Постквантовые криптографические алгоритмы цифровой подписи: сравнительный анализ и главные проблемы

Качмазов Руслан Александрович

Бакалавр 3 курса

ФКН ПИ НИУ ВШЭ, Москва, Россия

E-mail: rakachmazov@edu.hse.ru

Научный руководитель *— Хаустов Александр Иванович*

После открытия алгоритма Шора [1] стало понятно, что большинство из используемых сегодня ассиметричных криптографических алгоритмов могут быть скомпрометированы при появлении достаточно мощного квантового компьютера, так как они основаны на проблеме дискретного логарифмирования и факторизации чисел, например, RSA и ECDSA. Учитывая то, что сфера квантовых вычислений активно развивается, криптографическое сообщество начало думать о внедрении новых алгоритмов, способных противостоять такого рода атакам – эта сфера была названа постквантовой криптографией. В основном, постквантовые алгоритмы строятся на задачах теории целочисленных решеток, кодов исправления ошибок, хэш-функций, систем многочленов от многих переменных, изогении элиптических кривых, теории кос и других.

В 2016 году NIST учредил конкурс, в котором отбирал алгоритмы инкапсуляции ключа (KEM) и цифровой подписи, результатом которого стали 3 финалиста в рамках цифровой подписи: CRYSTALS-Dilithium (решетки), SPHINCS+ (хэш-функции) и Falcon (решетки). Отечественная криптография не осталась в стороне, и в рамках ТК26 была создана рабочая группа 2.5, занимающаяся постквантовой криптографией. Представлены первые версии алгоритмов Гиперикум (хэш-функции) и Шиповник (коды ошибок).

В работе описан теоретический разбор криптостойкости пяти постквантовых алгоритмов цифровой подписи, описанных выше. Проведен сравнительный анализ по скорости, размеру ключей и подписи, сложности программной реализации. Также рассмотрен потенциальный процесс перехода на постквантовую криптографию, затрагивающий гибридное шифрование и множество этапов адаптации систем.

Литература

1. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring (англ.) // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134. — ISBN 0-8186-6580-7