из V_{32}, то вероятность линейной независимости системы равна $\prod_{i=0}^{7}(1-2^{i-32})$, то есть превышает $1-2^{24}$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Романько Д. А., Фомичев В. М.* О способах построения криптографических генераторов с заданным показателем бесповторности выходных последовательностей // Прикладная дискретная математика. Приложение. 2016. № 9. С. 65–67.

УДК 004.056.55 DOI 10.17223/2226308X/9/29

КРИПТОАНАЛИЗ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА $(k-1)$-ПОДКОДАХ КОДА РИДА — МАЛЛЕРА

И. В. Чижов, М. А. Бородин

Описаны два вида криптосистем Мак-Элиса, построенных на подкодах кода Рида — Маллера. Изучен вопрос эквивалентных ключей для этих криптосистем. Получен результат о сводимости одной криптосистемы к другой. Приведены алгоритмы, которые позволяют применить атаку Чижова — Бородина к рассматриваемым криптосистемам для некоторых параметров кодов Рида — Маллера.

Ключевые слова: *криптосистема Мак-Элиса, подкоды Рида — Маллера, автоморфизмы кодов Рида — Маллера, произведение Шура, квадрат кода.*

Криптосистема Мак-Элиса предложена в 1978 г. Р. Дж. Мак-Элисом. Её стойкость основана на предположении сложности декодирования кода общего положения. Оригинальная криптосистема Мак-Элиса строится на двоичных кодах Гоппы. Для повышения эксплуатационных характеристик В. М. Сидельников предложил использовать коды Рида — Маллера [1]. Однако в 2007 г. Л. Миндера и А. Шокроллахи предложили достаточно эффективную атаку на такую криптосистему [2]. Кроме того, в 2013 г. Бородин и Чижов ещё больше понизили стойкость этой криптосистемы, а также построили полиномиальную атаку в случае использования кода Рида — Маллера $RM(r,m)$ с такими параметрами, что $(r, m-1)=1$ [3].

Бывает, что атаки на кодовые криптосистемы, работающие в случае использования полного кода, оказываются бесполезными в случае использования некоторых подкодов кода. Так была предложена криптосистема Бергера — Луадро, построенная на подкодах кода Рида — Соломона. В работе рассматриваются два аналога криптосистемы Бергера — Луадро, построенных на $(k-1)$-подкодах кода Рида — Маллера $RM(r,m)$.

Пусть V_n — множество всех двоичных векторов длины n. Известно, что с каждой булевой функцией $f(x_1,x_2,\ldots,x_m) : V_m \to V_1$ можно связать вектор значений $\Omega_f = (f(0,0,\ldots,0), f(0,0,\ldots,1),\ldots,f(1,1,\ldots,1))$. В дальнейшем не будем делать различий в обозначениях между булевой функцией и её вектором значений. Каждая булева функция может быть представлена полиномом Жегалкина: $f(x_1,x_2,\ldots,x_m) = \bigoplus_{u=(u_1,u_2,\ldots,u_m)\in V_m} g_f(u)x^u$, здесь $x^u = x_1^{u_1}x_2^{u_2}\ldots x_m^{u_m}$ и $x_i^{u_i} = x_i$, если $u_i = 1$, и $x_i^{u_i} = 1$, если $u_i = 0$, а $g_f(u)$ — некоторая булева функция.

Определение 1. Степенью булевой функции называется наименьшее целое положительное число d, такое, что $g_f(u) = 0$ для всех u веса больше d, т. е. $\mathrm{wt}(u) > d$.

Определение 2. Кодом Рида — Маллера $RM(r,m)$ называется множество всех векторов значений булевых функций от m переменных, степень которых не превосходит r.

Базисом кода являются все мономы степени r от m переменных:

$$1,\ x_1,\ \ldots,\ x_{m-1},\ x_1x_2,\ \ldots,\ x_{m-1}x_m,\ \ldots,\ x_1x_2\cdots x_r,\ \ldots,\ x_{m-r-1}\cdots x_m. \qquad (1)$$

Для двоичного набора $\alpha = (\alpha_{m-1},\ldots,\alpha_0)$ символом $|\alpha|$ обозначим представление двоичной строки в виде десятичного числа α, т. е. $|\alpha| = \alpha_0 + 2\alpha_1 + \ldots + 2^{m-1}\alpha_{m-1}$. Введём отношение порядка для векторов $\alpha, \beta \in V_m$. Будем считать, что $\alpha < \beta$, если либо $\mathrm{wt}(\alpha) < \mathrm{wt}(\beta)$, либо $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$ и $|\alpha| < |\beta|$. Тогда можно ввести отношение порядка на множестве мономов: $x^\alpha < x^\beta$, если $\alpha < \beta$.

Определение 3. Стандартной формой порождающей матрицы кода $RM(r,m)$ будем называть матрицу, составленную из всех векторов значений мономов (1), стоящих в порядке возрастания.

Обозначим также символом $\mathbf{A}(r,m)$ множество всех таких наборов $\alpha = (\alpha_{m-1}, \ldots,\alpha_0)$, что моном x^α входит в стандартную форму порождающей матрицы кода $RM(r,m)$.

Устройство криптосистемы первого типа $McElRM1(r,m)$. Для генерации ключей строится стандартная форма порождающей матрицы R кода $RM(r,m)$. Далее выбирается случайная двоичная невырожденная $(k\times n)$-матрица $H = (h_{ij})$ и случайная подстановка $\sigma \in S_n$, представленная в виде перестановочной $(n\times n)$-матрицы P_σ. Затем вычисляется матрица $G' = H\cdot R\cdot P_\sigma = H\cdot R^\sigma$ и из неё удаляется первая строка, получается $((k-1)\times n)$-матрица G. *Секретным ключом* криптосистемы является набор $(H, P_\sigma) = (H,\sigma)$, а *открытым ключом* — матрица G и (r,m) — параметры кода Рида — Маллера, однако, ради удобства, параметры в открытый ключ не включены.

Устройство криптосистемы второго типа $McElRM2(r,m)$. Для генерации ключей строится стандартная форма порождающей матрицы R кода $RM(r,m)$. Далее выбирается случайный номер i, $1 \leqslant i \leqslant k$. Из матрицы R удаляется строка с номером i. Получившуюся в результате матрицу обозначим через $R[i]$. Выбирается случайная двоичная невырожденная $((k-1)\times n)$-матрица $H = (h_{ij})$ и случайная перестановочная $(n\times n)$-матрица $P_\sigma = (p_{ij})$. Вычисляется матрица $G = H\cdot R[i]\cdot P_\sigma = H\cdot (R[i])^\sigma$. *Секретным ключом* криптосистемы является набор $(H, P_\sigma, i) = (H,\sigma,i)$, а *открытым ключом* — матрица G.

Определение 4. Два секретных ключа (H_1,σ_1) и (H_2,σ_2) называются *эквивалентными*, если соответствующие им открытые ключи G_1 и G_2 равны.

В работе решается задача восстановления секретного ключа криптосистемы или эквивалентного ему по открытому ключу.

Пусть (H,σ) — некоторый секретный ключ криптосистемы $McElRM1(r,m)$; G — соответствующий ему открытый ключ; $\sigma_{A,b}$ — некоторый автоморфизм кода Рида — Маллера. Тогда для порождающей матрицы R кода Рида — Маллера существует единственная матрица $H_{A,b}$ (невырожденная), что $H_{A,b}R = R\sigma_{A,b}$.

Теорема 1. Пусть $[(H,\sigma)]$ — класс эквивалентности секретного ключа (H,σ) криптосистемы $McElRM1$. Тогда $\{(HH_{A,b}, \sigma_{A,b}^{-1}\sigma) : \sigma_{A,b} \in \mathrm{Aut}(RM(r,m))\} \subseteq [(H,\sigma)]$.

Пусть C — произвольный $(k-1)$-подкод кода Рида — Маллера $RM(r,m)$. Рассмотрим такой моном $f_{\min} = x^{\alpha_{\min}}$, что для всех $\alpha' < \alpha_{\min}$ моном $x^{\alpha'} \in C$, а $f_{\min} \notin C$. Такой

моном существует и единственный. Пусть $\alpha = \alpha_{\min}$. Для всех $\alpha' > \alpha$ либо моном $x^{\alpha'} \in C$, либо $x^{\alpha'} \oplus x^{\alpha} \in C$, т. е. $x^{\alpha'} \oplus a(\alpha')x^{\alpha} \in C$ для некоторого $a(\alpha') \in \{0, 1\}$. Введём вектор $a = (a(\alpha') : \alpha' \in \mathbf{A}(r, m))$. Тогда код C однозначно определяется векторами α и a. Будем в дальнейшем такой код обозначать символом $C_{\alpha,a}(r, m)$, причём $a(\alpha') = 0$ для всех $\alpha' < \alpha$ и $a(\alpha) = 1$. Отметим, что открытый ключ G криптосистемы первого типа — это порождающая матрица кода $C^{\sigma}_{\alpha,a}$ для некоторого α и a.

Для построения атаки на криптосистему первого типа используем идеи работы [3].

Определение 5. Пусть C и B — два линейных $[n, k]$-кода. Произведением $C \circ B$ назовём код, состоящий из всех возможных произведений кодовых слов $c \cdot b$, $c \in C$, $b \in B$. Здесь $c \cdot b = (c_1 \cdot b_1, c_2 \cdot b_2, \ldots, c_n \cdot b_n)$, если $c = (c_1, \ldots, c_n)$ и $b = (b_1, \ldots, b_n)$.

Доказаны следующие теоремы.

Теорема 2. Пусть $r_1 + r_2 \leqslant m$. Пусть также $\alpha^1 \in \mathbf{A}(r_1, m)$, $\alpha^2 \in \mathbf{A}(r_2, m)$, причём выполнено одно из двух условий:

1) $\alpha^1 \neq \alpha^2$, $\alpha^1, \alpha^2 > 0$;
2) $\alpha^1 = \alpha^2 = \alpha$ и $\mathrm{wt}(\alpha) \geqslant 2$.

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

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

Теорема 3. Пусть $2r < m$. Тогда для любых α, таких, что $\mathrm{wt}(\alpha) = 1$, либо $C_{\alpha,a}(r, m) \circ C_{\alpha,a}(r, m) = RM(2r, m)$, либо существует такой автоморфизм $\sigma_{A,b}$ кода Рида — Маллера $RM(r, m)$, что $C_{\alpha,a}(r, m) \circ C_{\alpha,a}(r, m) = C^{\sigma_{A,b}}_{1,0}(2r, m)$.

Общая схема атаки на криптосистему первого типа $McElRM1(r, m)$:

Ш а г 1. По матрице G построить порождающую матрицу кода $RM^{\sigma}(r, m)$.

Ш а г 2. Применить атаку Чижова — Бородина к этой матрице.

Для реализации первого шага предложен полиномиальный по сложности алгоритм, корректность работы которого доказывается при помощи теорем 2 и 3. Входным значением для алгоритма является открытый ключ криптосистемы $McElRM1(r, m)$ — матрица G, которая соответствует подкоду $C^{\sigma}_{\alpha,a}$. Выходным значением является порождающая матрица кода $RM^{\sigma}(r, m)$. Алгоритм применим для следующих параметров: $2r \leqslant m - 1$ при любом $\mathrm{wt}(\alpha)$ и для $2r \geqslant m$ при $\mathrm{wt}(\alpha) \leqslant m - r - 1$.

ЛИТЕРАТУРА

1. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. № 2. С. 3–20.
2. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
3. *Бородин М. А., Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.