Криптоанализ криптосистемы Мак-Элиса, построенной на подкодах кода Рида-Маллера

Агапова Екатерина Алексеевна

Студент

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 Рида-Маллера. Использовать коды Рида-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. Чижов [2] понизили стойкость этой криптосистемы, а также построили полиномиальную атаку в случае использования кода Рида-Маллера $RM(r,m)$ с такими параметрами, что НОД$(r, m-1) = 1$.

В работе предлагается атака на криптосистему Мак-Элиса, основанную на $(k-1)$ – подкодах кода Рида-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 $(k-1)$—подкод кода Рида-Маллера $RM(r,m)$. Рассмотрим такой моном $f_{min} = x^{\alpha}$, что $f_{min} \notin C$ и

$$C_{\alpha,a}(r,m): \begin{cases} \forall \alpha' : \ \alpha' < \alpha, \ x^{\alpha'}; \\ \forall \alpha' : \ \alpha' > \alpha, \ x^{\alpha'} \oplus a(\alpha') x^{\alpha}; \end{cases}$$

Здесь

$$A(r,m) = \{\alpha = (\alpha_{m-1}, ...\alpha_0) | x^{\alpha} \in RM(r,m)\},$$
$$a = (a(\alpha') | \alpha' \in A(r,m), \alpha' \neq \alpha).$$

Теорема 1. *Пусть $2r < m$. Тогда для любых $\alpha, wt(\alpha) = 1$, либо*

$$C_{\alpha,a}(r,m) \circ C_{\alpha,a}(r,m) = RM(2r,m), \tag{1}$$

либо существует такой автоморфизм $\sigma_{A,b}$ кода $RM(r,m)$, что

$$C_{\alpha,a}(r,m) \circ C_{\alpha,a}(r,m) = C_{1,0}^{\sigma_{A,b}}(2r,m). \tag{2}$$

Теорема 2. *Пусть* $r_1 + r_2 < m$. *Пусть также* $\alpha \in \mathbf{A}(r_1, m), \beta \in \mathbf{A}(r_2, m)$, *причем выполнено одно из двух условий:*

- $\alpha \neq \beta,\ \alpha, \beta > 0$;
- $\alpha = \beta$ *и* $wt(\alpha) \geqslant 2$.

Тогда для любых a^1 *и* a^2 *выполняется равенство:*

$$C_{\alpha,a^1}(r_1, m) \circ C_{\beta,a^2}(r_2, m) = RM(r_1 + r_2, m). \tag{3}$$

С помощью данных свойств умножения подкодов в работе была предложена атака на криптосистему Мак-Элиса, основанную на $(k-1)$ – подкодах кода Рида-Маллера. Алгоритм атаки восстановит секретный ключ рассматриваемой криптосистемы за полиномиальное время от битовой длины секретного ключа в случае использования кода $RM(r, m)$ с такими параметрами, что 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.