ДОСЛІДЖЕННЯ СТРУКТУРИ ГРАФА ІЗОГЕНІЙ ЕЛІПТИЧНОЇ КРИВОЇ ЕДВАРДСА

Абрамов С.В.

Київський столичний університет імені Бориса Грінченка,
кафедра комп'ютерних наук,
Україна.

E-mail: s.abramov.asp@kubg.edu.ua

Abstract

After the appearance of reports about the appearance of quantum computers in the near future, which easily break some codes, post-quantum cryptography (PQC) arose, studying quantum-resistant cryptographic algorithms. The most promising areas of PQC is the use of the CSIDH (Commutative Supersingular isogeny Diffie-Hellman key exchange) algorithm, on the isogenies of Edwards elliptic curves. The properties of the graph of isogenies of Edwards elliptic curves significantly determine the properties of the cryptographic algorithm.

Після повідомлень про появу незабаром квантових комп'ютерів, які легко зламують деякі шифри, виникла постквантова криптографія (PQC), що вивчає квантово-стійкі криптографічні алгоритми. Найбільш перспективним напрямом PQC є використання алгоритму CSIDH (Commutative Supersingular isogeny Diffie-Hellman key exchange), який спочатку був створений на ізогенії еліптичних кривих Монтгомері [1]. Їхня стійкість заснована на блуканні в ізогенному графі та труднощі знаходження шляху у графі ізогеній еліптичних кривих. Криптографічні алгоритми даного сімейства відрізняються відносно невисокою швидкодією, але водночас пропонують найкоротші відкриті ключі та шифротексти.

Криптосистема дозволяє двом учасникам, які не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку при цьому ефективно протистояти криптоаналітичній атаці противника, який володіє квантовим комп'ютером.

Пізніше було запропоновано замінити криву Монтгомері на криву Едвардса [2], яка забезпечує більшу швидкодію алгоритму. У загальній формі крива Едвардса має вигляд і визначається параметрами *a, d :*

$$E_{a,d}: \quad x^2 + ay^2 = 1 + dx^2y^2, \quad \text{параметри } a, d \in F_p^*,\ a \neq d,\quad d \neq 1.$$

Ізогенні криві Едвардса мають такий самий вигляд і відрізняються лише параметрами, які однозначно ідентифікують криву. Для кривої з параметрами *a, d* обчислення параметрів *a', d'* ізогенної кривої ступеню l здійснюється згідно формули [3]:

$$a' = a^l; \quad d' = A^8 d^l, \text{ где } A = \prod_{i=1}^{s} \alpha_i. \tag{1}$$

При цьому параметр *a* зазвичай дорівнює 1, тому, що його зміна дає ізоморфну криву. Величини α_i це координати ядра ізогенії.

Розглянемо граф ізогеній у якого у вершинах розташовуються параметри d ізогенних кривих a ребра це ізогенні відображення кривих з параметрами згідно (1). Властивості алгоритму CSIDH суттєво залежать від типу кривих, структури та розміру графа ізогеній. Тому при створенні систем шифрування за алгоритмами CSIDH на кривій Едвардса, важливо знати властивості графа ізогеній цих кривих.

Розглянемо простий приклад графа ізогеній еліптичних кривих порядку $\#N_E$. Обмежимося ізогеніями ступенів $\{l_k\} = \{3,5,7\}$, при цьому модуль поля над яким визначена крива дорівнює p= 8 * 3 * 5 * 7 – 1 = 839. Над полем можуть існувати еліптичні криві з порядком $\#E = p + 1 - t$; де $t -$ слід рівняння ендоморфізма Фробеніуса ($|t| \leq 2\sqrt{p}$). Якщо t<0 отримуємо криву класу квадратичного кручення E^t, її порядок $\#E^t = p + 1 + t$.

Порядки кривих різних класів E і E^t симетричні відносно середнього значення $p + 1$. Для суперсингулярной кривой $t = 0$ порядки обох класів кривих дорівнюють $p + 1$, а множина ступенів ізогеній однакова. У разі несуперсингулярних кривих порядки кривих різних класів відрізняються на 2t, тоді є множина ступенів ізогеній на кривих двох класів, пов'язаних як пари квадратичного кручення з різними порядками. Перехід між класами дуже простий і швидкий, що пояснюється тим, що параметри цих класів адитивно зворотні: $(a, d) \leftrightarrow (-a, -d)$.

У таблиці 1 показані результати дослідження кількості кривих C_E порядку #E з модулем 839. У таблиці вказані параметри кривих d, при a=1.

Таблиця 1.

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
#E	784	792	800	808	816	824	832	**840**	848	856	864	872	880	888	896
C_E	8	26	30	16	48	30	18	**66**	18	30	48	16	30	26	8

У таблиці є 66 суперсингулярних кривих порядку 840 у котрих слід Фробеніуса t=0. Ці криві утворюють два сегменти по 33 кривих 840 порядку (всього 66 кривих), які складають два замкнутих циклу ланцюжків ізогеній 3 ступеня. Криві обох сегментів є парами квадратичного кручення і пов’язані через інверсію $d=d^{-1}$, яка здійснюється досить складними обчислюваннями. Ізогенні переходи між кривими першого сегменту відповідають позитивному напрямку групової операції алгоритму CSIDH, а криві другого сегменту – зворотному негативному напрямку. Перехід від позитивного напрямку до негативного і назад здійснюється через інверсію.

Шлях по графу між двома вершинами складається з окремих ізогенних переходів (кроків) по ізогеніях різного порядку. Внаслідок комутативності кроки можна виконувати у різній послідовності. Це можна використовувати для надання вигляду випадковості для підвищення захисту від криптоаналітиків. Крім того, криві кожного сегменту також складають по 3 цикли ізогеній 5, 7 порядку по 11 ізогеній у кожному циклі. Ланцюжки 5, 7 ізогеній не пов'язані між собою, а тільки через ланцюг 3 ізогеній. Це не обмежує шляхи за графом, але шлях ізогеніями 5,7 порядку залежить від попереднього шляху і підвищує його випадковість.

Крім суперсингулярних кривих у таблиці є пари квадратичного кручення несуперсингулярних кривих, які також використовують у криптоалгоритмах. Наприклад, криві порядку p+1=840, t=+24, тоді маємо пару циклів з 96 кривих $\#E^t$=864, #E=816. Кількість кривих збільшується, але не всі криві можна використовувати для шифрування, це треба перевіряти.

Вивчення простого графа ізогеній допомагає побачити закономірності для подальшого глибшого їх вивчення.

Література

1. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).

2. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с.

3. Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. Computing of odd degree isogenies on supersingular twisted Edwards curves. CEUR Workshop Proceedings , 2021, 2923, pp. 1–11. (2021)