УДК 004.021

О построении схем обязательств, основанных на сложности математических задач постквантовой криптографии

Мутигуллин Р. Р. (Университет ИТМО)

Научный руководитель – преподаватель, Давыдов В. В.

(Университет ИТМО)

Мутигуллин Р. Р. (автор) Подпись

Давыдов В. В. (научный руководитель) Подпись

Введение. Развитие квантовых компьютеров приближает день, когда современные асимметричные криптографические алгоритмы будут взломаны, например, по алгоритму Шора [1]. В связи с этим разрабатываются алгоритмы, основанные на постквантовых математических задачах, которые будут устойчивы к атакам с применением квантовых компьютеров. Одна из актуальных задач в этой сфере - разработка постквантовой схемы обязательства. Схемы обязательства применяются в секретном электронном голосовании, схемах электронной подписи, доказательствах с нулевым разглашением и т.д. В этой работе будут проанализированы некоторые существующие схемы обязательства и определены задачи для решения при разработке следующих алгоритмов.

Основная часть. Постквантовая криптография включает в себя пять разделов:

1. Криптография на кодах, исправляющих ошибки – раздел, который использует помехоустойчивые коды и сложные математические задачи для построения криптографических алгоритмов. Для алгоритмов в этом разделе важно использовать криптостойкие коды. Одним из таких является код Гоппы.
2. Криптография на хеш-функциях. Криптостойкость схем из этого раздела основывается на криптостойкости использованной хеш-функции.
3. Криптография на решетках. Решетка – множество комбинаций линейно-независимых векторов с целыми коэффициентами. Публичным и закрытым ключом здесь являются базисы решетки с разными свойствами. Криптографическая сложность основывается на математических задачах, например, на задачах поиска кратчайшего вектора и поиска ближайшего вектора.
4. Криптография на изогениях эллиптических кривых. Изогения кривой – это рациональное отображение множества точек одной кривой на множество точек другой кривой. Криптостойкость алгоритмов основывается, например, на таких математических задачах – задаче поиска кольца эндоморфизмов для суперсингулярной кривой и задаче поиска изогении между двумя кривыми.
5. Криптография на многомерных уравнениях – раздел, который основывается на задаче решения системы многомерных уравнений.

Рассмотрим некоторые схемы обязательства, построенные на постквантовых задачах:

1. Схема обязательства на кодах, исправляющих ошибки, представленная в 2019 году. Безопасность алгоритма основывается на синдромном декодировании и на кодах Гоппы [3].
2. Схема обязательства на решетках, представленная в 2018 году. Этот алгоритм основывается на математических задачах Module-SIS и ModuleLWE, которые по сути являются векторными задачами о рюкзаке над конкретным кольцом [4].
3. Схема обязательства на изогениях эллиптических кривых, разработанная в 2021 году. Алгоритм основан на задаче нахождения кольца эндоморфизмов для суперсингулярной эллиптической кривой [2].

Важным свойством схемы обязательства является ее гомоморфность. Без этого свойства применение схемы заметно ограничено, например, ее не получится использовать для секретного электронного голосования. Из представленных алгоритмов только второй вариант имеет такое свойство, а также он является быстрейшим из них. Однако размер обязательства в нем слишком большой - 4,4 килобайта. Похожие свойства и у первого варианта, только он не является гомоморфным. Схема на изогениях, напротив, является медленной и не гомоморфной, но обязательство для нее занимает меньше всего памяти. Это свойства

большинства алгоритмов, основанных на изогениях эллиптических кривых. В будущих работах планируется развивать и разрабатывать схемы на изогениях, ведь это самая молодая и неизведанная отрасль в постквантовой криптографии. При разработке схемы важно уделить внимание свойству гомоморфности и скорости алгоритма.

Выводы. Проведен обзор и анализ существующих схем обязательств, основанных на задачах постквантовой криптографии и определены приоритетные задачи при разработке таких схем в следующих работах.

Из представленных алгоритмов только второй вариант имеет свойство гомоморфности, а также он является быстрейшим из них. Однако размер обязательства в нем слишком большой - 4,4 килобайта. Похожие свойства и у первого варианта, только он не является гомоморфным. Схема на изогениях, напротив, является медленной и не гомоморфной, но обязательство для нее занимает меньше всего памяти. Это свойства большинства алгоритмов, основанных на изогениях эллиптических кривых.

Таким образом, приоритетными разделами при разработке схем обязательств являются изогении и решетки благодаря лидерству по потреблению памяти обязательством и скорости соответственно. При разработке схемы на изогениях актуальной задачей является сделать ее вычислительно быстрой и гомоморфной, а при разработке схемы на решетках – уменьшить размер обязательства.

Список использованных источников:

1. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science, pages 124–134, 1994.
2. Bruno Sterner. Commitment Schemes from Supersingular Elliptic Curve Isogeny Graphs. — Surrey Centre for Cyber Security, University of Surrey, UK, 2021.
3. Pedro Branco. A Post-Quantum UC-Commitment Scheme in the Global Random Oracle Model from Code-Based Assumptions. 2019.
4. Carsten Baum, Ivan Damgard, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In Dario Catalano and Roberto De Prisco, editors, Security and Cryptography for Networks, pages 368–385, Cham, 2018. Springer International Publishing.

Мутигуллин Р. Р. (автор) Подпись

Давыдов В. В. (научный руководитель) Подпись