УДК 004.056

Схемы обязательств, построенные на изогениях суперсингулярных эллиптических кривых

Хуцаева А. Ф. (ИТМО)

Научный руководитель – доктор технических наук, доцент Беззатеев С.В. (ИТМО)

Введение. В современном цифровом мире криптографические схемы обязательств имеют важное значение. Они позволяют доказывать владение информацией без ее фактического раскрытия, другими словами, фиксировать некоторое значение.

Однако с появлением квантового компьютера ряд схем обязательств перестанет быть востребованным, так как некоторые их свойства не будут выполняться. Решением данной проблемы является построение схем на математических задачах, при решении которых квантовые компьютеры не имеют преимущества. Таким образом, исследование и разработка схем обязательств, несомненно, является актуальным направлением в обеспечении безопасности в цифровой эре.

Основная часть. В работе предлагаются постквантовые варианты схем обязательств Педерсена [1] и Эль-Гамаля [2]. Данная работа является продолжением и расширением проекта [3].

Как и оригинальные схемы, разработанные включают в себя три основных алгоритма: Запуск, Обязательство и Проверка. Запуск позволяет задать требуемый уровень безопасности и получить на выходе ключ обязательства ck. Обязательство: на основе полученного ранее ключа и некоторого случайного параметра r генерируется обязательство для m: $C_{ck}(r, m)$. И наконец, когда параметры r', m' рассекречены, алгоритм Проверка позволяет провести верификацию, что $C_{ck}(r, m) == C_{ck}(r', m')$.

Предложенные схемы основываются на сложности поиска изогений суперсингулярных эллиптических кривых, за основу взята задача обращения группового действия [4]. Можно заключить, что безопасность схем основывается на сложности обращения группового действия и безопасности схем [1], [2].

Выводы. Преимуществом разработанных схем является устойчивость к атакам на квантовом компьютере. При программной реализации оценивались такие параметры, как скорость генерации обязательства и размеры полученного параметра. Схема обязательств считается одним из ключевых инструментов для обеспечения прозрачности и надежности в различных областях, например, в электронном голосовании или конфиденциальных вычислениях.

Список использованных источников:

1. Pedersen T. P. Non-interactive and information-theoretic secure verifiable secret sharing //Advances in Cryptology—CRYPTO'91: Proceedings. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. – С. 129-140.
2. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms //IEEE transactions on information theory. – 1985. – Т. 31. – №. 4. – С. 469-472.
3. Хуцаева А. Ф., Исайчева А. В. Анализ и реализация протокола конфиденциальных активов// Сборник тезисов летней школы-конференции "Криптография и информационная безопасность" - 2023
4. Castryck W. et al. CSIDH: an efficient post-quantum commutative group action //International Conference on the Theory and Application of Cryptology and Information Security. – Springer, Cham, 2018. – С. 395-427.

Хуцаева А. Ф. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись