УДК 004.056

Обзор алгоритмов поиска изогений между эллиптическими кривыми
Скибина А.О. (ГУАП), Малеев Л.Б. (ГУАП)

Научный руководитель – кандидат технических наук, доцент Давыдов В.В.
(ГУАП)

Введение. Криптографические алгоритмы применяются в самых разных сферах – от защиты персональных данных до обеспечения безопасных финансовых транзакций. Однако большинство из них не будут устойчивы к атакам с появлением квантового компьютера [1]. Одним из вариантов замены таким алгоритмам являются постквантовые протоколы, построенные на изогениях суперсингулярных эллиптических кривых. Например, на изогениях построена подпись SQISign [2] – участник конкурса дополнительных электронных подписей Национального Института Стандартов и Технологий (NIST).

На данный момент алгоритмы для поиска изогений плохо систематизированы в литературе. Основными задачами данной работы являются обзор, структурирование и анализ существующих алгоритмов, поиск эффективного применения.

Основная часть. Изогении являются гомоморфизмами между эллиптическими кривыми: отображают точки одной эллиптической кривой в точки другой, сохраняя групповую операцию сложения точек.

В данной работе рассматриваются алгоритмы поиска изогений Vélu, Kohel, Galbraith и $\sqrt{elu}$, оценивается их сложность. Алгоритм Vélu [3] – первый алгоритм для поиска изогений, предложенный в 1971 году. Вычисление отображения основано на известном ядре изогении. Алгоритм Kohel [4] вычисляет изогению на основе многочлена ядра, что ускоряет задачи, связанные с подсчётом точек. На основе диссертационной работы (автор – David Kohel) Galbraith предложил алгоритм [5], который использует модулярные полиномы и цепочки изогений. Алгоритм $\sqrt{elu}$ [6] – улучшенная версия классического Vélu. Основная идея заключается в том, чтобы использовать алгоритм больших и маленьких шагов. Он реиндексирует точки ядра аддитивной группы G , порождённой точкой P на эллиптической кривой с порядком N , для более быстрых вычислений эллиптических полиномов, за время пропорциональное квадратному корню. Такой подход позволяет уменьшить количество вычислений. Изучена практическая применимость каждого алгоритма.

Вывод. Проанализированы четыре алгоритма поиска изогений между эллиптическими кривыми, сделаны выводы о преимуществах и недостатках каждого алгоритма. Определены возможности применения каждого алгоритма. Дана оценка асимптотической сложности.

Список использованных источников.

1. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM review, vol. 41, no. 2, pp. 303–332, 1999.
2. De Feo L. et al. SQISign: compact post-quantum signatures from quaternions and isogenies // Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26. – Springer International Publishing, 2020. – С. 64–93.
3. J. Vélu, Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, S´erie A., 273, pp. 238–241 (1971).
4. D. Kohel, Endomorphism rings of elliptic curves over finite fields, PhD thesis, University of California Berkeley, (1996).
5. Galbraith S. D. Constructing isogenies between elliptic curves over finite fields. — London Math. Soc. J. Comput. Math., 1999, v. 2, p. 118–138.

6. Square-root Vélu algorithm for elliptic-curve isogenies // Sagemath URL: https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/hom_velusqrt.html