

ВОПРОСЫ ПРОГРАММНОЙ РЕАЛИЗАЦИИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА КВАЗИЦИКЛИЧЕСКИХ MDPC КОДАХ

Соколова Анастасия Александровна

Студентка

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: soko.anastasiia@gmail.com

Все криптосистемы, основанные на сложности решения задачи факторизации или дискретного логифрирования могут быть атакованы за полиномиальное время на квантовом компьютере [3]. Это приведет к снижению стойкости большинства реализованных на практике криптосистем, таких, как RSA или DSA.

Одним из возможных и актуальных вариантов решения этой проблемы является использование кодовых криптосистем, например, криптосистемы Мак-Элиса.

Основная идея ее построения состоит в том, что некоторый линейный код, имеющий эффективные алгоритмы декодирования, маскируется под код, не обладающий видимой алгебраической и комбинаторной структурой (код общего положения). Считается, что его декодирование представляет собой трудную задачу.

Код с малой плотностью проверок на чётность (LDPC-код) подходит для использования в схеме, предложенной Мак-Элисом. Каждая строка проверочной матрицы может рассматриваться как кодовое слово «небольшого» веса, дуального к LDPC-коду. Поэтому становится осуществимой атака «в лоб», которая осуществляет поиск слов минимального веса в дуальном коде и строит из них разреженную проверочную матрицу.

Небольшое увеличение длины и веса строки проверочной матрицы является достаточным для того, чтобы избежать всех известных атак, основанных на стандартных алгоритмах декодирования. Коды такого вида названы кодами со средней плотностью проверок на четность (MDPC-коды) [1].

В данной работе была предложена и реализована на языке C модификация криптосистемы Мак-Элиса, эффективно использующая квазициклические MDPC коды.

MDPC-коды в предложенной реализации декодируются модификацией алгоритма Галлагера [2]. Этот итеративный декодирующий алгоритм позволяет корректировать ошибки, эффективность повышается линейно при увеличении длины кода и уменьшается почти

линейно при увеличении веса строки проверочной матрицы. Выбор именно квазициклических МДРС-кодов был обусловлен тем, что на практике они требуют ключей значительно более компактной длины, нежели обычные МДРС-коды, что является критичным на практике.

Достигнутая в текущей версии реализации алгоритма скорость позволяет эффективно проводить вычисления вплоть до $r = 1599$ (длина открытого ключа в битах). Этапы шифрования и расшифрования занимают около 80 миллисекунд, в то время, как полное время работы алгоритма со всеми этапами, включая генерацию ключей, занимает около 24 секунд. Ранее на том же вычислительном устройстве был достигнут результат в 50 секунд, в текущей же реализации длина кода для ключа, генерируемого за такое же время, составляет, приблизительно, $r_1 = 2050$ бит. Все вычисления и замеры проводились на персональном компьютере (8 ядер Intel Core i7, 2.70GHz).

Литература

1. Misoczki R., Tillich J.-P., Sendrier N., Barreto P. S. L. M. MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. // Cryptology ePrint Archive, Report 2012/409, 2012.
2. Gallager R. G. Low-Density Parity-Check Codes. // M.I.T. Press, 1963.
3. Bernstein D. J., Buchmann J., and Dahmen E., editors. Post-Quantum Cryptography. // Springer-Verlag, 2009.
4. Чижов И. В. Пространство ключей криптосистемы Мак-Элиса-Сидельникова. // Диссертация, кафедра информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова, защищена в 2010 г.
5. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки // М.: Связь, 1979.