УДК 004.942

АНАЛИЗ СТОЙКОСТИ ПОСТКВАНТОВОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ NTRUENCRYPT

Авторы:

Разумов Павел Владимирович – студент 5-го кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: therazumov@gmail.com

Смирнов Иван Андреевич – студент 5-го кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: terran.doatk@mail.ru

Черкесова Лариса Владимировна – доцент, д.ф.-м.н., и профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: chia2002@inbox.ru

Короченцев Денис Александрович – доцент, к.т.н., и заведующий кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: mytelefon@mail.ru

Поркшеян Виталий Маркосович – доцент, к.ф.-м.н., декан факультета «Информатика и вычислительная техника» Донского государственного технического университета, Ростов-на-Дону, e-mail: spu-40@donstu.ru

Научный руководитель – доцент, д.ф.-м.н., и профессор кафедры «Кибербезопасность информационных систем» Донского государственного технического университета, Ростов-на-Дону, e-mail: chia2002@inbox.ru

Введение. Криптографическая система NTRUEncrypt способна обеспечить необходимый уровень безопасности по чрезвычайно низкой стоимости, обладая при этом высокими показателями быстродействия и низкими требованиями к объёму памяти. Данное условие является немаловажным фактором привлекательности криптосистемы NTRUEncrypt и её широкого использования в настоящее время.

Цель работы. С введением в эксплуатацию квантовых технологий многие криптографические системы становятся бесполезными, в том числе и криптосистема RSA. Благодаря изложенному факту необходимо сделать вывод, что криптосистема NTRUEncrypt является более стойкая к атакам квантовых компьютеров за счёт трудностей поиска кратчайшего вектора решётки.

Базовые положения исследования. На сегодняшний день многочисленные из множества недостатков доработаны, что влечет за собой практическое применение криптосистемы NTRUEncrypt, являющейся более быстрой, чем алгоритм RSA. Этот факт подтверждают специалисты RSA Labs, а также независимые исследователи.

Более того, учитывая тот факт, что криптосистема NTRUencrypt является постквантовой, ее криптостойкость к различного рода атакам является довольно высокой, так как криптостойкость алгоритма обеспечивается отсутствием алгоритма поиска кратчайшего вектора решётки.

Промежуточные результаты. Наиболее значимыми факторами создания квантовых компьютеров в целях усиления криптостойкости алгоритма NTRUencrypt являются задачи быстрой факторизации и дискретного логарифмирования.

Вывод. С введением в эксплуатацию квантовых технологий многие криптографические системы становятся менее криптографически стойкими, в том числе такие, как криптосистема RSA. В качестве альтернативной системы исследована криптосистема NTRUEncrypt, являющаяся более стойкой к атакам квантовых компьютеров за счёт трудностей поиска кратчайшего вектора решётки.