УДК 004.056

РАЗРАБОТКА СХЕМЫ ПОРОГОВОЙ ПОДПИСИ, ОСНОВАННОЙ НА ТЕОРИИ РЕШЕТОК

Леевик А.Г. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – Давыдов В.В.

(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. Криптография на решетках является одним из основных направлений постквантовой криптографии. Национальным институтом стандартов и технологий США были выбраны финалисты конкурса по стандартизации нового постквантового алгоритма, среди которых присутствуют схемы электронной подписи и шифрования с открытым ключом, построенные на теории решеток. Схема пороговой подписи является одной из важных составляющих, используемых в информационных системах с повышенным риском. На данный момент все используемые схемы пороговой подписи основаны на задачах, которые могут быть решены с использованием квантового компьютера, поэтому разработка постквантовых пороговых схем является актуальной задачей на сегодняшний день. Ранее разработанные схемы пороговой подписи на решетках либо были построены на небезопасных и/или неэффективных алгоритмах, либо не обладали свойством изменчивости порога подписи.

Основная часть. В данной работе представлена новая схема пороговой подписи, построенная на алгоритмах теории решеток с доказанной безопасностью, а также обладающая свойством изменения порога. Для данной схемы показана ее корректность, а также доказана ее безопасность. Разработанная схема основана на работе Дамгора [1], в которой представлена n-из-n пороговая подпись. В свою очередь схема Дамгора использует алгоритм подписи, который основан на работе Любашевского [2], а также используется в схеме электронной подписи Dilithium [3]. Новая схема по факту расширяет схему Дамгора, добавляя в нее новое свойство изменения порога. Данное свойство было реализовано путем комбинирования оригинальной схемы со схемой разделения секрета Шамира [4].

Выводы. Данная схема может считаться безопасной схемой пороговой электронной подписи, построенной на новейших алгоритмах теории решеток. Данная схема может применяться в децентрализованных системах, а также может являться дополнительным механизмом защиты, используемым для обеспечения конфиденциальности закрытого ключа пользователя в критически важных информационных системах, как например, банковских системах.

Список использованных источников:

1. Damgård, C. Orlandi, A. Takahashi, and M. Tibouchi, “Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices,” Journal of Cryptology, vol. 35, no. 2, pp. 1–56, 2022.
2. V. Lyubashevsky, “Lattice signatures without trapdoors,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2012, pp. 738–755.
3. Ducas L. et al. Crystals-dilithium: A lattice-based digital signature scheme //IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2018. – С. 238-268.
4. Shamir A. How to share a secret //Communications of the ACM. – 1979. – Т. 22. – №. 11. – С. 612-613.

Леевик А.Г. (автор)

Давыдов В.В. (научный руководитель)