УДК 003.26

ОЦЕНКА КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ МОДИФИЦИРОВАННОЙ СХЕМЫ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ СХЕМЫ ШТЕРНА

Ниткин И.С.
Научный руководитель – Давыдов В.В.
Университет ИТМО

Введение.

Современные криптографические алгоритмы, построенные на вычислительной сложности факторизации натурального числа, дискретного логарифмирования в конечном поле и извлечении квадратного корня в кольце вычетов по модулю составного числа потенциально уязвимы к атакам при помощи квантового компьютера [1]. Решением данной проблемы является разработка криптографических схем на основе вычислительных задач, решение которых за полиномиальное время не может быть получено с помощью квантового компьютера. Данный раздел криптографии (пост-квантовая криптография) является одним из наиболее востребованных в рамках современных исследований [2].

Схема Штерна [3] представляет собой схему идентификации с нулевым разглашением, построенную на вычислительной сложности решения NP-полной проблемы синдромного декодирования произвольного линейного кода. Для осуществления проверки веса Хэмминга секретного ключа в структуре схемы Штерна используются перестановки.

Основная часть.

При использовании схемы Штерна в неинтерактивном виде, может быть реализована схема электронной подписи. При этом хранение перестановок занимает значительную часть памяти по сравнению с другими элементами структуры подписи. Для уменьшения объема памяти, необходимого для хранения перестановки предлагается алгоритм, позволяющий при помощи регистра сдвига с линейной обратной связью генерировать случайную перестановку из подмножества перестановок заданной мощности. Перестановка, сгенерированная этим алгоритмом, может быть описана при помощи вектора значений, длина которого значительно меньше длины перестановки.

Использование предложенного алгоритма для генерации перестановок электронной подписи на основе схемы Штерна позволяет сократить размер подписи, при этом практически не оказывая влияния на время работы алгоритмов.

На основе экспериментальных исследований произведена оценка уровня криптографической стойкости описанной модифицированной схемы подписи на основе схемы Штерна и сделаны выводы о возможности ее применения.

Заключение.

Таким образом, в рамках проведенного исследования предложен алгоритм генерации перестановки для модифицированной схемы подписи на основе схемы Штерна, произведена сравнительная оценка характеристик стандартной и модифицированной схем подписи, а также рассчитана сравнительная оценка уровня криптографической стойкости этих схем.

Список использованных источников:

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring / P. W. Shor // Proceedings of the 35th Annual Symposium on Foundations of Computer Science : электронный журнал. – URL: https://doi.org/10.1109/SFCS.1994.365700.
2. Bernstein D.J. Introduction to post-quantum cryptography / D.J. Bernstein. – Berlin : Springer, 2009. – 248 с. – URL: https://doi.org/10.1007/978-3-540-88702-7_1 (дата обращения: 19.12.2022).

3. Stern J. A new identification scheme based on syndrome decoding / J. Stern // Advances in Cryptology — CRYPTO : электронный журнал. – URL: https://link.springer.com/content/pdf/10.1007/3-540-48329-2_2.pdf?pdf=inline%20link. – Дата публикации: 1993.

Ниткин И.С. (автор) _____

Давыдов В.В. (научный руководитель) _____