

КРИПТОАНАЛИЗ КODOVЫХ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ, ПОСТРОЕННЫХ НА ПОДКОДАХ КОДА РИДА-МАЛЛЕРА

Агапова Екатерина Алексеевна

Магистрант

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

E-mail: aea1994@yandex.ru

В работе изучается постквантовая криптосистема Мак-Элиса, основанная на подкодах кода Риды-Маллера. Использовать коды Риды-Маллера $RM(r, m)$ для построения криптосистемы Мак-Элиса предложил В.М. Сидельников [1] в 1996 году. В 2007 году Л. Миндер и А. Шокроллахи предложили достаточно эффективную атаку на такую криптосистему. В 2013 году М. Бородин и И. Чижев [2] понизили стойкость этой криптосистемы, а также построили полиномиальную атаку в случае использования кода Риды-Маллера $RM(r, m)$ с такими параметрами, что $\text{НОД}(r, m - 1) = 1$.

В работе предлагается атака на криптосистему Мак-Элиса, основанную на $(k - 2)$ – подкодах кода Риды-Маллера. Для построения атаки были использованы введенные в [2] операции: бинарная операция умножения $\circ$ двух кодов и унарная операция $\perp$ взятия ортогонального кода.

Пусть C — произвольный $(k - 2)$ – подкод кода Риды-Маллера $RM(r, m)$, из которого были удалены мономы $f_1 = x^{\alpha_1}$ и $f_2 = x^{\alpha_2}$, $\alpha_1 < \alpha_2$. Заметим, что такие мономы существуют, так как подкод C не совпадает со всем кодом $RM(r, m)$, и находятся методом перебора всех мономов, начиная с монома $1 = x^{(0,0,\dots,0)}$. Введем векторы $a_1 = (a_1(\alpha') | \alpha' \in \mathbf{A}(r, m))$ и $a_2 = (a_2(\alpha') | \alpha' \in \mathbf{A}(r, m))$. Будем в дальнейшем такой код обозначать символом $C_{\alpha_1, \alpha_2, a_1, a_2}(r, m)$:

$$C_{\alpha_1, \alpha_2, a_1, a_2}(r, m) : \begin{cases} \forall \alpha' : \alpha' < \alpha_1, x^{\alpha'}; \\ \forall \alpha' : \alpha_1 < \alpha' < \alpha_2, x^{\alpha'} \oplus a_1(\alpha')x^{\alpha_1}; \\ \forall \alpha' : \alpha_2 < \alpha', x^{\alpha'} \oplus a_1(\alpha')x^{\alpha_1} \oplus a_2(\alpha')x^{\alpha_2}; \end{cases}$$

Теорема 1. Пусть $\alpha_1 \in \mathbf{A}(r, m)$, $\alpha_2 \in \mathbf{A}(r, m)$, $\alpha_1 > \alpha_2$, $wt(\alpha_1)$, $wt(\alpha_2) \geq 2$. Тогда для любых a_1 и a_2 выполняется равенство:

$$C_{\alpha_1, \alpha_2, a_1, a_2}(r, m) \circ C_{\alpha_1, \alpha_2, a_1, a_2}(r, m) = RM(2r, m).$$

Также верны следующие утверждения:

1. Код, ортогональный $(k - 2)$ – подкоду кода Рида-Маллера $RM(r, m)$ $C_{1,2,0,0}^\perp$, имеет вид:

$$C_{1,2,0,0}^\perp = \left(\begin{array}{c} RM^\perp(r, m) \\ \overline{x_2} \ \overline{x_3} \dots \overline{x_m} \\ \overline{x_1} \ \overline{x_3} \dots \overline{x_m} \end{array} \right)$$

2. При умножении кода $C_{1,2,0,0}^\perp$ на себя t раз ($t \geq 2$) получится код вида:

$$t \cdot C_{1,2,0,0}^\perp = \left(\begin{array}{c} RM^\perp(tr, m) \\ \overline{x_1} \ \overline{x_2} \dots \overline{x_m} \\ \overline{x_2} \ \overline{x_3} \dots \overline{x_m} \\ \overline{x_1} \ \overline{x_3} \dots \overline{x_m} \end{array} \right)$$

С помощью данных свойств действий над подкодами в работе была предложена атака на криптосистему Мак-Элиса, основанную на $(k - 2)$ – подкодах кода Рида-Маллера $C_{\alpha_1, \alpha_2, a_1, a_2}(r, m)$, таких что $\alpha_1 > \alpha_2$, $wt(\alpha_1)$, $wt(\alpha_2) \geq 2$. Алгоритм атаки восстановит секретный ключ рассматриваемой криптосистемы по её открытому ключу за полиномиальное время от битовой длины открытого ключа в случае использования кода $RM(r, m)$ с такими параметрами, что $\text{НОД}(r, m - 1) = 1$ и $2r < m - 1$.

Литература

1. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида-Маллера, Дискретная математика. 1994. Т. 6(2).
2. Бородин М. А., Чижов И. В. Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида-Маллера.
3. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol. 1978. Vol. January.