УДК 004.056.55

Разработка алгоритма забывчивой подписи, основанного на криптографии на изогениях

Хуцаева А. Ф. (Университет ИТМО)
Научный руководитель – преподаватель Давыдов В. В.
(Университет ИТМО)

Введение. В современном мире, где большинство покупок, банковских операций и прочих действий, совершаются в сети Интернет, конфиденциальность становится в приоритете. Так, рассматривая вопрос о защите личной информации, Л. Чен в 1994 году предложил концепцию забывчивой подписи [1]. Стойкость подписи основана на сложности решения задачи дискретного логарифмирования, что делает ее уязвимой к атакам на квантовом компьютере. Решить данную проблему можно, построив забывчивую подпись на задаче, стойкой к атакам на квантовом компьютере. Одной из перспективных задач постквантовой криптографии, активно исследуемых в последнее время, является задача поиска изогений эллиптических кривых [2]. Таким образом, становится актуальным разработка забывчивой подписи, основанной на криптографии на изогениях.

Основная часть. В работе рассмотрены варианты реализации забывчивой подписи, основанной на сложности поиска изогений эллиптических кривых, а именно проблеме поиска множественных обратных для группового действия [3], которая пригодна для использования в постквантовых алгоритмах.

Благодаря свойствам группы классов идеалов, с помощью которых предлагается вычисление изогений, можно эффективно перенести концепцию, предложенную Л. Ченом, на криптографию на изогениях.

В протоколе принимают участие три стороны: подписывающая, проверяющая (тот, кому подписывают документ) и доверительный центр. Подписывающая и проверяющая стороны взаимодействуют через доверительный центр. Подпись имеет два варианта реализации: первый из них представляет собой схему подписи с n ключами, а второй – схему подписи с n сообщениями.

Использование подобной схемы позволяет реализовать такие протоколы подписи как: генерация открытого ключа и закрытого ключа, подпись сообщения и проверка подписи.

Выводы. Постквантовая схема забывчивой подписи может быть применена в системах, где обязательна конфиденциальность, анонимность пользователей. Отличительной особенностью схемы является устойчивость к известным на сегодняшний день атакам на квантовом компьютере. Также подписи на изогениях имеют небольшие размеры ключей.

Список использованных источников:

1. Chen L. Oblivious signatures //ESORICS. – 1994. – С. 161-172.
2. Jao D., De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies //Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4. – Springer Berlin Heidelberg, 2011. – С. 19-34.
3. 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

Давыдов В. В. (научный руководитель) Подпись