\varphi_A : E_0 \to E_A$ с ядром $K_A := \langle P_A + [n_A]Q_A\rangle$. Абонент A также вычисляет образ $\{\varphi_A(P_B), \varphi_A(Q_B)\}$ и посылает эти точки абоненту B вместе с эллиптической кривой E_A (т.е. ее описанием).

Протокол SIDH

Аналогично, абонент B выбирает случайный элемент $n_B \in_R \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ и строит изогению $\varphi_B : E_0 \to E_B$ с ядром $K_B := \langle P_B + [n_B]Q_B \rangle$. Абонент B также вычисляет образ $\{\varphi_B(P_A), \varphi_B(Q_A)\}$ и посылает эти точки абоненту A. Получив от абонента B набор $E_B, \varphi_B(P_A), \varphi_B(Q_A)$, абонент A строит изогению $\varphi'_A : E_B \to E_{AB}$ с ядром $\langle \varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$; абонент B выполняет аналогичные действия.
В качестве общего ключа используется j-инвариант кривой

$$E_{AB} = \varphi'_B(\varphi_A(E_0)) = \varphi'_A(\varphi_B(E_0)) = E_0/\langle P_A + [n_A]Q_A, P_B + [n_B]Q_B \rangle .$$

Анализ: классический вычислитель

Тотальное опробование: $(l+1)l^{e-1}$ циклических подгрупп порядка $l^e \Rightarrow O(l^e)$ или $O(p^{1/2})$ опробований.
Встреча посередине: память – $O(p^{1/4})$, время – $O(p^{1/4})$. (Adj et al., eprint 2018/313)

Параллельный метод поиска коллизий: $O\left(\frac{p^{3/8}}{m\ w^{1/2}}t\right)$

(m – кол-во процессоров, w – объем памяти, t – трудоемкость итерационной ф-ции)
Вывод: параллельный метод поиска коллизий — наилучший (Costello et al., eprint 2019/298)

Анализ: квантовый вычислитель

Алгоритм поиска зацеплений (claw) (Tani): пусть $g_1 : X_1 \to Y$, $g_2 : X_2 \to Y$, найти такие x_1, x_2: $g_1(x_1) = g_2(x_2)$.
Пусть $\#X_1 \approx \#X_2 \approx N$, $\#Y \gg N$, тогда время работы – $O(N^{2/3})$.
У нас время – $O(p^{1/6})$ (и память $O(p^{1/6})$).
Метод Гровера: время – $O(p^{1/4})$, память – $O(1)$.
(Jacques et Schanck, eprint 2019/103)
Quantum golden collision search: $O(p^{3/14})$ гейтов и $O(p^{1/14})$ памяти
(Jacques et Schrottenloher, SAC 2020)

Форзиция: общая характеристика

- Схема – типа SIDH
- Только эфемерные ключи
- Три уровня стойкости – 80, 128 и 256 битов
- Стартовая кривая E_{19}
- Представление кривых в форме Монтгомери
- Отказ от компрессии открытых ключей в пользу быстродействия

Форзи́ция (лат. Forsythia) — род кустарников и небольших деревьев семейства Маслиновые.

Уровни стойкости

Три уровня стойкости – 80, 128 и 256 битов – определяются характеристикой базового поля.

Число	Формула	Классическая стойкость	Квантовая стойкость
p_{271}	$2^{132} \cdot 3^{85} \cdot 11 - 1$	82	122 (131)
p_{415}	$2^{208} \cdot 3^{129} \cdot 5 - 1$	135	183 (203)
p_{754}	$2^{372} \cdot 3^{239} \cdot 7 - 1$	262	329 (372)

Размер открытого ключа – $6\lceil \log_2(p) \rceil$.

Расчет уровней стойкости

Квантовый вычислитель

Опробование ключа блочного шифра (“Кузнечик”) – $\approx 2^{20}$ квантовых гейтов (Денисенко и др., 2019).
Нижняя оценка на реализацию одного опробования задачи CSSI в $\approx 2^{22}$ квантовых гейтов (Jacques, Schanck, 2019).
Таким образом, p выбираем так, что эквивалентная длина блочного шифра $n_Q(p) \approx p/2 + 4$.

Расчет уровней стойкости

Классический вычислитель

Одно опробование ключа блочного шифра за $t_1 = 2^{10}$ операций (NIST 2016).
Одно вычисление итерационной функции параллельного метода поиска коллизий – t_2 операций, эквивалентная длина блочного шифра составит $n_C(P) = 3/8 \log_2 p + \log_2 t_2 - \log_2 t_1 - 1/2 \log_2 w$.
Таким образом, для обеспечения стойкости, эквивалентной стойкости n-битового блочного шифра, необходимо взять p такое, что $\min\{n_C(P), n_Q(p)\} \geq n$.
(считаем $t_2 \approx 2^{22}$, $w \approx 2^{49}$ – суперкомпьютер FUGAKU).

Стартовая кривая

В SIKE: кривая $y^2 = x^3 + x$ с j-инвариантом 1728 (I этап) или 2-изогенная ей кривая (II этап).
Мы предлагаем использовать кривую

$$E_{19} : y^2 = x^3 - 2^3 19x + 2 \cdot 19^2$$

с j-инвариантом $-2^{15}3^3$.
E_{19} не обладает эндоморфизмами степени 2 и 3, то есть петлями в графах 2 и 3-изогений. Также у нее отсутствуют кратные дуги в графах 2 и 3-изогений.
Для суперсингулярности кривой E_{19} необходимо и достаточно, чтобы $\left(\frac{-19}{p}\right) = -1$.

Реализация

Подготовлены прототипы программной реализации.

Python

`https://github.com/s-v-grebnev/Forsythia/`
Производительность (Intel Core i5@1.8GHz): **0.24-0.26 с** на одной стороне для p_{271}; **0.8 с** на одной стороне для p_{415}.

SAGE + Cython

Производительность (Intel Core i5@1.8GHz): **0.013 с** на одной стороне для p_{271}, **0.02 с** на одной стороне для p_{415}.

Основные результаты работы на данном этапе:

- предложен постквантовый протокол выработки общего ключа двумя абонентами на основе протокола SIDH;
- выбраны параметры протокола, в том числе характеристики поля, стартовая кривая;
- разработан прототип программной реализации.

Основные задачи для дальнейшей работы:

- подготовка описания протокола в формате методических рекомендаций;
- разработка оптимизированной программной реализации.

Спасибо за внимание.

sg@qapp.tech