Math-Net.Ru

Общероссийский математический портал

М. А. Бородин, И. В. Чижов, Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера, *Дискрет. матем.*, 2014, том 26, выпуск 1, 10–20

DOI: <https://doi.org/10.4213/dm1264>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.95.254.165

26 апреля 2023 г., 15:13:25

Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера

© 2014 г. М. А. Бородин¹, И. В. Чижов²

Криптосистема Мак-Элиса является криптосистемой с открытым ключом, стойкость которой основана на сложности задачи декодирования произвольного кода, исправляющего ошибки. В 1994 году В. М. Сидельников предложил для построения криптосистемы использовать двоичные коды Рида–Маллера. В 2007 году Л. Миндер и А. Шокроллахи построили структурную атаку на криптосистему Мак-Элиса, в основе которой лежат коды Рида–Маллера. В работе получено улучшение этой атаки, а также предложена полиномиальная атака на криптосистему Мак-Элиса, построенную на основе таких кодов Рида–Маллера $RM(r, m)$, что $\text{НОД}(r, m - 1) = 1$.

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 Р. Дж. Мак-Элисом [1]. Основная идея ее построения состоит в маскировке некоторого кода, имеющего эффективные алгоритмы декодирования, под код, не обладающий видимой алгебраической и комбинаторной структурой; такие коды принято называть кодами общего положения. Криптосистема Мак-Элиса является альтернативой таким криптосистемам, как RSA и ЭльГамала, которые получили широкое практическое применение. Однако развитие квантовых вычислений может понизить их стойкость, что приведет к отказу от использования этих криптосистем. Таким образом, исследование криптосистем с открытым ключом, стойкость которых основана не на сложности задач дискретного логарифмирования и факторизации чисел, является достаточно важным.

В алгоритме шифрования криптосистемы Мак-Элиса используются случайные векторы некоторого фиксированного веса, поэтому для реализации криптосистемы на практике требуются хорошие датчики случайных чисел, что не всегда удобно. В 1986 году Г. Нидеррайтер [4] предложил эквивалентный вариант криптосистемы Мак-Элиса, в котором нет необходимости использовать датчик случайных чисел. Но в этом случае падает скорость передачи, т. е. отношение длины открытого текста к длине шифртекста. В варианте Г. Нидеррайтера скорость передачи напрямую зависит от числа ошибок, которые исправляет код, лежащий в основе криптосистемы. Чем больше ошибок исправляет код, тем выше скорость передачи криптосистемы. Чтобы увеличить скорость передачи, В.М. Сидельников [3] в 1994 году предложил использовать коды Рида–Маллера $RM(r, m)$.

^{1,2} Место работы: МГУ им. М. В. Ломоносова
e-mail: bor1m@mail.ru, ivchizhov@gmail.com

Кодом Рида–Маллера $RM(r, m)$ называется линейное пространство, которое состоит из вектор-значений Ω_f булевых функций $f(x_1, \dots, x_m)$, степень нелинейности которых (максимальная длина монома, входящего в полином Жегалкина функции f) не превосходит r . Под вектор-значением булевой функции $f(x_1, \dots, x_m)$ будем понимать двоичный вектор Ω_f длины $n = 2^m$

$$\Omega_f = (f(0, \dots, 0, 0), f(0, \dots, 0, 1), f(0, \dots, 1, 0), \dots, f(1, \dots, 1, 1)).$$

Далее для простоты изложения не будем делать различий в обозначении между булевой функцией f и ее вектор-значением Ω_f .

Известно [4], что код $RM(r, m)$ имеет размерность $k = \sum_{i=0}^r \binom{m}{i}$, длину $n = 2^m$ и кодовое расстояние (минимальный вес ненулевых векторов кода) $d = 2^{m-r}$.

В 2007 году Л. Миндера и А. Шокроллахи [5] построили структурную атаку на вариант криптосистемы Мак-Элиса, предложенный В. М. Сидельниковым. Структурная атака предполагает восстановление секретного ключа криптосистемы по ее открытому ключу. Секретным ключом криптосистемы Мак-Элиса, построенной на основе кода Рида–Маллера $RM(r, m)$ с параметрами r и m , является пара (H, σ) . Здесь H — невырожденная $(k \times k)$ -матрица над полем $F_2 = \{0, 1\}$, которая выбирается случайно и равномерно из множества всех двоичных невырожденных $(k \times k)$ -матриц, а σ — подстановка на множестве координат кодовых слов кода $RM(r, m)$. При этом k — размерность кода $RM(r, m)$, а n — его длина.

Еще несколько слов о подстановке σ . Обычно подстановка σ моделируется матрицей, имеющей размеры $n \times n$, в каждой строчке и в каждом столбце которой стоит только одна единица. В дальнейшем будем обозначать результат применения подстановки σ к вектору a длины n как a^σ , т. е. если $a = (a_1, a_2, \dots, a_n)$, то $a^\sigma = (a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)})$, а результат применения этой же подстановки к каждому вектору из некоторого множества векторов C длины n — это множество $C^\sigma = \{c^\sigma \mid c \in C\}$.

Открытым ключом криптосистемы Мак-Элиса является матрица $G = H \cdot R \cdot \sigma$. Здесь подстановка из секретного ключа σ моделируется соответствующей матрицей, а R — порождающая матрица кода Рида–Маллера $RM(r, m)$, которая состоит из единичного вектора и вектор-значений всех мономов от m переменных степени нелинейности, не превосходящей r :

$$R = \begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_r \end{pmatrix},$$

где $G_0 = \Omega_1 = (1, 1, \dots, 1)$,

$$G_1 = \begin{pmatrix} \Omega_{x_m} \\ \vdots \\ \Omega_{x_2} \\ \Omega_{x_1} \end{pmatrix}, G_2 = \begin{pmatrix} \Omega_{x_{m-1}x_m} \\ \vdots \\ \Omega_{x_1x_3} \\ \Omega_{x_1x_2} \end{pmatrix}, G_r = \begin{pmatrix} \Omega_{x_{m-r+1}x_{m-r+2} \dots x_m} \\ \vdots \\ \Omega_{x_1x_2 \dots x_{r-1}x_{r+1}} \\ \Omega_{x_1x_2 \dots x_{r-1}x_r} \end{pmatrix}.$$

Заметим, что $H \cdot R$ — базис кода $RM(r, m)$, поэтому матрица G представляет собой базис кода $RM^\sigma(r, m)$, т. е. она является порождающей матрицей этого кода.

Структурная атака на криптосистему Мак-Элиса предполагает поиск такой матрицы H' и такой подстановки σ' , что $H' \cdot G \cdot \sigma' = R$. А для этого достаточно найти

такую подстановку σ' , что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$, так как тогда $G' = G \cdot \sigma'$ — порождающая матрица кода $RM(r, m)$ и для поиска матрицы H' достаточно будет решить систему линейных алгебраических уравнений $H'G' = R$.

Фактически Л. Миндер и А. Шокроллахи предложили алгоритм поиска по коду $RM^\sigma(r, m)$ такой подстановки σ' , что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Опишем типовую схему атаки на криптосистему Мак-Элиса, предложенную Л. Миндером и А. Шокроллахи.

Шаг 1. По коду $RM^\sigma(r, m)$ построить код $RM^\sigma(r - 1, m)$.

Шаг 2. Повторять шаг 1 до тех пор, пока не будет построен код $RM^\sigma(1, m)$.

Шаг 3. Найти такую подстановку σ' , что $RM^{\sigma \cdot \sigma'}(1, m) = RM(1, m)$. Тогда найденная подстановка σ' будет искомой, то есть удовлетворять условию

$$RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m).$$

Шаг 4. Зная подстановку σ' , восстановить матрицу H' .

При этом редукцию на шаге 1 от кода $RM^\sigma(r, m)$ к коду $RM^\sigma(r - 1, m)$ предлагается осуществлять следующим образом. Известно [4], что существует базис кода $RM^\sigma(r - 1, m)$, состоящий из слов минимального веса этого кода, а слово минимального веса этого кода является произведением двух слов минимального веса кода $RM^\sigma(r - 1, m)$. Тогда необходимо набрать достаточное число слов минимального веса кода $RM^\sigma(r, m)$ и построить с помощью них базис для кода $RM^\sigma(r - 1, m)$. Но в общем случае задача поиска слова минимального веса в коде является $\mathbb{NP}$ -трудной, и ожидаемая сложность атаки будет слишком большой. Справедливо следующее утверждение Л. Миндера и А. Шокроллахи [5].

Утверждение 1. *Существует алгоритм со сложностью $\exp((\log_2(n))^r C_r(1 + o(1)))$, где $n = 2^m$, C_r — константа, не зависящая от n , который по коду $RM^\sigma(r, m)$ строит код $RM^\sigma(r - 1, m)$.*

Фактически сложность всей атаки Л. Миндера и А. Шокроллахи будет определяться сложностью редукции на первом шаге, так как

- на каждой итерации шага 2 величина r уменьшается,
- на шаге 4 решается система линейных уравнений, и поэтому его сложность равна $O(n^3)$ битовых операций,
- шаг 3 алгоритма, в силу следующей теоремы, требует $O(n^3)$ битовых операций.

Теорема 1. *Существует алгоритм со сложностью $O(n^3)$ битовых операций, где $n = 2^m$, который по порождающей матрице кода $RM^\sigma(1, m)$ строит такую перестановку σ' , что*

$$RM^{\sigma \cdot \sigma'}(1, m) = RM(1, m).$$

Доказательство. Пусть G — произвольная порождающая $((m + 1) \times 2^m)$ -матрица кода $RM^\sigma(1, m)$, содержащая единичную строку. Пусть G' — $(m \times 2^m)$ -матрица, получающаяся из G удалением этой строки. В матрице G' имеется 2^m столбцов длины m . Значит, либо в этой матрице имеются два одинаковых столбца, либо все

столбцы различны, т. е. она состоит из всех возможных двоичных вектор-столбцов длины m .

В матрице G' не может быть одинаковых столбцов. Предположим обратное, тогда и в матрице G найдутся два одинаковых столбца. А значит, в коде, ортогональном к коду $RM^\sigma(1, m)$, будет лежать вектор веса 2, что невозможно, так как его кодовое расстояние равно $d = 2^2 > 2$. Итак, в матрице G' нет двух одинаковых столбцов. Возьмём в качестве σ' подстановку, которая упорядочивает столбцы матрицы G в порядке возрастания чисел, двоичными представлениями которых являются столбцы матрицы G' (старшие биты сверху). Под действием подстановки σ' матрица G , очевидно, перейдет в порождающую матрицу R кода $RM(1, m)$ (с точностью до перестановки строк). Такую подстановку можно найти, выполнив сортировку столбцов матрицы G' . Сложность сортировки равна $O(n \log_2 n)$. Остается из произвольной порождающей матрицы G кода $RM^\sigma(1, m)$ получить матрицу, содержащую строку из единиц. Для этого достаточно решить систему линейных уравнений:

$$(a_1 \dots a_{m+1}) \cdot G = (1 \dots 1).$$

Тогда матрица AG , где

$$A = \begin{pmatrix} a_1 & \dots & a_{m+1} \\ a_1 \oplus 1 & \dots & a_{m+1} \\ \vdots & \dots & \vdots \\ a_1 & \dots & a_{m+1} \oplus 1 \end{pmatrix},$$

будет искомой. Для решения системы линейных уравнений и вычисления произведения матриц требуется $O(n^3)$ операций.

В настоящей работе предлагается другой подход к выполнению редукции первого шага алгоритма Л. Миндера и А. Шокроллахи.

Теорема 2. *Существует алгоритм, который по кодам $RM^\sigma(r_1, m)$ и $RM^\sigma(r_2, m)$ строит код $RM^\sigma(r_1 + r_2, m)$ и имеет сложность $O(n^4)$ битовых операций, где $n = 2^m$ — длина рассматриваемых кодов.*

Доказательство. Рассмотрим базис $\{f_1, f_2, \dots, f_{k_1}\}$ кода $RM^\sigma(r_1, m)$ и базис $\{g_1, g_2, \dots, g_{k_2}\}$ кода $RM^\sigma(r_2, m)$. Результат покоординатного умножения двух вектор-значений Ω_{f_i} и Ω_{g_j} есть вектор-значение $\Omega_{f_i g_j}$, соответствующий функции $f_i g_j$. Напомним, что между булевой функцией и ее вектор-значением не делается различий.

Рассмотрим код C , который является линейной оболочкой векторов $f_i g_j$, где $1 \leq i \leq k_1$, $1 \leq j \leq k_2$:

$$\{f_1 g_1, f_1 g_2, \dots, f_1 g_{k_2}, f_2 g_1, \dots, f_2 g_{k_2}, \dots, f_{k_1} g_1, \dots, f_{k_1} g_{k_2}\}.$$

Докажем, что построенный код совпадает с кодом $RM^\sigma(r_1 + r_2, m)$. С одной стороны $C \subseteq RM^\sigma(r_1 + r_2, m)$, так как степень произведения $(f_i)^{\sigma^{-1}}(g_j)^{\sigma^{-1}}$, $1 \leq i \leq k_1$, $1 \leq j \leq k_2$, не превосходит суммы степеней функций, входящих в него, т. е.

$$\deg((f_i)^{\sigma^{-1}}(g_j)^{\sigma^{-1}}) \leq \deg(f_i^{\sigma^{-1}}) + \deg(g_j^{\sigma^{-1}}) \leq r_1 + r_2, \quad 1 \leq i \leq k_1, 1 \leq j \leq k_2.$$

Докажем обратное включение. Для этого оценим снизу размерность кода C . Так как размерность кода не изменяется от применения к нему операции подстановки,

достаточно оценить размерность кода $C^{\sigma^{-1}}$. Этот код является линейной оболочкой векторов $(f_i)^{\sigma^{-1}}(g_j)^{\sigma^{-1}} = f'_i \cdot g'_j$, $1 \leq i \leq k_1$, $1 \leq j \leq k_2$. При этом $\{f'_1, f'_2, \dots, f'_{k_1}\}$ — базис кода $RM(r_1, m)$, а $\{g'_1, g'_2, \dots, g'_{k_2}\}$ — базис кода $RM(r_2, m)$. Не ограничивая общности, будем считать, что $r_1 \leq r_2$. Докажем, что код $C^{\sigma^{-1}}$ содержит следующие линейно независимые векторы:

$$\{1, \{x_{j_1} x_{j_2} \dots x_{j_s}\}_{s=1, \dots, r_1+r_2, 1 \leq j_1 < j_2 < \dots < j_s \leq m}\}.$$

Число этих векторов равно

$$\sum_{i=0}^{r_1+r_2} \binom{m}{i} = \dim RM(r_1 + r_2, m).$$

Значит, в этом случае $\dim C = \dim C^{\sigma^{-1}} \geq \dim RM(r_1 + r_2, m) = \dim RM^{\sigma}(r_1 + r_2, m)$ и $C = RM^{\sigma}(r_1 + r_2, m)$.

Рассмотрим вектор $f \in \{1, x_{i_1} x_{i_2} \dots x_{i_t}, 1 \leq t \leq r_1, 1 \leq i_1 < i_2 < \dots < i_t \leq m\}$. Он лежит как в коде $RM(r_1, m)$, так и в коде $RM(r_2, m)$, поэтому его можно разложить по базисам этих кодов:

$$f = \sum_{i=1}^{k_1} \alpha_i f'_i = \sum_{j=1}^{k_2} \beta_j g'_j.$$

Тогда справедлива цепочка равенств

$$f = f \cdot f = \sum_{i=1}^{k_1} \alpha_i f'_i \cdot \sum_{j=1}^{k_2} \beta_j g'_j = \sum_{i,j} \alpha_i \beta_j f'_i g'_j.$$

Так как $f'_i g'_j \in C^{\sigma^{-1}}$, то вектор f также принадлежит коду $C^{\sigma^{-1}}$.

Рассмотрим вектор $f \in \{x_{i_1} \dots x_{i_t}, r_1 + 1 \leq t \leq r_1 + r_2, 1 \leq i_1 < \dots < i_t \leq m\}$. Тогда f можно представить в виде

$$f = x_{i_1} x_{i_2} \dots x_{i_{r_1}} x_{i_{r_1+1}} \dots x_{i_t}.$$

При этом $x_{i_1} x_{i_2} \dots x_{i_{r_1}} \in RM(r_1, m)$, а $x_{i_{r_1+1}} \dots x_{i_t} \in RM(r_2, m)$, так как $1 \leq t - r_1 \leq r_2$. Значит, справедливы разложения

$$x_{i_1} x_{i_2} \dots x_{i_{r_1}} = \sum_{i=1}^{k_1} \alpha_i f'_i, \quad x_{i_{r_1+1}} \dots x_{i_t} = \sum_{j=1}^{k_2} \beta_j g'_j.$$

Отсюда получаем

$$f = \sum_{i=1}^{k_1} \alpha_i f'_i \cdot \sum_{j=1}^{k_2} \beta_j g'_j = \sum_{i,j} \alpha_i \beta_j f'_i g'_j.$$

Так как $f'_i g'_j \in C^{\sigma^{-1}}$, то вектор f также принадлежит коду $C^{\sigma^{-1}}$.

Осталось оценить число операций, которое необходимо для построения кода $RM^{\sigma}(r_1 + r_2, m)$. Пусть $\{f_1, f_2, \dots, f_{k_1}\}$ — произвольный базис кода $RM^{\sigma}(r_1, m)$, $\{g_1, g_2, \dots, g_{k_2}\}$ — произвольный базис кода $RM^{\sigma}(r_2, m)$, и пусть $L = \{h_1, h_2, \dots, h_k\}$ состоит из всех линейно независимых произведений $f_i \cdot g_j$, $1 \leq i \leq k_1$, $1 \leq j \leq k_2$. По

построению линейная оболочка L совпадает с C . Итак, для построения кода C достаточно построить множество L , которое является его базисом. Будем формировать L следующим образом. Пусть сначала $L = \{f_1g_1\}$ (предполагается, что $f_1g_1 \neq 0$; если это не так, то надо, последовательно перебирая произведения f_ig_j , найти первый ненулевой вектор). Добавим к L вектор f_1g_2 и найдем ранг системы $\{f_1g_1, f_1g_2\}$, записав ее в виде матрицы и приведя потом эту матрицу к верхнетреугольному виду. Для этого требуется 1 побитовое сложение двух векторов. Если в результате ранг будет меньше 2, т. е. система оказалась линейно зависимой, то удалим вектор f_1g_2 из L и перейдем к следующему вектору, повторив приведение к верхнетреугольному виду. Пусть мы рассмотрели x_1 векторов до получения линейно независимой системы из двух векторов. Тогда будет выполнено не более x_1 сложений векторов длины n . Совершенно аналогично построим систему из трех линейно независимых векторов. Так как система из первых двух векторов уже приведена к верхнетреугольному виду, то в процессе приведения системы из трех векторов к верхнетреугольному виду потребуется 2 сложения векторов длины n . Пусть мы рассмотрели x_2 кандидатов на третий вектор, тогда всего было сделано $2x_2$ сложений векторов длины n . Продолжая рассуждения, можно заключить, что сложность построения полного базиса кода L потребует

$$N = \sum_{i=1}^{k(1,2)-1} i \cdot x_i$$

сложений векторов длины n , где $k(1,2)$ — размерность кода $RM^\sigma(r_1 + r_2, m)$. Поскольку общее число рассмотренных векторов не может быть больше числа произведений f_ig_j , $\sum_{j=1}^{k(1,2)-1} x_j \leq k_1 \cdot k_2$, получаем оценку для N :

$$N \leq k(1,2) \cdot \sum_{i=1}^{k(1,m)-1} x_i \leq k(1,2) \cdot k_1 \cdot k_2.$$

Так как $k(1,2), k_1, k_2 \leq n$, то $L \leq n^3$. Тогда число операций над битами для построения базиса имеет порядок $O(N \cdot n) = O(n^4)$.

На основании теоремы 2 можно ввести операцию $RM^\sigma(r_1, m) \odot RM^\sigma(r_2, m)$ следующим образом. Рассмотрим базис $\{f_1, f_2, \dots, f_{k_1}\}$ кода $RM^\sigma(r_1, m)$ и базис $\{g_1, g_2, \dots, g_{k_2}\}$ кода $RM^\sigma(r_2, m)$. Обозначим через $RM^\sigma(r_1, m) \odot RM^\sigma(r_2, m)$ код C , который является линейной оболочкой векторов f_ig_j , где $1 \leq i \leq k_1, 1 \leq j \leq k_2$:

$$\{f_1g_1, f_1g_2, \dots, f_1g_{k_2}, f_2g_1, \dots, f_2g_{k_2}, \dots, f_{k_1}g_1, \dots, f_{k_1}g_{k_2}\}.$$

В силу теоремы 2 введенная операция не зависит от выбора базисов кода и к тому же

$$RM^\sigma(r_1, m) \odot RM^\sigma(r_2, m) = RM^\sigma(r_1 + r_2, m).$$

Теорема 3. *Существует алгоритм, который по коду $RM^\sigma(r, m)$ строит код $RM^\sigma(m - r - 1, m)$ со сложностью $O(n^3)$, где n — длина кода $RM(r, m)$.*

Доказательство. Известно [4], что порождающая матрица $(R^\sigma)^\perp$ кода $(RM^\sigma(r, m))^\perp = RM^\sigma(m - r - 1, m)$ может быть построена путем применения алгоритма гауссовского исключения к порождающей матрице R^σ кода $RM^\sigma(r, m)$. Сложность этого алгоритма оценивается величиной $O(n^3)$, где n — длина кода $RM^\sigma(r, m)$.

Итак, можно рассмотреть следующие операции:

- (1) Умножение $\odot$ кодов $RM^\sigma(r_1, m)$ и $RM^\sigma(r_2, m)$:
 $RM^\sigma(r_1, m) \odot RM^\sigma(r_2, m) = RM^\sigma(r_1 + r_2, m)$.
- (2) Взятие ортогонального кода $\perp$ к коду $RM^\sigma(r, m)$:
 $(RM^\sigma(r, m))^\perp = RM^\sigma(m - r - 1, m)$.

С помощью них можно получать из кода $RM^\sigma(r, m)$ новые коды $RM^\sigma(t \neq r, m)$. Например, $RM^\sigma(r, m) \odot RM^\sigma(r, m) = RM^\sigma(2r, m)$, $(RM^\sigma(2r, m))^\perp = RM^\sigma(m - 2r - 1, m)$, и так далее.

Кроме того, можно рассматривать суперпозицию указанных операций.

Определение 1. Пусть $U = \{x \odot y, x^\perp\}$. Множество формул над U описывается следующими условиями.

- (1) Элемент $u \in U$ является формулой над U глубины 1.
- (2) Пусть $v(x_1, x_2, \dots, x_p)$ — формула над U глубины s . Тогда $x_{p+1} \odot v$ и $v^\perp$, где x_{p+1} — символ переменной, являются формулами над U глубины $s + 1$.
- (3) Других формул нет.

Определение 2. Замыканием $[RM^\sigma(r, m)]$ кода $RM^\sigma(r, m)$ называется множество всех кодов $RM^\sigma(t, m)$, которые могут быть представлены в виде

$$RM^\sigma(t, m) = v(RM^\sigma(r, m), RM^\sigma(r, m), \dots, RM^\sigma(r, m)),$$

где $v(x_1, \dots, x_p)$ — формула над U .

Изучим множество $[RM^\sigma(r, m)]$.

Утверждение 2. Код $RM^\sigma(t, m)$, $1 \leq t \leq m - 2$, принадлежит $[RM^\sigma(r, m)]$ тогда и только тогда, когда существуют такие целые числа a и $b \neq 0$, что $t = a \cdot (m - 1) + b \cdot r$.

Доказательство. Докажем, что если $RM^\sigma(t, m) \in [RM^\sigma(r, m)]$, то найдутся такие целые числа a и $b \neq 0$, что $t = a \cdot (m - 1) + b \cdot r$. Воспользуемся индукцией по глубине формулы. Если $RM^\sigma(t, m)$ получено из $RM^\sigma(r, m)$ формулой глубины 1, то либо $RM^\sigma(t, m) = (RM^\sigma(r, m))^\perp = RM^\sigma(m - r - 1, m)$, либо $RM^\sigma(t, m) = RM^\sigma(r, m) \odot RM^\sigma(r, m) = RM^\sigma(2r, m)$. Таким образом, утверждение для кодов, полученных применением формул глубины 1, выполняется.

Пусть утверждение верно для всех кодов $RM^\sigma(t, m)$, полученных из $RM^\sigma(r, m)$ применением формул глубины не больше $s - 1$. Докажем утверждение для всех $RM^\sigma(t, m)$, полученных из $RM^\sigma(r, m)$ применением формул глубины s . Возможны два случая:

- (1) Код $RM^\sigma(t, m) = RM^\sigma(t', m) \odot RM^\sigma(t'', m)$, где коды $RM^\sigma(t', m)$ и $RM^\sigma(t'', m)$ получаются из $RM^\sigma(r, m)$ с помощью формул глубины не больше $s - 1$. Тогда по предположению индукции существуют такие целые числа $a', b' \neq 0, a'', b'' \neq 0$, что $t' = a'(m - 1) + b'r$ и $t'' = a''(m - 1) + b''r$. Из определения операции $\odot$ получаем, что $t = (a' + a'')(m - 1) + (b' + b'')r$. Пусть $b' + b'' = 0$. Тогда $t = (a' + a'')(m - 1)$ и $t > m - 2$, либо $t \leq 0$, а значит, операция $\odot$ не могла быть применена к кодам $RM^\sigma(t', m)$ и $RM^\sigma(t'', m)$. Утверждение в этом случае верно.

- (2) Код $RM^\sigma(t, m) = (RM^\sigma(t', m))^\perp$, где код $RM^\sigma(t', m)$ получается из $RM^\sigma(r, m)$ с помощью формул глубины не больше $s - 1$. Тогда по предположению индукции существуют такие целые числа $a', b' \neq 0$, что $t' = a'(m - 1) + b'r$. Из определения операции $\perp$ получаем, что $t = m - 1 - a'(m - 1) - b'r = (-a' + 1)(m - 1) + (-b')r$, то есть утверждение в этом случае также верно.

Докажем обратное, т.е. если найдутся целые числа a и $b \neq 0$, для которых $t = a \cdot (m - 1) + b \cdot r$, то $RM^\sigma(t, m) \in [RM^\sigma(r, m)]$. Возможно четыре случая:

- (1) $a \geq 0, b > 0$. Учитывая, что $1 \leq t \leq m - 2$, получаем $a(m - 1) + br \leq m - 2$. Значит, $br \leq (1 - a)(m - 1) - 1$. Если $a \geq 1$, то

$$br \leq -((a - 1)(m - 1) + 1) \leq 0,$$

поэтому $b = 0$, что невозможно по условию. Итак, $a = 0$. Тогда t имеет вид $t = br \leq m - 2$. Значит, $RM^\sigma(t, m)$ получается b -кратным применением операции $\odot$ к коду $RM^\sigma(r, m)$:

$$RM^\sigma(t, m) = \underbrace{RM^\sigma(r, m) \odot RM^\sigma(r, m) \odot \dots \odot RM^\sigma(r, m)}_b.$$

В этом случае утверждение доказано.

- (2) $a \geq 0, b < 0$. Представим число $b' = -b > 0$ в виде $b' = q \cdot a - s$, где q, s — неотрицательные целые числа и $0 \leq s \leq a - 1$. Тогда

$$t = a(m - 1) - b'r = a(m - 1 - qr) + sr.$$

Так как $s, r \geq 0$ и $t \leq m - 2$, то $0 < a(m - 1 - qr) \leq m - 2$. Значит, $0 < m - 1 - qr \leq m - 2$ и $1 \leq qr \leq m - 2$. Итак, с помощью операции $\odot$ можно получить код $RM^\sigma(qr, m)$, применив к которому операцию $\perp$, можно получить код $RM^\sigma(m - 1 - qr, m)$. Теперь и к этому коду можно применить операцию $\odot$. Тогда получим код $RM^\sigma(a(m - 1 - qr), m)$. Осталось доказать, что можно из $RM^\sigma(r, m)$ получить код $RM^\sigma(sr, m)$. Тогда искомым код $RM^\sigma(t, m)$ можно получить с помощью операции $\odot$:

$$RM^\sigma(a(m - 1 - qr), m) \odot RM^\sigma(sr, m) = RM^\sigma(t, m).$$

Так как $m - 1 - qr, a > 0$ и $t \leq m - 2$, то $0 \leq sr \leq m - 2$, а значит, код $RM^\sigma(sr, m)$ выражается следующим образом:

$$RM^\sigma(sr, m) = \underbrace{RM^\sigma(r, m) \odot RM^\sigma(r, m) \odot \dots \odot RM^\sigma(r, m)}_s.$$

- (3) $a \leq 0, b < 0$. Так как $t = a(m - 1) + br \leq 0$, то этот случай невозможен.
- (4) $a \leq 0, b > 0$. Рассмотрим код $RM^\sigma(m - 1 - t, m) = RM^\sigma((1 - a)(m - 1) - br, m)$. Для него $(1 - a) \geq 0$ и $(-b) < 0$. Как и в случае 2, можно получить код $RM^\sigma(m - 1 - t, m)$, применение к которому операции $\perp$ дает требуемый код.

Утверждение 3. Пусть

$$t_{\min}(r, m) = \min_{RM^\sigma(t, m) \in [RM^\sigma(r, m)]} t.$$

Справедливо равенство $t_{\min}(r, m) = \text{НОД}(r, m - 1)$.

Доказательство. В силу утверждения 2 множество $[RM^\sigma(r, m)]$ состоит из всех кодов $RM^\sigma(t, m)$, для которых существуют такие целые числа a и b , $b \neq 0$, что

$$t = a(m - 1) + br.$$

Очевидно, что $d = \text{НОД}(r, m - 1)$ обладает этим свойством, значит, $RM^\sigma(d, m) \in [RM^\sigma(r, m)]$. Пусть $RM^\sigma(t, m) \in [RM^\sigma(r, m)]$ и $t < d$. Так как d делит $m - 1$ и делит r , то d делит t , что невозможно.

Утверждение 4. Пусть $\text{НОД}(r, m - 1) = d$. Тогда существует алгоритм, который по коду $RM^\sigma(r, m)$ строит код $RM^\sigma(d, m)$ со сложностью $O(n^4 \log_2 n)$.

Доказательство. В силу утверждения 3 из кода $RM^\sigma(r, m)$ можно с помощью операций $\odot$ и $\perp$ получить код $RM^\sigma(d, m)$, где $d = \text{НОД}(r, m - 1)$. Вычислим битовую сложность такого построения. Так как $RM^\sigma(d, m) \in [RM^\sigma(r, m)]$, то из утверждения 2 следует, что найдутся такие два целых числа a и $b \neq 0$, что

$$d = a(m - 1) + br.$$

Можно считать, что $|b| \leq m - 1$. В противном случае представим $|b|$ в виде $b = a'(m - 1) + b'$, где $|b'| \leq m - 1$ и перейдем к новому представлению: $d = (a + a'r)(m - 1) + b'r$. Как и в утверждении 2, рассмотрим случаи.

- (1) $a \geq 0$, $b > 0$. Как следует из доказательства утверждения 2, в этом случае $d = br$. Значит, d делится на r , поэтому исходный код $RM^\sigma(r, m)$ является кодом $RM^\sigma(d, m)$.
- (2) $a \geq 0$, $b < 0$. Как следует из доказательства утверждения 2, в этом случае $d = a(m - 1 - qr) + sr$, $0 < m - 1 - qr \leq m - 2$, $1 \leq sr \leq m - 2$. Итак, с помощью операции $\odot$ можно получить код $RM^\sigma(qr, m)$, применив к которому операцию $\perp$, можно получить код $RM^\sigma(m - 1 - qr, m)$. В силу утверждений 2 и 3 для этого требуется $O((q - 1)n^4 + n^3)$ операций. Теперь, применив операцию $\odot$ к полученному коду, построим код $RM^\sigma(a(m - 1 - qr), m)$ за $O((q - 1 + a - 1)n^4 + n^3)$ операций. Код $RM^\sigma(sr, m)$ можно построить за $O((s - 1)n^4)$ операций, значит, искомым код $RM^\sigma(d, m)$ можно построить за $O((q + a + s - 2)n^4 + n^3)$ операций. Учитывая, что $s < a$ и $q \leq |b|$, получим, что общее число операций равно

$$O((|b| + 2a)n^4).$$

Так как $b \leq m - 1 < m$ и $a = \frac{d + |b|r}{m - 1} \leq \frac{r + (m - 1)r}{m - 1} = \frac{rm}{m - 1} < m$, то сложность построения нужного кода в этом случае равна $O(mn^4) = O(n^4 \log_2 n)$.

- (3) $a \leq 0$, $b > 0$. Этот случай отличается от случая 2 дополнительным применением операции $\perp$; так как сложность этой операции равна $O(n^3)$, то общая сложность будет равна $O(n^4 \log_2 n)$.

Итак, в силу утверждения 4 по коду $RM^\sigma(r, m)$ можно эффективно за полиномиальное время построить код $RM^\sigma(d, m)$, где $d = \text{НОД}(r, m - 1)$. Используем этот факт для построения новой атаки на криптосистему Мак-Элиса.

Опишем типовую схему атаки.

Шаг 1. Используя операции $\odot$ и $\perp$, по коду $RM^\sigma(r, m)$ построить код $RM^\sigma(d, m)$, где $d = \text{НОД}(r, m - 1)$.

Шаг 2. По коду $RM^\sigma(d, m)$, используя алгоритм Л. Миндера и А. Шокроллахи, построить код $RM^\sigma(d - 1, m)$.

Шаг 3. Построить код

$$\begin{aligned} \left((RM^\sigma(d, m))^\perp \odot RM^\sigma(d - 1, m) \right)^\perp &= \\ &= (RM^\sigma(m - d - 1, m) \odot RM^\sigma(d - 1, m))^\perp = \\ &= (RM^\sigma(m - 2, m))^\perp = RM^\sigma(1, m). \end{aligned}$$

Шаг 4. Найти такую подстановку σ' , что $RM^{\sigma \cdot \sigma'}(1, m) = RM(1, m)$. Тогда найденная подстановка σ' будет искомой, то есть удовлетворять условию

$$RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m).$$

Шаг 5. Зная подстановку σ' , восстановить матрицу H' .

Следствием из утверждения 4 и теоремы 1 является следующая основная теорема о сложности предложенной атаки.

Теорема 4. Пусть $\text{НОД}(r, m - 1) = d > 1$. Тогда существует алгоритм со сложностью $\exp((\log_2(n))^d C_d(1 + o(1)))$ битовых операций, который по порождающей матрице кода $RM^\sigma(r, m)$ находит такую подстановку σ' , что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Доказательство. Самая трудоемкая часть описанного алгоритма — шаг 3, который согласно утверждению 1 имеет сложность $\exp((\log_2(n))^d C_d(1 + o(1)))$.

В случае, когда $\text{НОД}(r, m - 1) = 1$, шаги 2 и 3 атаки выполнять не требуется, а значит, атака на криптосистему в этом случае становится полиномиальной, а именно, справедлива следующая теорема.

Теорема 5. Пусть $\text{НОД}(r, m - 1) = 1$. Тогда существует алгоритм со сложностью $O(n^4 \log_2 n)$ битовых операций, который по порождающей матрице кода $RM^\sigma(r, m)$ находит такую подстановку σ' , что $RM^{\sigma \cdot \sigma'}(r, m) = RM(r, m)$.

Таким образом, в работе построен алгоритм, который восстанавливает секретный ключ криптосистемы Мак-Элиса, построенной на основе таких кодов Рида-Маллера $RM(r, m)$, что $\text{НОД}(r, m - 1) = 1$, за полиномиальное время от битовой длины секретного ключа. Для других параметров кода описанная атака имеет во многих случаях меньшую сложность, чем атака Миндера-Шокроллахи, которая до настоящего время являлась лучшей.

Список литературы

1. McEliece R. J., A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol.* (1978.) **January**, 114–116.
2. Н. Neiderreiter, Knapsack-type cryptosystems and algebraic coding theory. *Probl. of Control and Inf. Theory.* (1986) **15**, 159–166.

3. Сидельников В. М., Открытое шифрование на основе двоичных кодов Рида–Маллера. *Дискретная математика* (1994) **6**, №2, 3–20.
4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж., *Теория кодов, исправляющих ошибки*. Связь, Москва, 1979.
5. Minder L., Shokrollahi A., Cryptanalysis of the Sidelnikov cryptosystem. In: *Lect. Notes Comput. Sci.* (Advances in Cryptology — EUROCRYPT 2007), **4515**, 2007, pp. 347–360.

Статья поступила 15.11.2013.