УДК 51-74

О ПОСТРОЕНИИ ГРАФОВ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД КОНЕЧНЫМИ ПОЛЯМИ РАЗЛИЧНЫХ ХАРАКТЕРИСТИК

Ковалева С. А. (Университет ИТМО), **Мезенев К.О.** (Университет ИТМО), **Давыдов В. В.** (Университет ИТМО)

Научный руководитель – преподаватель Давыдов В. В.
(Университет ИТМО)

Введение. Криптография играет решающую роль в обеспечении безопасности связи и обмена информацией в современном цифровом мире. Эллиптические кривые на сегодняшний день широко используются для создания безопасных криптографических ключей. Одним из современных направлений является криптография, основанная на изогениях между эллиптическими кривыми. В работе рассматриваются графы изогений между кривыми над различными полями и изучаются их свойства.

Основная часть. Криптография на изогениях между эллиптическими кривыми – относительно молодая область постквантовой криптографии, в которой стойкость алгоритмов и протоколов основана на поиске пути в больших графах. В основной части работы строятся и изучаются графы изогений между эллиптическими кривыми над различными полями. Рассматриваются графы изогений для суперсингулярных и несуперсингулярных эллиптических кривых, описываются их свойства, делаются выводы о применимости выбранных кривых для различных целей в криптографии, обосновывается выбор конечных полей [1].

Выводы. В ходе работы был проанализирован выбор эллиптических кривых над различными конечными полями для достижения заданного уровня безопасности в различных криптографических алгоритмах, основанных на математической задаче поиска изогений. Были построены графы изогений для различных кривых, изучены свойства полученных графов. Делаются выводы о выборе кривых и конечных полей для получения графов изогений с необходимыми свойствами.

Список использованных источников:

1. Gora Adj, Omran Ahmadi, and Alfred Menezes. On isogeny graphs of supersingular elliptic curves over finite fields. Cryptology ePrint Archive, Report 2018/132, 2018. https://eprint.iacr.org/2018/132.

Ковалева С.А. (автор) Подпись

Мезенев К.О. (автор) Подпись

Давыдов В.В. (автор, научный руководитель) Подпись