Исследование свойств криптосистемы типа Мак-Элиса-Сидельникова, построенной на основе случайных кодов

Попова Елизавета Александровна

Студент

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

E-mail: lady-lizochka@yandex.ru

Научный руководитель — *Чижов Иван Владимирович*

С приходом эры квантовых компьютеров криптосистемы, построенные на сложности задач факторизации и дискретного логарифмиорования, потеряют свою стойкость. Поэтому крайне актуальным является исследование криптосистем с открытым ключом, стойкость которых основана на других сложных задачах, например, на задаче декодирования кода общего положения. Примером такой криптосистемы является криптосистема Мак-Элиса.

Одна из модификаций этой криптосистемы, описанная в статье [1], явилась основой данной работы. Была рассмотрена криптосистема Мак-Элиса, открытый и секретный ключи которой имеют вид $K_{pub} = S(RM|Rand)P$, $K_{sec} = (M, P)$, где $RM = RM(m, r)$ — порождающая матрица кода Рида-Маллера порядка r и размерности m, $Rand$ — порождающая матрица случайного $[n, k]$–кода, S — невырожденная, а P — перестановочная матрицы.

Для исследования была взята модель, в которой противнику кроме открытого ключа известна порождающая матрица случайного кода $Rand$, и целью является восстановление перестановочной матрицы P. В рамках данной работы с использованием сигнатурного метода [2] была разработана атака, восстанавливающая P в описанной выше модели. Алгоритм данной атаки приведен ниже.

Вход: матрицы K_{pub} и $(RM|Rand)$.

1. Посчитать все спектры оболочек кодов, полученных выкалыванием каждого столбца из порождающей матрицы $(RM|Rand)$. Сделать те же рассчеты при выкалывании всех пар столбцов. На выходе данного шага имеется таблица соответствия вектора спектра и столбца, при выкалывании которого получается данный вектор.

2. Для кода с порождающей матрицей K_{pub} посчитать спектры оболочек выколотых кодов. При этом выделить те столбцы,

при выкалывании которых получается уникальный спектр. Эти столбцы однозначно идентифицируемы по таблице из пункта 1. Обозначим их множество за I_0.

3. Посчитать спектры оболочек кодов, полученных выкалыванием из кода с порождающей матрицей K_{pub} двух столбцов i, j, где $i \in I_0$, $j \notin I_0$, добавляя при этом в множество I_0 столбцы, однозначно идентифицируемые по полученным спектрам дважды выколотых кодов. Данный процесс продолжается, пока появляются новые столбцы в I_0.

4. Посчитать матрицу квадрата кода с порождающей матрицей K_{pub}. Для квадрата кода выполнить шаги 2 и 3

5. Если после шага 4 остались столбцы, которые нельзя однозначно идентифицировать по их спектрам, то для полного восстановления матрицы P используется полный перебор всех возможных вариантов по оставшимся столбцам.

Сложность предложенной атаки $\leq n \cdot 2^{S_1} + \binom{n}{2} \cdot 2^{S_2} + L!$, где S_1, S_2 - размерности оболочек выколотых и дважды выколотых кодов соответственно, L - количество неразличимых столбцов. На основе [3] было доказано, что с наибольшей вероятностью $S_1 = 1$ и $S_2 = 1$.

Результаты применения данной атаки к ключам разного размера представлены в таблице ниже.

Размеры $K_{pub} = (k \times n)$	S_1	S_2	L
(22×128)	1	1	7
(93×512)	1	1	10
(130×1024)	1	1	25

Литература

1. Kabatiansky G., Tavernier C. A new code-based cryptosystem via pseudorepetition of codes, In Proceedings of Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk,Russia, 2018, P. 189-191
2. Sendrier N. The Supporting Splitting Algorithm, IEEE Transactions on Information Theory, 2000, V. 46, P. 1193-1203
3. Sendrier N. On the Dimension of the Hull, SIAM Journal on Discrete Mathematics, 1997, P. 282-293.