Math-Net.Ru

Общероссийский математический портал

И. В. Чижов, Ключевое пространство криптосистемы Мак-Элиса–Сидельникова, *Дискрет. матем.*, 2009, том 21, выпуск 3, 132–159

DOI: <https://doi.org/10.4213/dm1066>

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: 54.209.52.79

26 апреля 2023 г., 12:03:07

Ключевое пространство криптосистемы Мак-Элиса–Сидельникова

© 2009 г. И. В. Чижов

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 г. Р. Дж. Мак-Элисом. Криптосистема Мак-Элиса основывается на NP -трудной проблеме в теории кодирования. В работе рассматривается некоторое обобщение криптосистемы Мак-Элиса, предложенное в 1994 г. В. М. Сидельниковым. Криптосистема Мак-Элиса–Сидельникова строится на основе u -кратного использования кодов Рида–Маллера $RM(r, m)$.

В работе исследуются вопросы, связанные с пространством эквивалентных секретных ключей новой криптосистемы, то есть секретных ключей, порождающих одинаковые открытые ключи. Исследуются вопросы структуры множества открытых ключей криптосистемы Мак-Элиса–Сидельникова для произвольного числа блоков. Для случая двух блоков ($u = 2$) описываются все классы эквивалентности секретных ключей с представителями особого вида.

1. Криптосистема Мак-Элиса–Сидельникова

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 году Р. Дж. Мак-Элисом [1]. Криптосистема Мак-Элиса относится к классу кодовых криптосистем, то есть криптосистем, стойкость которых опирается на сложность некоторых задач из теории кодов, исправляющих ошибки. Фундаментом криптосистемы Мак-Элиса является некоторый код, исправляющий ошибки. Для построения криптосистемы Мак-Элиса, вообще говоря, можно использовать любой код, исправляющий ошибки, однако, к нему нужно предъявить ряд требований, обеспечивающих необходимую стойкость криптосистемы и высокую скорость алгоритмов шифрования и расшифрования. В работе [1] Мак-Элис предложил использовать коды Гоппы. Иногда криптосистему Мак-Элиса, построенную на кодах Гоппы, называют оригинальной криптосистемой Мак-Элиса. В. М. Сидельников в работе [2] предложил использовать для построения криптосистемы двоичные коды Рида–Маллера $RM(r, m)$ и провел криптографический анализ такого варианта криптосистемы Мак-Элиса. В результате В. М. Сидельников пришел к выводу, что модификация криптосистемы Мак-Элиса, построенная на кодах Рида–Маллера, не обеспечивает необходимого уровня стойкости. В той же работе [2] автор предлагает усиленный вариант криптосистемы на основе кодов Рида–Маллера. Именно усиленный вариант криптосистемы Мак-Элиса на основе кодов Рида–Маллера в настоящей работе называется криптосистемой Мак-Элиса–Сидельникова. Опишем конструкцию, предложенную В. М. Сидельниковым.

Определение 1. Кодом Рида–Маллера $RM(r, m)$ называется множество вектор-значений Ω_f всех булевых функций $f(x_1, \dots, x_m)$, степень нелинейности (максимальная длина монома, входящего в полином Жегалкина функции f) которых не превосходит r , то есть

$$RM(r, m) = \left\{ \Omega_f = (z_1, \dots, z_n), \quad n = 2^m: \right. \\ \left. f(x_1, \dots, x_m) = a_0 \oplus \bigoplus_{s=1}^t \bigoplus_{1 \leq i_1 < \dots < i_s \leq m} a_{i_1, \dots, i_s} x_{i_1} \dots x_{i_s}, \quad t \leq r \right\}.$$

Известно, что код $RM(r, m)$ имеет размерность

$$k = \sum_{i=0}^r \binom{m}{i},$$

длину $n = 2^m$ и кодовое расстояние $d = 2^{m-r}$, (см. [6]). Всюду далее через R будем обозначать порождающую матрицу кода Рида–Маллера $RM(r, m)$. Будем полагать, что матрица R состоит из векторов значений всех мономов от m переменных степени нелинейности не выше r . К тому же, если перенумеровать сверху от 1 до k строки матрицы R , в строке с номером i , $2 \leq i \leq k$, стоит вектор значений монома $x_{i_1} x_{i_2} \dots x_{i_t}$, где i_j , $1 \leq j \leq t$, — номера позиций, в которых стоит единица в двоичном разложении числа $i - 1$, а в строке с номером 1 — вектор из всех единиц. Матрицу R такого вида будем называть стандартной порождающей матрицей кода Рида–Маллера $RM(r, m)$.

Как обычно, группу перестановок на множестве из n элементов будем обозначать S_n . С перестановками тесно связаны перестановочные матрицы, то есть такие матрицы, в каждой строке и в каждом столбце которых стоит ровно одна единица. В дальнейшем мы не будем делать различия между перестановочными матрицами и перестановками.

Опишем устройство криптосистемы Мак–Элиса–Сидельникова. Секретным ключом криптосистемы является кортеж $(H_1, H_2, \dots, H_u, \Gamma)$. Здесь $H_1, H_2, \dots, H_u$ — невырожденные $k \times k$ матрицы над полем $F_2 = \{0, 1\}$, которые выбираются случайно и равновероятно из множества $GL_k(F_2)$ всех двоичных невырожденных $k \times k$ матриц над полем F_2 . Матрица Γ — перестановочная $(un \times un)$ матрица.

Открытым ключом криптосистемы Мак–Элиса–Сидельникова является матрица

$$G' = (H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma,$$

где символом $\parallel$ обозначена конкатенация матриц по столбцам. Каждую матрицу $H_i R$ будем называть блоком, при этом $H_1 R$ — первым блоком, $H_2 R$ — вторым и так далее. Алгоритмы шифрования и расшифрования подробно описаны в [2].

Для кодов Рида–Маллера существуют эффективные алгоритмы декодирования в пределах кодового расстояния [6], а это обуславливает высокую скорость расшифрования. Заметим также, что существуют хорошие алгоритмы декодирования кодов Рида–Маллера и при числе ошибок, превосходящем половину кодового расстояния [8], что позволяет увеличить скорость передачи в криптосистеме.

2. Структура множества открытых ключей криптосистемы Мак-Элиса–Сидельникова для произвольного числа блоков

Одно из самых первых направлений исследования новой криптосистемы — изучение множества открытых ключей. Обозначим через $\mathcal{C}$ множество всех открытых ключей криптосистемы Мак-Элиса–Сидельникова.

Введем ряд необходимых в дальнейшем определений.

Определение 2. Группой автоморфизмов $\text{Aut}(\mathcal{C})$ некоторого линейного двоичного кода $\mathcal{C}$ с порождающей матрицей G называется множество перестановок (или перестановочных матриц, что тоже самое) P , для которых существует невырожденная матрица A (для каждой перестановки — своя матрица) такая, что $GP = AG$.

В дальнейшем не будем делать различий между перестановкой и соответствующей ей перестановочной матрицей. Кроме того, если P — перестановка, то в некоторых случаях будет удобней использовать обозначение G^P вместо GP .

Определение 3. Про невырожденную матрицу A будем говорить, что она задает автоморфизм линейного двоичного кода $\mathcal{C}$ с порождающей матрицей G , если существует перестановка P такая, что $AG = GP$.

Предложение 1. Пусть в порождающей матрице G кода $\mathcal{C}$ нет одинаковых столбцов. Тогда можно установить взаимно однозначное соответствие между матрицами, задающими автоморфизм кода $\mathcal{C}$, и группой автоморфизмов $\text{Aut}(\mathcal{C})$ этого кода.

Доказательство. Поставим в соответствие перестановке P из $\text{Aut}(\mathcal{C})$ такую матрицу A , что $GP = AG$. В силу определения автоморфизма подобная матрица существует. В силу определения матрицы, задающей автоморфизм, такое отображение является сюръективным.

Осталось доказать, что для любых $P_1 \neq P_2$ соответствующие им матрицы A_1 и A_2 различны. Действительно, пусть $A_1 = A_2$, тогда $GP_1 = A_1G = A_2G = GP_2$. Следовательно, $GP_1P_2^{-1} = G$. В порождающей матрице G кода $\mathcal{C}$ нет одинаковых столбцов, поэтому $P_1 = P_2$. Что и требовалось доказать.

В порождающей матрице кода Рида–Маллера $RM(r, m)$ нет одинаковых столбцов, поэтому предложение 1 справедливо для группы автоморфизмов кода Рида–Маллера.

В настоящий момент группа автоморфизмов известна для небольшого класса кодов. В частности, она полностью описана для кодов Рида–Маллера $RM(r, m)$.

Предложение 2. Для r , $1 \leq r \leq m - 2$, группа автоморфизмов кода Рида–Маллера $RM(r, m)$ совпадает с полной аффинной группой $GA(m)$, то есть

$$\text{Aut}(RM(r, m)) = GA(m).$$

Доказательство этого предложения можно найти в [6].

Рассмотрим некоторую перестановку P из группы автоморфизмов кода Рида–Маллера $RM(r, m)$. Построим, используя ее, i длинных перестановок $\mathcal{P}[i] \in S_{in}$ следующим образом. $\mathcal{P}[i](j) = j$ для любого $j \notin I = \{(i-1)n+1, (i-1)n+2, \dots, in\}$, а $\mathcal{P}[i](I) = P(I)$. Другими словами, перестановка $\mathcal{P}[i]$ в i -м блоке действует как перестановка P , а во всех остальных блоках — как единичная перестановка.

Определение 4. Группой расширенных автоморфизмов $\mathcal{A}_u(RM(r, m))$ кода Рида–Маллера $RM(r, m)$ назовем множество всех возможных произведений описанных перестановок $\mathcal{P}[i]$ для всех возможных i , $1 \leq i \leq u$, и всех возможных перестановок P из группы автоморфизмов кода Рида–Маллера.

Очевидны следующие свойства расширенных автоморфизмов.

Предложение 3. Для любых $\mathcal{P}[i]$ и $\mathcal{Q}[j]$, $i \neq j$, справедливо равенство

$$\mathcal{P}[i]\mathcal{Q}[j] = \mathcal{Q}[j]\mathcal{P}[i].$$

Пусть $\mathcal{P}[i]$ соответствует автоморфизму P , а $\mathcal{P}^{-1}[i]$ соответствует автоморфизму P^{-1} , тогда

$$(\mathcal{P}[i])^{-1} = \mathcal{P}^{-1}[i].$$

Дадим следующее определение эквивалентности секретных ключей в криптосистеме Мак–Элиса–Сидельникова.

Определение 5. Два секретных ключа $(H_1, H_2, \dots, H_u, \Gamma)$ и $(H'_1, H'_2, \dots, H'_u, \Gamma')$ назовем эквивалентными, если соответствующие им открытые ключи совпадают, то есть выполняется соотношение

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R) \Gamma'.$$

Заметим, что введенное отношение действительно является отношением эквивалентности. Тем самым все множество секретных ключей разбивается на классы эквивалентности и число классов эквивалентности совпадает с числом открытых ключей. Класс эквивалентности с представителем $(H_1, \dots, H_u, \Gamma)$ будем обозначать $[(H_1, \dots, H_u, \Gamma)]$.

Рассмотрим множество $\mathcal{G}(H_1, H_2, \dots, H_u)$, состоящее из перестановок $\Gamma \in S_{un}$, для которых существуют невырожденные двоичные матрицы $H'_1, H'_2, \dots, H'_u$ такие, что

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R).$$

Справедлива следующая теорема.

Теорема 1. Существует взаимно однозначное соответствие между классом эквивалентности $[(H_1, H_2, \dots, H_u, \Gamma)]$ и множеством $\mathcal{G}(H_1, H_2, \dots, H_u)$.

Доказательство. Для начала заметим, что тождественная перестановка Id принадлежит множеству $\mathcal{G}(H_1, H_2, \dots, H_u)$. Рассмотрим отображение f , переводящее любой ключ $(M_1, M_2, \dots, M_u, \Gamma')$ из класса эквивалентности $[(H_1, H_2, \dots, H_u, \Gamma)]$ в перестановку $\Gamma(\Gamma')^{-1}$. Из соотношения

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma = (M_1 R \parallel M_2 R \parallel \dots \parallel M_u R) \Gamma'$$

следует, что перестановка $\Gamma(\Gamma')^{-1}$ принадлежит множеству $\mathcal{G}(H_1, H_2, \dots, H_u)$.

Докажем, что f — инъекция. Пусть два секретных ключа $(A_1, A_2, \dots, A_u, \Gamma_1)$ и $(B_1, B_2, \dots, B_u, \Gamma_2)$ из рассматриваемого класса эквивалентности переводятся с помощью f в перестановки $\Gamma_1 \Gamma_1^{-1}$ и $\Gamma_2 \Gamma_2^{-1}$ соответственно так, что $\Gamma_1 \Gamma_1^{-1} = \Gamma_2 \Gamma_2^{-1}$. Тогда $\Gamma_1 = \Gamma_2$, а значит и $A_1 = B_1, A_2 = B_2, \dots, A_u = B_u$, то есть ключи совпадают.

Теперь рассмотрим некоторую перестановку Γ_g из множества $\mathcal{G}(H_1, H_2, \dots, H_u)$. Тогда для Γ_g найдутся такие матрицы $H'_1, H'_2, \dots, H'_u$, что

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma_g = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R).$$

Положим

$$\Gamma' = \Gamma_g^{-1} \Gamma, \quad M_1 = H'_1, \quad \dots, \quad M_u = H'_u.$$

В этом случае

$$(H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R) \Gamma_g^{-1} \Gamma = (H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma,$$

то есть секретный ключ $(M_1, M_2, \dots, M_u, \Gamma_g^{-1} \Gamma)$ эквивалентен $(H_1, H_2, \dots, H_u, \Gamma)$. Тем самым доказано, что отображение f сюръективно.

Итак, отображение f инъективно и сюръективно, а значит, f — взаимно однозначное отображение класса эквивалентности с представителем $(H_1, H_2, \dots, H_u, \Gamma)$ в множество $\mathcal{G}(H_1, H_2, \dots, H_u)$.

В процессе доказательства теоремы 1 было доказано следующее утверждение.

Предложение 4. *Класс эквивалентности $[(H_1, \dots, H_u, \Gamma)]$ состоит из ключей вида $(H'_1, \dots, H'_u, \Gamma_g \Gamma)$, где Γ_g^{-1} принадлежит множеству $\mathcal{G}(H_1, \dots, H_u)$ и*

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R) \Gamma_g.$$

Тем самым вопрос изучения эквивалентных секретных ключей сводится к описанию множеств $\mathcal{G}(H_1, \dots, H_u)$.

Установим некоторые свойства множества $\mathcal{G}(H_1, \dots, H_u)$.

Предложение 5. *Для любой невырожденной матрицы H справедливо равенство*

$$\mathcal{G}(H_1, H_2, \dots, H_u) = \mathcal{G}(HH_1, HH_2, \dots, HH_u).$$

Доказательство. Рассмотрим произвольную перестановку Γ из $\mathcal{G}(H_1, H_2, \dots, H_u)$. Для этой перестановки найдутся такие матрицы $H'_1, H'_2, \dots, H'_u$, что

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R).$$

Умножив последнее соотношение на любую невырожденную матрицу H , получим равенство

$$(HH_1 R \parallel HH_2 R \parallel \dots \parallel HH_u R) \Gamma = (HH'_1 R \parallel HH'_2 R \parallel \dots \parallel HH'_u R).$$

Отсюда следует, что перестановка Γ принадлежит множеству $\mathcal{G}(HH_1, HH_2, \dots, HH_u)$, то есть

$$\mathcal{G}(H_1, H_2, \dots, H_u) \subseteq \mathcal{G}(HH_1, HH_2, \dots, HH_u).$$

Легко показать и обратное включение. Действительно, рассмотрим перестановку Γ из множества $\mathcal{G}(HH_1, HH_2, \dots, HH_u)$. Тогда для нее будет справедливо соотношение

$$(HH_1 R \parallel HH_2 R \parallel \dots \parallel HH_u R) \Gamma = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R).$$

Умножив его на H^{-1} , получим равенство

$$(H_1 R \parallel H_2 R \parallel \dots \parallel H_u R) \Gamma = (H^{-1} H'_1 R \parallel H^{-1} H'_2 R \parallel \dots \parallel H^{-1} H'_u R).$$

А это и означает, что $\Gamma \in \mathcal{G}(H_1, H_2, \dots, H_u)$, следовательно,

$$\mathcal{G}(H_1, H_2, \dots, H_u) \supseteq \mathcal{G}(HH_1, HH_2, \dots, HH_u).$$

Предложение доказано.

Предложение 6. Пусть кортежи $(H_1, \dots, H_u)$ и $(M_1, \dots, M_u)$ таковы, что существует перестановка $P \in S_{un}$, для которой

$$(H_1 R \parallel \dots \parallel H_u R)P = (M_1 R \parallel \dots \parallel M_u R).$$

Тогда

$$\mathcal{G}(H_1, \dots, H_u) = P\mathcal{G}(M_1, \dots, M_u).$$

Доказательство. Рассмотрим перестановку Γ из множества $\mathcal{G}(H_1, \dots, H_u)$. Для нее найдутся матрицы $H'_1, \dots, H'_u$ такие, что

$$(H_1 R \parallel \dots \parallel H_u R)\Gamma = (H'_1 R \parallel \dots \parallel H'_u R).$$

С другой стороны,

$$(H_1 R \parallel \dots \parallel H_u R)P = (M_1 R \parallel \dots \parallel M_u R).$$

Поэтому

$$(M_1 R \parallel \dots \parallel M_u R)P^{-1}\Gamma = (H'_1 R \parallel \dots \parallel H'_u R).$$

Следовательно, $P^{-1}\Gamma \in \mathcal{G}(M_1, \dots, M_u)$, то есть $\Gamma \in P\mathcal{G}(M_1, \dots, M_u)$. Значит,

$$\mathcal{G}(H_1, \dots, H_u) \subseteq P\mathcal{G}(M_1, \dots, M_u).$$

Рассмотрим теперь перестановку $\Gamma = P\Gamma'$, $\Gamma' \in \mathcal{G}(M_1, \dots, M_u)$, другими словами, перестановка Γ принадлежит множеству $P\mathcal{G}(M_1, \dots, M_u)$. Для перестановки Γ' справедливо соотношение

$$(M_1 R \parallel \dots \parallel M_u R)\Gamma' = (M'_1 R \parallel \dots \parallel M'_u R).$$

Из условия следует, что

$$(H_1 R \parallel \dots \parallel H_u R)\Gamma = (H_1 R \parallel \dots \parallel H_u R)P\Gamma' = (M'_1 R \parallel \dots \parallel M'_u R).$$

А это означает, что $\Gamma \in \mathcal{G}(H_1, \dots, H_u)$. Отсюда

$$\mathcal{G}(H_1, \dots, H_u) \supseteq P\mathcal{G}(M_1, \dots, M_u).$$

Тем самым предложение доказано.

Из последнего предложения вытекает важное следствие.

Следствие 1. Пусть невырожденные $k \times k$ матрицы $D_1, D_2, \dots, D_u$ таковы, что существуют перестановки $P_1, P_2, \dots, P_u$ из группы автоморфизмов кода Риды–Маллера $RM(r, m)$, что

$$D_1 R = R P_1, \quad D_2 R = R P_2, \dots, D_u R = R P_u.$$

Пусть $\mathcal{P}_1[1], \mathcal{P}_2[2], \dots, \mathcal{P}_u[u]$ — перестановки из $\mathcal{A}_u(RM(r, m))$, соответствующие перестановкам $P_1, \dots, P_u$. Тогда

$$\mathcal{G}(E, \dots, E) = \mathcal{P}_1[1]\mathcal{P}_2[2] \dots \mathcal{P}_u[u]\mathcal{G}(D_1, \dots, D_u).$$

Следующее предложение в несколько другом виде было получено в [9].

Предложение 7. Множество $\mathcal{G}(E, \dots, E)$ состоит из перестановок вида $\Gamma\mathcal{P}$, где Γ такова, что $(R \parallel \dots \parallel R)\Gamma = (R \parallel \dots \parallel R)$, а $\mathcal{P}$ — перестановка из группы $\mathcal{A}_u(RM(r, m))$.

Доказательство. Рассмотрим любую перестановку Γ' из множества $\mathcal{G}(E, \dots, E)$. Для нее найдутся матрицы $H_1, \dots, H_u$ такие, что

$$(R \parallel \dots \parallel R)\Gamma' = (H_1 R \parallel \dots \parallel H_u R).$$

В матрице R нет одинаковых столбцов, поэтому матрицы $H_i R$ должны состоять из столбцов матрицы R , а значит матрицы H_i задают некоторый автоморфизм P_i , которому соответствует расширенный автоморфизм $\mathcal{P}_i[i]$. Значит, существует перестановка $\mathcal{P} \in \mathcal{A}_u(RM(r, m))$ такая, что

$$(R \parallel \dots \parallel R)\Gamma'\mathcal{P}^{-1} = (R \parallel \dots \parallel R).$$

Отсюда немедленно следует, что для перестановки $\Gamma'\mathcal{P}^{-1} = \Gamma$ справедливо равенство

$$(R \parallel \dots \parallel R)\Gamma = (R \parallel \dots \parallel R).$$

Тем самым

$$\Gamma' = \Gamma\mathcal{P}.$$

Несложно также проверить, что любая перестановка вида $\Gamma\mathcal{P}$ принадлежит множеству $\mathcal{G}(E, \dots, E)$. Этим завершается доказательство предложения.

В процессе доказательства предложения 7 было получено следующее утверждение.

Следствие 2. Класс эквивалентности $[(E, \dots, E, \Gamma)]$ состоит из таких ключей $(D_1, \dots, D_u, \mathcal{P}\Gamma)$, что матрицы D_i , $i = 1, \dots, u$, задают автоморфизм кода $RM(r, m)$, а перестановка $\mathcal{P} \in \mathcal{G}(E, \dots, E)$.

Объединяя предложение 5 и следствие 1, получим следующую основную теорему.

Теорема 2. Пусть невырожденные матрицы $D_1, D_2, \dots, D_u$ задают соответственно автоморфизмы $P_1, P_2, \dots, P_u$ кода $RM(r, m)$. Пусть $\mathcal{P}_1[1], \mathcal{P}_2[2], \dots, \mathcal{P}_u[u]$ — перестановки из $\mathcal{A}_u(RM(r, m))$, соответствующие перестановкам $P_1, \dots, P_u$, и пусть H — любая невырожденная матрица. Тогда

$$\mathcal{G}(E, \dots, E) = \mathcal{P}_1[1]\mathcal{P}_2[2] \dots \mathcal{P}_u[u]\mathcal{G}(HD_1, \dots, HD_u).$$

Последняя теорема вместе с предложением 4 дает полное описание класса эквивалентности секретного ключа $(HD_1, \dots, HD_u, \Gamma)$, где $H, D_1, \dots, D_u$ удовлетворяют условию теоремы, а Γ — некоторая перестановка.

Теорема 3. Пусть невырожденные матрицы $D_1, D_2, \dots, D_u$ задают соответственно автоморфизмы $P_1, P_2, \dots, P_u$ кода $RM(r, m)$. Пусть $\mathcal{P}_1[1], \mathcal{P}_2[2], \dots, \mathcal{P}_u[u]$ — перестановки из $\mathcal{A}_u(RM(r, m))$, соответствующие перестановкам $P_1, \dots, P_u$, и пусть H — любая невырожденная матрица.

Тогда класс эквивалентности $[(HD_1, HD_2, \dots, HD_u, \Gamma)]$ состоит из кортежей вида $(HA_1, HA_2, \dots, HA_u, \mathfrak{Q}_1^{-1}[1]\mathfrak{Q}_2^{-1}[2] \dots \mathfrak{Q}_u^{-1}[u]\Gamma'\mathcal{P}_1[1]\mathcal{P}_2[2] \dots \mathcal{P}_u[u]\Gamma)$, где $A_1, \dots, A_u$ задают автоморфизмы $Q_1, \dots, Q_u$ кода Ридса–Маллера $RM(r, m)$, $\mathfrak{Q}_1[1], \dots, \mathfrak{Q}_u[u]$, — соответствующие этим автоморфизмам расширенные автоморфизмы, а перестановка Γ' сохраняет матрицу $(R \parallel R \parallel \dots \parallel R)$, то есть

$$(R \parallel R \parallel \dots \parallel R)\Gamma' = (R \parallel R \parallel \dots \parallel R).$$

Доказательство. Класс эквивалентности $[(HD_1, HD_2, \dots, HD_u, \Gamma)]$, согласно предложению 4, состоит из кортежей $(H'_1, \dots, H'_u, \Gamma_g \Gamma)$, где $\Gamma_g^{-1} \in \mathcal{G}(HD_1, \dots, HD_u)$ и

$$(HD_1 R \parallel HD_2 R \parallel \dots \parallel HD_u R) \Gamma_g^{-1} = (H'_1 R \parallel H'_2 R \parallel \dots \parallel H'_u R).$$

Так как Γ_g^{-1} принадлежит множеству $\mathcal{G}(HD_1, HD_2, \dots, HD_u)$, в силу теоремы 2 Γ_g^{-1} представима в виде

$$\Gamma_g^{-1} = (\mathcal{P}_u[u])^{-1} (\mathcal{P}_{u-1}[u-1])^{-1} \dots (\mathcal{P}_1[1])^{-1} \Gamma_e,$$

где $\Gamma_e \in \mathcal{G}(E, E, \dots, E)$. В силу свойств расширенных автоморфизмов (см. предложение 3) перестановка Γ_g^{-1} может быть представлена в виде

$$\Gamma_g^{-1} = \mathcal{P}_1^{-1}[1] \mathcal{P}_2^{-1}[2] \dots \mathcal{P}_u^{-1}[u] \Gamma_e.$$

Далее, в силу предложения 7, перестановка Γ_e имеет вид

$$\Gamma_e = \Gamma' \mathcal{Q}_1[1] \mathcal{Q}_2[2] \dots \mathcal{Q}_u[u],$$

где $\mathcal{Q}_i[i]$, $1 \leq i \leq u$, — расширенные автоморфизмы, соответствующие некоторым автоморфизмам $Q_1, \dots, Q_u$, а перестановка Γ' сохраняет матрицу $(R \parallel R \parallel \dots \parallel R)$, то есть

$$(R \parallel R \parallel \dots \parallel R) \Gamma' = (R \parallel R \parallel \dots \parallel R).$$

Предположим теперь, что автоморфизмы $Q_1, \dots, Q_u$ соответствуют матрицам $A_1, \dots, A_u$. Тогда после применения перестановки Γ_g^{-1} к матрице $(HD_1 R \parallel HD_2 R \parallel \dots \parallel HD_u R)$ получим, что

$$(HD_1 R \parallel \dots \parallel HD_u R) \Gamma_g^{-1} = (HA_1 R \parallel \dots \parallel HA_u R) = (H'_1 R \parallel \dots \parallel H'_u R).$$

Последнее означает, что $H'_i = HA_i$, $1 \leq i \leq u$. Для завершения доказательства достаточно вычислить перестановку Γ_g , используя выражение для обратной перестановки Γ_g^{-1} , а также воспользоваться свойствами расширенных автоморфизмов и тем, что $(\Gamma')^{-1}$ сохраняет матрицу $(R \parallel R \parallel \dots \parallel R)$.

3. Классы эквивалентных ключей в случае $u = 2$

Согласно теореме 1 и предложению 5, для случая $u = 2$ задача поиска эквивалентных ключей криптосистемы Мак-Элиса–Сидельникова основывается на изучении множеств $\mathcal{G}(E, H)$. В случае, когда матрица H задает автоморфизм кода $RM(r, m)$, описание множества $\mathcal{G}(E, H)$ дает теорема 2. Представляется интересным получение описания этого множества в случае каких-то других матриц H .

Для некоторого вектора $\tilde{\alpha} = (\alpha_1, \dots, \alpha_k)$, $\alpha_i = 1$, рассмотрим $k \times k$ матрицу $T_{\tilde{\alpha}}^i$ вида

$$T_{\tilde{\alpha}}^i = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \dots & 1 & \dots & \alpha_k \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \leftarrow i$$

$\uparrow$
 i

Строки матрицы R обозначим через r_j , $1 \leq j \leq k$.

Теорема 4. Пусть $i = 1$, тогда

$$\mathcal{G}(E, T_{\tilde{\alpha}}^1) = \{\Gamma \in \mathcal{G}(E, E) \mid (0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)\}.$$

Здесь символом e^1 обозначен k -мерный вектор, у которого на первом месте стоит 1, а на всех остальных местах — 0, а $RM(r, m) \times RM(r, m)$ — множество всех возможных векторов $(f \parallel g)$ длины $2n$ таких, что $f, g \in RM(r, m)$.

Доказательство. Все строки матрицы $(R \parallel T_{\tilde{\alpha}}^1 R)$, кроме первой, будут иметь вид $(r_j \parallel r_j)$. Строка с номером 1 будет иметь вид $(r_1 \parallel \tilde{\alpha} R)$. При этом $r_1 = (11 \dots 1)$ — вектор из единиц.

Любая перестановка $\Gamma \in \mathcal{G}(E, T_{\tilde{\alpha}}^1)$ переводит слово $(r_j \parallel r_j)(j \neq 1)$ в слово $(w \parallel v)$ такое, что $w, v \in RM(r, m)$. Очевидно также, что вектор $(r_1 \parallel r_1) = (11 \dots 1 \parallel 11 \dots 1)$ под действием перестановки Γ переходит в себя, а это означает, что каждая строка матрицы $(R \parallel R)$ переходит в строку, левая и правая половины которой представляют собой слово кода Рида–Маллера $RM(r, m)$. При этом

$$(r_1 \parallel \tilde{\alpha} R)\Gamma = (r'_1 \parallel r''_1), \quad r'_1, r''_1 \in RM(r, m),$$

так как $\Gamma \in \mathcal{G}(E, T_{\tilde{\alpha}}^1)$. Но $r_1 = (11 \dots 1) = e^1 R$ и поэтому

$$\begin{aligned} (0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma &= (e^1 R \parallel e^1 R)\Gamma \oplus (e^1 R \parallel \tilde{\alpha} R)\Gamma \\ &= (1 \dots 1 \parallel 1 \dots 1) \oplus (r'_1 \parallel r''_1) = (r' \parallel r''). \end{aligned}$$

Здесь $r', r'' \in RM(r, m)$.

Окончательно получаем, что выполнено включение

$$\mathcal{G}(E, T_{\tilde{\alpha}}^1) \subseteq \{\Gamma \in \mathcal{G}(E, E) \mid (0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)\}.$$

Докажем обратное включение. Рассмотрим перестановку $\Gamma \in \mathcal{G}(E, E)$ такую, что $(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)$. Из предложения 7 следует, что перестановка Γ может быть представлена в виде $\Gamma = \Gamma' \mathcal{P}$. Для перестановки Γ' выполнено соотношение $(R \parallel R)\Gamma' = (R \parallel R)$, а перестановка $\mathcal{P}$ является расширенным автоморфизмом кода $RM(r, m)$. Иными словами, перестановка $\mathcal{P}$ имеет вид $\mathcal{P} = \gamma[1]\delta[2]$, где γ и δ — автоморфизмы кода $RM(r, m)$.

При действии на первую строку $(11 \dots 1 \parallel \tilde{\alpha} R)$ матрицы $(R \parallel T_{\tilde{\alpha}}^1 R)$ перестановкой Γ' получим, что

$$(1 \dots 1 \parallel \tilde{\alpha} R)\Gamma' = (f \parallel g),$$

причем первые координаты векторов f и g равны единице, так как $(R \parallel R)\Gamma' = (R \parallel R)$ и в первой координате вектора $\tilde{\alpha} R$ стоит 1.

Следовательно, при действии на вектор $(1 \dots 1 \parallel \tilde{\alpha} R)$ перестановки Γ получим равенство

$$(1 \dots 1 \parallel \tilde{\alpha} R)\Gamma = (f^\gamma \parallel g^\delta).$$

Докажем, что система векторов $(f^\gamma, r_2^\gamma, \dots, r_k^\gamma)$ линейно независима. Поскольку γ — перестановка, для этого достаточно доказать, что система $(f, r_2, \dots, r_k)$ линейно независима. Система векторов $(r_2, \dots, r_k)$ линейно независима, так как она входит в порождающую матрицу R кода Рида–Маллера $RM(r, m)$, причем в силу свойств матрицы R у

всех векторов $(r_2, \dots, r_k)$ в первой координате стоит 0. У вектора f в первой координате стоит 1. Следовательно, никакая линейная комбинация векторов системы $(r_2, \dots, r_k)$ не может дать вектор f , а значит, рассматриваемая система является линейно независимой. Аналогично доказывается, что система $(g, r_2, \dots, r_k)$ также линейно независима.

Итак, при действии перестановки Γ на матрицу $(R \parallel T_{\tilde{\alpha}}^1 R)$ в результате получим, что

$$(R \parallel T_{\tilde{\alpha}}^1 R)\Gamma = (G_1^\gamma \parallel G_2^\delta),$$

где G_1 и G_2 представляют собой некоторые матрицы, состоящие из линейно независимых строк $(f, r_2, \dots, r_k)$ и $(g, r_2, \dots, r_k)$ соответственно. При этом $r_2, \dots, r_k$ — векторы кода Рида–Маллера $RM(r, m)$. Докажем, что f и g — также векторы кода Рида–Маллера $RM(r, m)$. Действительно, рассмотрим вектор $(0 \parallel (e^1 \oplus \tilde{\alpha})R)$. Справедливо соотношение

$$(0 \parallel (e^1 \oplus \tilde{\alpha})R) = (1 \dots 1 \parallel \tilde{\alpha}R) \oplus (1 \dots 1 \parallel 1 \dots 1).$$

Отсюда следует, что

$$(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma = (f^\gamma \oplus 1 \parallel g^\delta \oplus 1).$$

При этом $(f^\gamma \oplus 1 \parallel g^\delta \oplus 1) \in RM(r, m) \times RM(r, m)$ в силу того, что $(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)$. Но γ и δ — автоморфизмы кода Рида–Маллера $RM(r, m)$, поэтому f и g — векторы кода Рида–Маллера $RM(r, m)$. Итак, векторы f и g в матрицах G_1 и G_2 принадлежат коду Рида–Маллера $RM(r, m)$, а значит, G_1 и G_2 — порождающие матрицы кода Рида–Маллера $RM(r, m)$. Вспоминая теперь, что γ и δ — автоморфизмы, заключаем, что $\Gamma \in \mathcal{G}(E, T_{\tilde{\alpha}}^1)$.

Теорема доказана.

Из теоремы 4 получаем полное описание класса эквивалентности $[(H, HT_{\tilde{\alpha}}^1, \Gamma)]$.

Теорема 5. Пусть $i = 1$, тогда класс эквивалентности $[(H, HT_{\tilde{\alpha}}^1, \Gamma)]$ состоит из кортежей вида $(HT_{\tilde{\beta}}^1 D_1, HT_{\tilde{\gamma}}^1 D_2, \mathcal{P}_1^{-1}[1]\mathcal{P}_2^{-1}[2](\Gamma')^{-1}\Gamma)$. Здесь D_1, D_2 — матрицы, задающие автоморфизмы P_1 и P_2 кода Рида–Маллера $RM(r, m)$, $\mathcal{P}_1[1], \mathcal{P}_2[2]$ — расширенные автоморфизмы, соответствующие P_1 и P_2 , перестановка Γ' сохраняет матрицу $(R \parallel R)$, а векторы β и γ определяются из соотношения

$$(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma' = ((e^1 \oplus \tilde{\beta})R \parallel (e^1 \oplus \tilde{\gamma})R).$$

Доказательство. По предложению 4, класс эквивалентности $[(H, HT_{\tilde{\alpha}}^1, \Gamma)]$ состоит из кортежей $(H'_1, H'_2, \Gamma_g \Gamma)$, где $\Gamma_g^{-1} \in \mathcal{G}(H, HT_{\tilde{\alpha}}^1)$ и $(HR \parallel HT_{\tilde{\alpha}}^1 R)\Gamma_g^{-1} = (H'_1 R \parallel H'_2 R)$. Из теоремы 4 и предложения 7 следует, что

$$\Gamma_g^{-1} = \Gamma' \mathcal{P}_1[1]\mathcal{P}_2[2],$$

где $\mathcal{P}_1[1], \mathcal{P}_2[2]$ — расширенные автоморфизмы кода $RM(r, m)$, соответствующие автоморфизмам P_1 и P_2 кода Рида–Маллера $RM(r, m)$, которые в свою очередь задаются матрицами D_1 и D_2 . Перестановка Γ' сохраняет матрицу $(R \parallel R)$ и, к тому же, $(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma' \in RM(r, m) \times RM(r, m)$. Справедливо представление

$$(0 \parallel (e^1 \oplus \tilde{\alpha})R) = (e^1 R \parallel e^1 R) \oplus (e^1 R \parallel \tilde{\alpha}R). \quad (1)$$

Далее,

$$(e^1 R \parallel e^1 R)\Gamma' = (e^1 R \parallel e^1 R),$$

так как Γ' сохраняет матрицу $(R \parallel R)$ и $(e^1 R \parallel e^1 R)$ — первая строка этой матрицы. Следовательно, $(e^1 R \parallel \tilde{\alpha} R)\Gamma' \in RM(r, m) \times RM(r, m)$, а значит найдутся такие $\tilde{\beta}$ и $\tilde{\gamma}$, что

$$(e^1 R \parallel \tilde{\alpha} R)\Gamma' = (\tilde{\beta} R \parallel \tilde{\gamma} R).$$

Объединяя это соотношение с равенством (1), получаем, что

$$(0 \parallel (e^1 \oplus \tilde{\alpha})R)\Gamma' = ((e^1 \oplus \tilde{\beta})R \parallel (e^1 \oplus \tilde{\gamma})R).$$

Применяя матрицу Γ_g^{-1} к матрице $(HR \parallel HT_{\tilde{\alpha}}^1 R)$, получаем, что

$$(HR \parallel HT_{\tilde{\alpha}}^1 R)\Gamma_g^{-1} = (HT_{\tilde{\beta}}^1 D_1 R \parallel HT_{\tilde{\gamma}}^1 D_2 R) = (H'_1 R \parallel H'_2 R).$$

Отсюда следует, что

$$H'_1 = HT_{\tilde{\beta}}^1 D_1, \quad H'_2 = HT_{\tilde{\gamma}}^1 D_2.$$

Осталось найти перестановку Γ_g . Используя представление для перестановки Γ_g^{-1} и свойства расширенных автоморфизмов, находим, что

$$\Gamma_g = (\Gamma_g^{-1})^{-1} = \mathcal{P}_1^{-1}[1]\mathcal{P}_2^{-1}[2](\Gamma')^{-1}.$$

Теорема доказана.

Перейдем теперь к изучению случая $i > 1$.

Символом R_j , $j = 1, \dots, 2n$ будем обозначать j -й столбец матрицы $(R \parallel T_{\tilde{\alpha}}^i R)$, причем будем считать, что нумерация столбцов сквозная. В соответствии с этой нумерацией столбцы с номерами R_t и R_{t+n} либо одинаковы, либо отличаются только в i -й координате. Далее будем рассматривать код Рида–Маллера $RM(r, m)$ с $r > 1$. Отметим, что полное описание множества $\mathcal{G}(E, H)$ для кода $RM(1, m)$ и всех матриц H было дано в [9].

Предложение 8. Пусть R — порождающая матрица кода $RM(r, m)$ и $r > 1$. Пусть также перестановка Γ с некоторыми невырожденными двоичными матрицами X , Y является решением уравнения

$$(R \parallel T_{\tilde{\alpha}}^i R)\Gamma = (XR \parallel YR),$$

то есть $\Gamma \in \mathcal{G}(E, T_{\tilde{\alpha}}^i)$. Тогда найдутся перестановки $\Gamma' \in S_{2n}$ и $\mathcal{P} = \sigma_L[1]\sigma_R[2] \in S_{2n}$, $\sigma_L, \sigma_R \in S_n$ такие, что

$$\Gamma = \Gamma'\mathcal{P}, \quad (R' \parallel R')\Gamma' = (R' \parallel R').$$

Здесь R' — матрица, получающаяся из матрицы R исключением i -й строки.

Доказательство. Матрицы XR , YR являются порождающими матрицами кода $RM(r, m)$, и поэтому дуальным кодом к XR и YR будет код $RM(m - r - 1, m)$ с кодовым расстоянием 2^{r+1} , при $r > 1$ кодовое расстояние дуального кода больше 4. Из этого факта следует, что в матрицах XR и YR не может быть двух одинаковых столбцов, в противном случае кодовое расстояние кода, дуального к этим кодам, будет равно 2, что невозможно.

Докажем, что в матрице XR нет двух пар столбцов (R_t, R_{t+n}) и (R_s, R_{s+n}) , $1 \leq t, s \leq n$, столбцов, отличающихся только в i -й координате. Действительно, предположив противное, можно заключить, что $R_t \oplus R_{t+n} \oplus R_s \oplus R_{s+n} = 0$, так как столбцы

в каждой паре отличаются только в i -й координате. Полученное соотношение означает, что в дуальном коде к коду, задаваемому матрицей XR , есть векторы веса 4, что невозможно в условиях утверждения. Итак, в матрице XR может быть либо одна, либо ни одной пары указанного вида.

Пусть теперь в XR имеется пара R_t, R_{t+n} столбцов, отличающихся только в i -й координате. Рассмотрим матрицу $(XR)'$, получающуюся из матрицы XR исключением i -й строки, и матрицу R' , получающуюся таким же образом из матрицы R . Итак, пусть R' состоит из столбцов $R'_1 R'_2 \dots R'_n$. В матрице $(XR)'$ будут столбцы R'_j для $j \neq s$, а вместо столбца R'_s будет столбец R'_{t+n} , который, очевидно, совпадает со столбцом R'_t . Наглядно матрица $(XR)'$ состоит из столбцов $R'_1, R'_2, \dots, R'_t, \dots, R'_{s-1}, R'_t, R'_{s+1}, \dots, R'_n$.

XR — порождающая матрица кода $RM(r, m)$, а в дуальном к этому коду лежит вектор из всех единиц. Поэтому сумма столбцов матриц R и XR , а значит и матриц R' и $(XR)'$, равна нулевому столбцу, то есть

$$\begin{aligned} R'_1 \oplus R'_2 \oplus \dots \oplus R'_t \oplus \dots \oplus R'_{s-1} \oplus R'_s \oplus R'_{s+1} \oplus \dots \oplus R'_n &= 0, \\ R'_1 \oplus R'_2 \oplus \dots \oplus R'_t \oplus \dots \oplus R'_{s-1} \oplus R'_t \oplus R'_{s+1} \oplus \dots \oplus R'_n &= 0. \end{aligned}$$

Складывая эти два равенства, получим $R'_s \oplus R'_t = 0$, то есть $R'_s = R'_t$. Иными словами, в матрице R столбцы R_s и R_t отличались только в i -й координате, но это означает, что $R_s = R_{t+n}$. Заметим, что к тому же $R_{s+n} = R_t$, так как в порождающей матрице кода $RM(r, m)$ не может быть двух одинаковых столбцов.

Итак, доказано, что в матрицах XR и YR либо вообще нет столбцов, отличающихся только в i -й координате, либо, если такая пара столбцов и есть, то в матрицах R и $T_{\alpha}^i R$ были одинаковые столбцы $R_s = R_{t+n}$ и $R_t = R_{s+n}$. В первом случае перестановка Γ сначала формирует матрицы XR и YR , при этом решая для каждой пары столбцов (R_t, R_{t+n}) , какой столбец в какой матрице будет лежать (этот процесс можно представить как применение перестановки Γ' из условия), а потом определяет порядок столбцов в каждой матрице с помощью перестановки $\mathcal{P}$. Во втором случае перестановка Γ будет формироваться из перестановки $\tilde{\Gamma}$, переводящей пары столбцов (R_s, R_t) и (R_{t+n}, R_{s+n}) друг в друга так, что R_s переходит в равный ему R_{t+n} , а R_t в равный ему R_{s+n} , и из перестановок $\Gamma', \mathcal{P}$ из первого случая. Но матрица $\tilde{\Gamma}$ также сохраняет матрицу $(R' \parallel R')$, так как $R'_t = R'_s = R'_{s+t} = R'_{t+n}$, поэтому сохраняет его произведение $\tilde{\Gamma}\Gamma'$. То есть и в этом случае утверждение выполняется. Предложение доказано.

Предложение 8 позволяет получить важное в дальнейшем следствие. Рассмотрим действие перестановки $\Gamma \in \mathcal{G}(E, T_{\alpha}^i)$ на матрицу $(R \parallel T_{\alpha}^i R)$. Обозначим через r_j строку с номером j матрицы R . Учитывая строение матрицы T_{α}^i , заключаем что

$$(R \parallel T_{\alpha}^i R) = \begin{pmatrix} r_1 & \parallel & r_1 \\ r_2 & \parallel & r_2 \\ & & \vdots \\ r_i & \parallel & r'_i \\ & & \vdots \\ r_k & \parallel & r_k \end{pmatrix},$$

здесь $r'_i = \tilde{\alpha} R$. В силу предложения 8 и полученного представления выполнены равенства

$$(R \parallel T_{\tilde{\alpha}}^i R) \Gamma = (R \parallel T_{\tilde{\alpha}}^i R) \Gamma' \cdot \mathcal{P} = \begin{pmatrix} r_1 & \parallel & r_1 \\ r_2 & \parallel & r_2 \\ & & \vdots \\ f & \parallel & g \\ & & \vdots \\ r_k & \parallel & r_k \end{pmatrix} \sigma_L[1] \sigma_R[2] = \begin{pmatrix} r_1^{\sigma_L} & \parallel & r_1^{\sigma_R} \\ r_2^{\sigma_L} & \parallel & r_2^{\sigma_R} \\ & & \vdots \\ f^{\sigma_L} & \parallel & g^{\sigma_R} \\ & & \vdots \\ r_k^{\sigma_L} & \parallel & r_k^{\sigma_R} \end{pmatrix},$$

здесь $(f \parallel g) = (r_i \parallel r'_i) \Gamma'$ и $\mathcal{P} = \sigma_L[1] \sigma_R[2]$. В силу того, что Γ принадлежит множеству $\mathcal{G}(E, T_{\tilde{\alpha}}^i)$, матрицы

$$B_L = \begin{pmatrix} r_1^{\sigma_L} \\ r_2^{\sigma_L} \\ \vdots \\ r_{i-1}^{\sigma_L} \\ r_{i+1}^{\sigma_L} \\ \vdots \\ r_k^{\sigma_L} \end{pmatrix}, \quad B_R = \begin{pmatrix} r_1^{\sigma_R} \\ r_2^{\sigma_R} \\ \vdots \\ r_{i-1}^{\sigma_R} \\ r_{i+1}^{\sigma_R} \\ \vdots \\ r_k^{\sigma_R} \end{pmatrix}$$

должны порождать некоторое подпространство кода Рида–Маллера $RM(r, m)$. Но легко видеть, что $B_L = (R')^{\sigma_L}$ и $B_R = (R')^{\sigma_R}$. Тем самым для описания множества перестановок $\mathcal{G}(E, T_{\tilde{\alpha}}^i)$ требуется изучить перестановки σ , осуществляющие перевод $(k-1)$ -мерного подпространства $\mathcal{R}'$ кода Рида–Маллера $RM(r, m)$ с порождающей матрицей R' в некоторое другое подпространство того же кода. Следующий раздел посвящен изучению таких перестановок.

4. Подпространства кода Рида–Маллера

Как выяснено в предыдущем разделе, для дальнейшего нам потребуется исследовать $(k-1)$ -мерные подпространства (подкоды) кода Рида–Маллера специального вида. Пусть, как и раньше, $RM(r, m)$ — код Рида–Маллера размерности k . Определим множества

$$\Pi_v = \{w \in RM(r, m) \mid (w, v) = 0\}.$$

Предложение 9. Все подпространства размерности $k-1$ кода $RM(r, m)$ исчерпываются множествами Π_v .

Доказательство. Пусть $RM(r, m)$ — код Рида–Маллера и k — его размерность. Требуется доказать, что для любого $(k-1)$ -мерного подкода Π существует вектор $v \in \mathbb{F}_2^n$ такой, что вектор w из кода $RM(r, m)$ лежит в подкоде Π , если и только если $(w, v) = 0$, то есть

$$(w, v) = w_1 v_1 \oplus w_2 v_2 \oplus \dots \oplus w_n v_n = 0.$$

Рассмотрим некоторый вектор v , не принадлежащий коду $RM^\perp(r, m)$. Тогда, очевидно, что Π_v — некоторый $(k-1)$ -мерный подкод кода $RM(r, m)$.

Осталось доказать, что любое $(k-1)$ -мерное пространство совпадает с некоторым Π_v . Рассмотрим некоторое $(k-1)$ -мерное подпространство Π . Заметим, что дуальное

пространство к Π имеет размерность $n - k + 1$, что в точности на единицу больше размерности кода $RM^\perp(r, m)$, а сам этот код лежит в $\Pi^\perp$. В силу этого найдется вектор v , который не лежит в коде $RM^\perp(r, m)$, но лежит в $\Pi^\perp$. Докажем, что $\Pi = \Pi_v$.

В силу того, что $v \in \Pi^\perp$, для любого $w \in \Pi$ выполняется соотношение $(w, v) = 0$, то есть $\Pi \subset \Pi_v$, но размерности этих кодов совпадают, поэтому отсюда немедленно следует, что и сами эти коды совпадают.

Предложение доказано.

Из предложения 9 следует, что любой подкод Π однозначно задается некоторым вектором v . Но возможна ситуация, когда несколько векторов v задают один и тот же код. Следующая теорема дает описание свойства, которым должны обладать такие векторы.

Предложение 10. *Для любых двух векторов v_1 и v_2 коды Π_{v_1} и Π_{v_2} совпадают, если и только если v_1 и v_2 лежат в одном смежном классе по коду $RM(m - r - 1, m)$, то есть $v_1 \oplus v_2 \in RM(m - r - 1, m)$.*

Доказательство. Пусть Π_{v_1} и Π_{v_2} совпадают. Тогда для любого вектора $w \in \Pi_{v_1}$ выполняются соотношения $(w, v_1) = 0$ и $(w, v_2) = 0$. Поэтому любой вектор w , лежащий в коде Π_{v_1} , ортогонален вектору $v_1 \oplus v_2$. С другой стороны, для любого вектора w из $RM(r, m)$, не лежащего в коде Π_{v_1} , выполняются соотношения $(w, v_1) = 1$ и $(w, v_2) = 1$. Отсюда следует, что любой вектор w кода Риды–Маллера $RM(r, m)$, не лежащий в Π_{v_1} , также ортогонален вектору $v_1 \oplus v_2$. Поэтому все векторы кода $RM(r, m)$ ортогональны вектору $v_1 \oplus v_2$. Другими словами, $v_1 \oplus v_2 \in RM(m - r - 1, m)$.

Пусть теперь $v_1 \oplus v_2 \in RM(m - r - 1, m)$. Докажем, что $\Pi_{v_1} = \Pi_{v_2}$. Рассмотрим любой вектор $x \in \Pi_{v_1}$. Во-первых, $x \in RM(r, m)$, а во-вторых, $(x, v_1) = 0$. Вектор v_1 представим в виде $v_1 = v_2 \oplus v$, где $v \in RM(m - r - 1, m)$. Следовательно, $(x, v_1) = (x, v_2) \oplus (x, v)$. При этом $(x, v) = 0$, поскольку $x \in RM(r, m)$, а $v \in RM(m - r - 1, m) = RM^\perp(r, m)$. Итак, $(x, v_1) = (x, v_2)$, а значит, $x \in \Pi_{v_2}$. Доказано включение $\Pi_{v_1} \subseteq \Pi_{v_2}$. Обратное включение, в силу симметрии $v_1 \oplus v_2$, доказывается аналогично.

Для изучения множества открытых ключей криптосистемы Мак–Элиса–Сидельникова важным оказывается вопрос об эквивалентности двух $(k - 1)$ -мерных подпространств. Будем говорить, что два подпространства эквивалентны, если одно подпространство переводится в другое некоторой перестановкой π . Действительно, в разделе 3 установлена связь множества $\mathcal{G}(E, T_{\alpha}^i)$ со специальным подкодом $\mathcal{R}'$ кода Риды–Маллера $RM(r, m)$. Напомним, что порождающая матрица R' подкода получается из порождающей матрицы R кода Риды–Маллера $RM(r, m)$ исключением строки с номером i . В силу выбора порождающей матрицы R , подкод $\mathcal{R}'$ с порождающей матрицей R' представляет собой те булевы функции из кода $RM(r, m)$, в полиноме Жегалкина которых нет монома $x_{i_1} \dots x_{i_t}$, соответствующего строке r_i матрицы R . Этот моном имеет некоторую степень t , причем $t > 0$, так как $i > 1$. Тем самым код $\mathcal{R}'$ задается вектором $v = \bar{x}_{j_1} \bar{x}_{j_2} \dots \bar{x}_{j_{m-t}}$. При этом

$$\begin{aligned} \{j_1, j_2, \dots, j_{m-t}\} \cup \{i_1, i_2, \dots, i_t\} &= \{1, 2, \dots, m\}, \\ \{j_1, j_2, \dots, j_{m-t}\} \cap \{i_1, i_2, \dots, i_t\} &= \emptyset. \end{aligned}$$

Очевидно, что существует аффинная перестановка π , которая переводит код $\mathcal{R}'$ в подкод Π_w , где $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$. Перестановка π просто осуществляет переименование переменных. Тем самым доказано следующее утверждение.

Предложение 11. Пусть $(R')^\pi$ — подпространство, которое получается из подпространства (R') применением к каждому вектору этого подпространства перестановки π . Тогда существует аффинная перестановка π такая, что $(R')^\pi = \Pi_w$, где $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$ и t — некоторое натуральное число, не большее r .

В силу предложения 11, для изучения множества открытых ключей криптосистемы Мак-Элиса–Сидельникова достаточно изучить эквивалентность двух подпространств, одно из которых задается вектором $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$.

Докажем основную лемму.

Лемма 1. Пусть Π_w — $(k-1)$ -мерное подпространство кода Риды–Маллера $RM(r, m)$, $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$. Пусть также перестановка σ такова, что Π_w^σ — подпространство кода $RM(r, m)$. Тогда

(i) если $1 < t \leq r$, то вектор v минимального веса кода $RM(s, m)$, $s > r$, вида

$$v = (x_{i_1} \oplus a_{i_1})(x_{i_2} \oplus a_{i_2}) \dots (x_{i_s} \oplus a_{i_s}),$$

здесь $x_{i_j} \neq x_{i_k}$, $j \neq k$, a_{i_j} — двоичные константы, под действием перестановки σ переходит в вектор минимального веса того же кода, то есть v^σ принадлежит $RM(s, m)$;

(ii) если $t = 1$, то вектор v минимального веса кода $RM(s, m)$, $s > r$, вида

$$v = (x_{i_1} \oplus a_{i_1})(x_{i_2} \oplus a_{i_2}) \dots (x_{i_s} \oplus a_{i_s}),$$

здесь $x_{i_j} \neq x_{i_k}$, $j \neq k$, a_{i_j} — двоичные константы и $i_j \neq t$ для любого $1 \leq j \leq s$, под действием перестановки σ переходит в вектор минимального веса того же кода, то есть $v^\sigma \in RM(s, m)$.

Доказательство. Докажем первую часть. Рассмотрим вектор

$$v = (x_{i_1} \oplus a_{i_1})(x_{i_2} \oplus a_{i_2}) \dots (x_{i_s} \oplus a_{i_s}).$$

По условию $x_{i_j} \neq x_{i_k}$, если $j \neq k$, и $s > r$, а значит, $\{i_1, i_2, \dots, i_s\} \neq \{m-t+1, \dots, m\}$. Рассмотрим два случая. Пусть сначала $\{m-t+1, \dots, m\}$ не содержится целиком во множестве $\{i_1, \dots, i_s\}$. Представим вектор v в виде произведения

$$v = M_r M_{r+1} \dots M_s. \quad (2)$$

Здесь M_j — векторы значений функций, которые определяются следующим образом

$$M_j = (x_{i_1} \oplus a_{i_1}) \dots (x_{i_{r-1}} \oplus a_{i_{r-1}})(x_{i_j} \oplus a_{i_j}).$$

Множества $\{i_1, \dots, i_{r-1}, i_j\}$ не содержат целиком множество $\{m-t+1, \dots, m\}$, а значит, $\{i_1, \dots, i_{r-1}, i_j\} \cup \{1, 2, \dots, m-t\} \neq \{1, 2, \dots, m\}$. Из этого следует, что произведение функций $M_j \cdot w$ имеет степень, строго меньшую m , поэтому скалярное произведение

$$(M_j, w) = wt(M_j \cdot w) \pmod{2} = 0.$$

Так как $\deg M_j = r$, заключаем, что $M_j \in \Pi_w$. Итак, вектор v представим в виде произведения векторов минимального веса кода Риды–Маллера $RM(r, m)$ из подпространства Π_w .

Докажем, что представление (2) справедливо и в случае, когда $\{m-t+1, \dots, m\}$ целиком содержится в множестве $\{i_1, \dots, i_s\}$. Не ограничивая общности, будем считать,

что $\{i_{r-t+2}, \dots, i_{r+1}\} = \{m-t+1, \dots, m\}$. При этом, очевидно, i_1 не лежит в множестве $\{m-t+1, \dots, m\}$. Следовательно, при $t > 1$, множества $\{i_1, \dots, i_{r-1}, i_j\}$ опять целиком не содержат множество $\{m-t+1, \dots, m\}$, а значит, векторы M_j лежат в подпространстве Π_w и справедливо представление (2).

Поддействуем на v перестановкой σ , учитывая представление (2)

$$v^\sigma = M_r^\sigma M_{r+1}^\sigma \dots M_s^\sigma = M'_r M'_{r+1} \dots M'_s.$$

По построению M_j — векторы минимального веса кода $RM(r, m)$, лежащие в подпространстве Π_w . Перестановка σ переводит векторы из Π_w в векторы кода $RM(r, m)$, значит $M'_j = M_j^\sigma$ — векторы минимального веса кода Риды–Маллера $RM(r, m)$. Из свойств векторов минимального веса (см. [6]) следует, что существуют линейно независимые аффинные функции $l_j^1, \dots, l_j^r$ такие, что $M'_j = l_j^1 \dots l_j^r$. Таким образом,

$$v^\sigma = l_r^1 \dots l_r^r \dots l_j^1 \dots l_j^r \dots l_s^1 \dots l_s^r.$$

Функцию v^σ можно представить в виде произведения множества аффинных функций l_j^i , $1 \leq i \leq r$, $r \leq j \leq s$. Выделим среди этого множества систему линейно независимых функций, состоящую из максимально возможного числа функций. Обозначим эти функции символами $l_1, \dots, l_d$. Все функции, не входящие в эту систему, можно выразить как некоторую сумму векторов $l_1, \dots, l_d$. Другими словами,

$$v^\sigma = l_1 l_2 \dots l_d \prod_j (b_1^j l_1 \oplus b_2^j l_2 \oplus \dots \oplus b_d^j l_d).$$

После раскрытия скобок и приведения подобных слагаемых получаем, что

$$v^\sigma = l_1 l_2 \dots l_d \prod_j (b_1^j \oplus b_2^j \oplus \dots \oplus b_d^j) l_1 l_2 \dots l_d = c l_1 l_2 \dots l_d,$$

где c — двоичная константа. В силу того, что $v \neq 0$, справедливо равенство $c = 1$. Далее, $d = s$, так как вес v^σ , с одной стороны, равен весу v , то есть равен 2^{m-s} , а с другой стороны, вес этого вектора равен 2^{m-d} , поэтому $m-s = m-d$. Таким образом, $v^\sigma = l_1 l_2 \dots l_s$. Значит, v^σ — вектор минимального веса кода $RM(s, m)$.

Для доказательства второй части леммы опять обратимся к представлению (2). В условиях леммы ни одно из M_j этого представления не содержит множитель вида $(x_m \oplus a)$. Возможны две ситуации, либо есть такой номер i_p , $p \in \{1, 2, \dots, r-1, j\}$, что $a_{i_p} = 0$ в функции M_j , то есть в M_j переменная x_{i_p} входит без отрицания, либо такого номера не существует, то есть все переменные M_j входят в M_j только с отрицанием. Множество существенных переменных булевой функции w содержит множество существенных переменных функции M_j , поэтому в первом случае $M_j w = 0$, а во втором $M_j w = w$. Заметив, что $wt(w) = 2 = 0 \pmod{2}$, получаем равенство $(M_j, w) = 0$, то есть M_j лежит в Π_w . Тем самым, вектор v представим в виде произведения векторов M_j минимального веса кода $RM(r, m)$, лежащих в Π_w . Следовательно, для завершения доказательства достаточно повторить рассуждения первой части.

Лемма доказана.

Предложение 12. Пусть $2r+1 < m$, $1 < t \leq r$, и $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$. Пусть также $(k-1)$ -мерное подпространство Π_w кода Риды–Маллера $RM(r, m)$ задается вектором w , и перестановка σ переводит Π_w в подпространство кода $RM(r, m)$. Тогда σ — автоморфизм кода Риды–Маллера $RM(r, m)$, то есть $\sigma \in \text{Aut}(RM(r, m))$.

Доказательство. Рассмотрим код $RM(m-r-1, m)$, который является ортогональным кодом к коду $RM(r, m)$. Рассмотрим стандартную порождающую матрицу $R(m-r-1, m)$ кода $RM(m-r-1, m)$. Поскольку $m > 2r+1$, матрица $R(m-r-1, m)$ содержит стандартную порождающую матрицу $R(r, m)$ кода $RM(r, m)$ и некоторое число мономов степени, большей r . В силу определения подпространства Π_w , в матрице $R(r, m)$ подпространству Π_w не принадлежит только вектор, соответствующий моному $x_{m-t+1} \dots x_m$. Модифицируем базис $R(m-r-1, m)$, заменив в нем вектор $x_{m-t+1} \dots x_m$ вектором

$$f = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-r-t-1} x_{m-t+1} \dots x_m.$$

Заметим, что такая замена возможна, так как $m-r-t-1 \geq m-2r-1 > 0$. Измененный базис $R'(m-r-1, m)$ останется базисом кода $RM(m-r-1, m)$, так как, с одной стороны, $f \in RM(m-r-1, m)$, а с другой, в полиноме Жегалкина функции f содержится моном $x_{m-t+1} \dots x_m$, что обеспечивает линейную независимость вектора значений функции f и оставшихся векторов матрицы $R(m-r-1, m)$.

Рассмотрим действие перестановки σ на базис $R'(m-r-1, m)$. Если вектор g базиса лежит в Π_w , то по условию g^σ лежит в $RM(r, m)$, а значит, при $m > 2r+1$ и в $RM(m-r-1, m)$. Далее, если g не лежит в Π_w , то либо $g = f$, либо g — моном, степени большей r . Как бы то ни было, вектор g имеет вид

$$g = (x_{i_1} \oplus a_{i_1})(x_{i_2} \oplus a_{i_2}) \dots (x_{i_s} \oplus a_{i_s}),$$

где $m-r-1 \geq s > r$. Применяя основную лемму, получим, что g^σ является вектором из кода $RM(s, m)$, который содержится в коде $RM(m-r-1, m)$. Итак, базис $R'(m-r-1, m)$ под действием σ переходит в базис кода $RM(m-r-1, m)$ и σ есть автоморфизм кода $RM(m-r-1, m)$, а так как $RM^\perp(r, m) = RM(m-r-1, m)$, и кода $RM(r, m)$, что и требовалось доказать.

Предложение 13. Пусть $2r \leq m$, $0 < t \leq r$, и $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$. Пусть также $(k-1)$ -мерное подпространство Π_w кода Риды–Маллера $RM(r, m)$ задается вектором w и для некоторой перестановки σ множество Π_w^σ — подпространство кода Риды–Маллера $RM(r, m)$. Тогда существует аффинная перестановка γ такая, что $\sigma = \sigma' \gamma$, где σ' — автоморфизм кода Π_w и к тому же $w^{\sigma'} = w$.

Доказательство. Заметим, что к w и σ можно применить при $t > 1$ первую часть основной леммы 1, а при $t = 1$ — вторую часть, так как вектор w не содержит символа переменной x_m . Итак, в силу основной леммы 1 справедливо представление

$$w^\sigma = l_1 l_2 \dots l_{m-t}.$$

Из этого представления следует, что w^σ не лежит в коде $RM^\perp(r, m)$, так как степень w^σ равна $m-t > m-r-1$. Далее, любой вектор x^σ , $x \in \Pi_w$, ортогонален вектору w^σ , так как x ортогонален w . Получаем, что

$$\Pi_w^\sigma = \Pi_{w^\sigma} = \Pi_{l_1 l_2 \dots l_{m-t}}. \quad (3)$$

Из представления вектора w^σ следует, что существует аффинная перестановка γ' , переводящая вектор w в вектор w^σ , то есть $w^{\gamma'} = w^\sigma$. В силу этого (3) можно переписать в виде

$$\Pi_w^\sigma = \Pi_{w^\sigma} = \Pi_{w^{\gamma'}}. \quad (4)$$

Однако, $\Pi_{w^{\gamma'}} = \Pi_w^{\gamma'}$, так как $w^{\gamma'}$ не лежит в коде $RM^\perp(r, m)$, перестановка γ' аффинная, а значит, $\Pi_w^{\gamma'}$ — подпространство кода $RM(r, m)$, и любой вектор из $\Pi_w^{\gamma'}$ ортогонален вектору $w^{\gamma'}$. Итак, доказано, что для любой перестановки σ , удовлетворяющей условию предложения, существует такая аффинная перестановка, что выполнена цепочка равенств

$$\Pi_w^\sigma = \Pi_{w^\sigma} = \Pi_{w^{\gamma'}} = \Pi_w^{\gamma'}.$$

Из равенства $\Pi_w^\sigma = \Pi_w^{\gamma'}$ следует, что $\delta = \sigma(\gamma')^{-1}$ является автоморфизмом кода Π_w . Возможно, окажется, что $w^\delta = w$, тогда, полагая $\sigma' = \delta$ и $\gamma = \gamma'$, получим требуемое. В противном случае, так как δ — автоморфизм кода Π_w , Π_w^δ — подпространство кода $RM(r, m)$, поэтому, если во всех рассуждениях выше заменить σ на δ , то получим, что найдется аффинная перестановка $\tilde{\gamma}$ такая, что $w^\delta = w^{\tilde{\gamma}}$, причем $\Pi_w^\delta = \Pi_w^{\tilde{\gamma}}$. Перестановка $\delta' = \delta\tilde{\gamma}^{-1}$, очевидно, из группы автоморфизмов кода Π_w , и к тому же для нее выполнено соотношение $w^{\delta'\tilde{\gamma}^{-1}} = w$. С другой стороны, $\delta = \sigma(\gamma')^{-1}$. Поэтому $\delta' = \delta\tilde{\gamma}^{-1} = \sigma(\gamma')^{-1}\tilde{\gamma}^{-1}$. Отсюда $\sigma = \sigma'\gamma$, где $\sigma' = \delta'$ — автоморфизм кода Π_w и $w^{\sigma'} = w$, а $\gamma = \tilde{\gamma}\gamma'$ — аффинная перестановка. Предложение доказано.

Предложение 13 позволяет свести изучение перестановок σ , которые переводят подпространство Π_w в другое подпространство кода Риди–Маллера $RM(r, m)$, к изучению некоторого подкласса автоморфизмов кода Π_w . Отметим, что предложение 13 справедливо для широкого класса параметров r, m и t . Однако для некоторых параметров описание перестановок σ уже было получено (см. предложение 12). Остались неизвестными только перестановки, отвечающие параметрам $2r \leq m \leq 2r + 1$, $t > 1$ и параметрам $2r \leq m$, $t = 1$.

Рассмотрим множество перестановок

$$I(\Pi_w) = \{\delta \in S_n \mid \forall x \in \Pi_w, x^\delta = x\}.$$

Иными словами множество $I(\Pi_w)$ состоит из перестановок, которые не изменяют кодовые слова кода Π_w . Эти перестановки в некотором смысле похожи на тождественную перестановку. Очевидно, что если в порождающей матрице кода Π_w нет одинаковых столбцов, то $I(\Pi_w)$ содержит только тождественную перестановку. Множество $I(\Pi_w)$ образует подгруппу в группе автоморфизмов Π_w .

Докажем одно свойство множества $I(\Pi_w)$, которое понадобится в дальнейшем.

Лемма 2. Пусть $1 < t \leq r$, тогда множество $I(\Pi_w)$ содержит только тождественную перестановку e , то есть

$$I(\Pi_w) = \{e\}.$$

Доказательство. Достаточно доказать, что при $t > 1$ порождающая матрица кода Π_w не содержит одинаковых столбцов. Но для этого достаточно показать, что кодовое расстояние $d(\Pi_w^\perp)$ кода $\Pi_w^\perp$ строго больше двух. Действительно, если это так, то порождающая матрица кода Π_w не может содержать одинаковые столбцы. Если бы она содержала одинаковые столбцы, то вектор веса 2 с единичными координатами только на местах, соответствующих одинаковым столбцам порождающей матрицы, лежал бы в дуальном коде, а значит, дуальный код не мог бы иметь кодовое расстояние, большее двух.

Итак, докажем, что кодовое расстояние $\Pi_w^\perp$ больше двух. Для этого найдем сначала это кодовое расстояние $d(\Pi_w^\perp)$.

Код $\Pi_w^\perp$, в силу определения, может быть представлен в виде объединения двух множеств

$$\Pi_w^\perp = RM^\perp(r, m) \cup \{w \oplus RM^\perp(r, m)\}. \quad (5)$$

Кодовое расстояние $RM^\perp(r, m)$ равно $2^{r+1} > 2^t$. При этом вектор $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$ имеет вес, в точности равный 2^t . Докажем, что $d(\Pi_w^\perp) = 2^t$. Рассмотрим произвольный вектор $f \in RM^\perp(r, m)$. Для веса вектора $w \oplus f$ справедливо соотношение

$$wt(w \oplus f) = wt(w) \oplus wt(f) - 2wt(wf).$$

Вес вектора w равен 2^t . Так как $t \leq r$, справедливы неравенства

$$0 \leq 2wt(wf) \leq 2^{t+1} \leq 2^{r+1}.$$

Но $2^{r+1} \leq wt(f)$, так как 2^{r+1} — кодовое расстояние кода $RM^\perp(r, m)$. Следовательно, $2wt(wf) \leq wt(f)$. Итак,

$$wt(w \oplus f) = wt(w) + wt(f) - 2wt(w \cdot f) \geq wt(w) = 2^t.$$

Этим доказано, что кодовое расстояние кода $\Pi_w^\perp$ равно 2^t . Для завершения доказательства леммы нужно заметить, что $t > 1$, а значит, и $2^t > 2$.

В дальнейшем нам потребуется множество перестановок $\text{Aut}(w, RM(r, m))$. Это множество содержит те и только те автоморфизмы кода Риды–Маллера $RM(r, m)$, которые сохраняют смежный класс $w \oplus RM^\perp(r, m)$, то есть

$$\gamma \in \text{Aut}(w, RM(r, m)) \iff (w \oplus RM^\perp(r, m))^\gamma = w \oplus RM^\perp(r, m), \gamma \in \text{Aut}(RM(r, m)).$$

Предложение 14. *Аффинная перестановка γ принадлежит группе автоморфизмов $\text{Aut}(\Pi_w)$, если и только если $\gamma \in \text{Aut}(w, RM(r, m))$.*

Доказательство. Аффинная перестановка γ принадлежит группе $\text{Aut}(\Pi_w)$, если и только если она принадлежит группе автоморфизмов дуального кода $\Pi_w^\perp$. Код $\Pi_w^\perp$, в силу определения, может быть представлен в виде (5). Так как перестановка γ — автоморфизм кода $RM(r, m)$, она и автоморфизм кода $RM^\perp(r, m)$, дуального к $RM(r, m)$, а значит, для того, чтобы она была и автоморфизмом кода $\Pi_w^\perp$, необходимо и достаточно, чтобы она сохраняла смежный класс $w \oplus RM^\perp(r, m)$, что и требовалось доказать.

Приведем без доказательства утверждение, необходимое для дальнейшего изложения.

Теорема 6. *Вес каждого слова в коде $RM(r, m)$ кратен $2^{\lceil (m-1)/r \rceil}$.*

Доказательство этой теоремы Мак-Элиса можно найти в [6].

Предложение 15. *Пусть $RM(r, m)$ — код Риды–Маллера, пусть также $0 < t \leq r$ и $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$. Пусть, кроме того, выполнено одно из условий:*

$$(i) \ t = 1;$$

$$(ii) \ m = 2r \text{ или } m = 2r + 1 \text{ и } t > 1.$$

Тогда перестановка σ , для которой $w^\sigma = w$, является автоморфизмом кода Π_w , если и только если $\sigma \in I(\Pi_w) \times \text{Aut}(w, RM(r, m))$.

Доказательство. Предположим сначала, что выполнено условие (i), то есть $t = 1$. Для кода, дуального к коду Π_w , справедливо представление (5), причем в этом представлении вектор $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-1}$ имеет вес, равный двум, и обращается в единицу на наборах $\tilde{\alpha} = \{0, 0, \dots, 0\}$ и $\tilde{\beta} = \{1, 0, \dots, 0\}$. Здесь предполагается, что α_i и β_i , $1 \leq i \leq m$, определяют значения переменной x_{m-i+1} . Рассмотрим теперь любую перестановку σ из группы автоморфизмов кода Π_w , сохраняющую вектор w . В силу того, что $w^\sigma = w$, перестановку σ можно представить в виде $\sigma = \sigma_L[1]\sigma_R[2]$, где σ_L — перестановка на множестве из двух элементов $\tilde{\alpha}$ и $\tilde{\beta}$, а σ_R переставляет оставшиеся $2^m - 2$ координаты. Отметим, что для σ_L выполняется соотношение $\sigma_L^2 = e$.

В коде $RM^\perp(r, m) = RM(m - r - 1, m)$ размерности $k^\perp$ можно так выбрать базис $f_1, f_2, \dots, f_{k^\perp}$, что все функции в этом базисе будут иметь минимальный вес и на наборе $\tilde{\alpha}$ обращаться в 1. Действительно, пусть $RM^*(m - r - 1, m)$ — выколотый код Рида–Маллера $RM(m - r - 1, m)$, то есть $RM^*(m - r - 1, m)$ получается из $RM(m - r - 1, m)$, если в каждом кодовом слове кода $RM(m - r - 1, m)$ выкинуть первую координату. Известно (см. [6]), что в коде $RM^*(m - r - 1, m)$ существует базис $f'_1, f'_2, \dots, f'_{k^\perp}$ из слов минимального веса. Слова минимального веса кода $RM^*(m - r - 1, m)$ имеют вес $2^{r+1} - 1$. Положим $f_i = (a_i \parallel f'_i)$, где a_i — сумма всех координат вектора f'_i , то есть общая проверка на четность вектора f'_i . Очевидно, что $f_1, f_2, \dots, f_{k^\perp}$ — базис кода $RM(m - r - 1, m)$, при этом все $a_i = 1$, так как вес f'_i нечетен.

Далее, в силу того, что в порождающей матрице кода $RM(m - r - 1, m)$ нет нулевых столбцов, среди функций f_i найдется хотя бы одна, принимающая на наборе $\tilde{\beta}$ значение 1.

Рассмотрим действие перестановки σ на этот базис. Для начала заметим, что все векторы f_i такие, что $f_i(\tilde{\alpha}) = f_i(\tilde{\beta}) = 1$, заведомо остаются в коде $RM(m - r - 1, m)$ после действия перестановки σ , так как если какой-то вектор f_i окажется не в коде $RM(m - r - 1, m)$, то в силу представления (5) в этом коде должен лежать вектор $f_i^\sigma \oplus w$, так как $\sigma \in \text{Aut}(\Pi_w)$. Но в последнем случае вес вектора f_i^σ уменьшился бы на 2, то есть стал бы равным $2^{r+1} - 2 < 2^{r+1}$, так как $f_i^\sigma(\tilde{\alpha}) = 1$ и $f_i^\sigma(\tilde{\beta}) = 1$. А это означает, что в коде $RM(m - r - 1, m)$ лежал бы вектор $f_i^\sigma \oplus w$, вес которого строго меньше кодового расстояния кода $RM(m - r - 1, m)$, что невозможно.

Векторы значений оставшихся функций базиса могут перейти либо также в код $RM(m - r - 1, m)$ после действия σ , либо в смежный класс $w \oplus RM(m - r - 1, m)$. Предположим, что существуют две функции f и g , входящие в базис, такие, что $f(\tilde{\alpha}) = g(\tilde{\alpha}) = 1$, $f(\tilde{\beta}) = g(\tilde{\beta}) = 0$, и они одновременно переходят в смежный класс под действием перестановки σ . Тогда, из определения смежного класса, $f^\sigma \oplus g^\sigma = w \oplus f_1 \oplus w \oplus g_1 = f_1 \oplus g_1$, причем $f_1, g_1 \in RM(m - r - 1, m)$, то есть вектор $f \oplus g$ из кода $RM(m - r - 1, m)$ остается в коде Рида–Маллера $RM(m - r - 1, m)$. При этом $(f \oplus g)(\tilde{\alpha}) = (f \oplus g)(\tilde{\beta}) = 0$. Заменяем в базисе вектор f вектором $f \oplus g$ и рассмотрим новый базис. Если в нем снова имеются два указанных ранее вектора, то проделаем с базисом такую же операцию замены. После конечного числа шагов получим базис, в котором все векторы f , кроме быть может одного вектора g , под действием перестановки σ остаются в коде $RM(m - r - 1, m)$. В ситуации, когда все векторы остаются в $RM(m - r - 1, m)$, перестановка σ является автоморфизмом кода $RM(m - r - 1, m)$, а значит, и кода $RM(r, m)$, поэтому σ — аффинная перестановка, а значит, $\sigma \in \text{Aut}(w, RM(r, m))$.

В случае, когда вектор g переходит в смежный класс, вектор $(g \oplus w)^\sigma$ лежит в $RM(m - r - 1, m)$. Но в этом случае $g^{\delta_L[1]e[2]\sigma_L[1]\sigma_R[2]} \in RM(m - r - 1, m)$, потому что добавление вектора w к g эквивалентно применению перестановки $\delta_L[1]e[2]$ (это следует из того, что $g(\tilde{\alpha}) \neq g(\tilde{\beta})$). Здесь δ_L — транспозиция столбцов с номерами $\tilde{\alpha}$ и $\tilde{\beta}$. Заметим, что это соотношение можно распространить на все оставшиеся f из базиса, так

как если $f(\tilde{\alpha}) = f(\tilde{\beta})$, то $f^{\delta_L[1]e[2]} = f$.

Следовательно, $\delta_L[1]e[2]\sigma_L[1]\sigma_R[2]$ — автоморфизм кода $RM(m-r-1, m)$. Итак, в этом случае $\sigma \in \delta_L^{-1}[1]e[2]\text{Aut}(w, RM(r, m))$. Осталось заметить, что $\delta_L^{-1}[1]e[2]$ принадлежит множеству $I(\Pi_w)$, так как она переставляет координаты, соответствующие одинаковым столбцам порождающей матрицы кода Π_w . Тем самым доказано, что в случае $t = 1$ перестановка σ принадлежит множеству $I(\Pi_w) \times \text{Aut}(w, RM(r, m))$. Докажем обратное, для этого рассмотрим перестановку $\sigma \in I(\Pi_w) \times \text{Aut}(w, RM(r, m))$. Найдутся такие перестановки $\delta \in I(\Pi_w)$ и $\gamma \in \text{Aut}(w, RM(r, m))$, что $\sigma = \delta\gamma$. Перестановка δ является автоморфизмом кода Π_w в силу определения, а γ является автоморфизмом этого кода в силу предложения 14. Следовательно, перестановка σ является автоморфизмом Π_w как произведение автоморфизмов. Итак, первая часть полностью доказана.

Пусть теперь выполнено условие (ii). В этом случае $1 < t \leq r$, а значит, $I(\Pi_w) = \{e\}$ в силу леммы 2. Тем самым требуется доказать, что если $w^\sigma = w$, то σ — автоморфизм кода Π_w , если и только если $\sigma \in \text{Aut}(w, RM(r, m))$. Как и выше, представим перестановку σ в виде $\sigma = \sigma_L[1]\sigma_R[2]$, где σ_L переставляет координаты, $\tilde{\alpha}_1, \tilde{\alpha}_2, \dots, \tilde{\alpha}_{2^t}$, соответствующие единицам вектора w , а σ_R переставляет координаты, соответствующие нулям этого вектора. В силу того, что $w = \bar{x}_1\bar{x}_2 \dots \bar{x}_{m-t}$, векторы $\tilde{\alpha}_i$ имеют вид

$$\begin{aligned} \tilde{\alpha}_1 &= \begin{pmatrix} x_m & x_{m-1} & & x_{m-t+2} & x_{m-t+1} & x_{m-t} & & x_1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \\ \tilde{\alpha}_2 &= \begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix} \\ \tilde{\alpha}_3 &= \begin{pmatrix} 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{pmatrix} \\ &\dots \\ \tilde{\alpha}_4 &= \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 0 & \dots & 0 \end{pmatrix} \end{aligned}$$

Построим порождающую матрицу $M(t)$ кода $RM(m-r-1, m)$ специального вида. Известно [6], что существует порождающая матрица $G(m-r-1, m)$ кода Риды–Маллера $RM(m-r-1, m)$, представляемая в следующем виде

$$G(m-r-1, m) = \begin{pmatrix} G(m-r-1, m-1) \\ \mathbb{O} \end{pmatrix} \parallel \begin{pmatrix} G(m-r-1, m-1) \\ G(m-r-2, m-1) \end{pmatrix}, \quad (6)$$

или в виде $G(m-r-1, m) = (G(m-r-1, m)_{L_1} \parallel G(m-r-1, m)_{L_2})$, если положить

$$\begin{aligned} G(m-r-1, m)_{L_1} &= \begin{pmatrix} G(m-r-1, m-1) \\ \mathbb{O} \end{pmatrix}, \\ G(m-r-1, m)_{L_2} &= \begin{pmatrix} G(m-r-1, m-1) \\ G(m-r-2, m-1) \end{pmatrix}. \end{aligned}$$

где $\mathbb{O}$ — матрица соответствующего размера, состоящая из нулей, $G(m-r-1, m-1)$ и $G(m-r-2, m-1)$ — порождающие матрицы кодов, соответственно, $RM(m-r-1, m-1)$ и $RM(m-r-2, m-1)$. Первый столбец подматрицы $G(m-r-1, m)_{L_1}$ имеет номер $|\tilde{\alpha}_1|_2 = 1$ во всей матрице, а первый столбец подматрицы $G(m-r-1, m)_{L_2}$ имеет номер $|\tilde{\alpha}_{2^{t-1}+1}|_2 = 2^{m-1}$. Здесь символом $|\tilde{\alpha}|_2$ обозначено десятичное число, двоичное представление которого равно $\tilde{\alpha}$. Выберем теперь в качестве базиса кодов $RM(m-r-1, m-1)$ и $RM(m-r-2, m-1)$ базис, состоящий из векторов минимального веса этих кодов. Как уже отмечалось при доказательстве первого случая, векторы этого базиса имеют вид $(1 \parallel v)$, где v — вектор минимального веса кодов $RM^*(m-r-1, m-1)$ и $RM^*(m-r-2, m-1)$. Следовательно, исходная порождающая матрица $G(m-r-1, m)$ при таком выборе базиса

будет иметь вид

$$G(m-r-1, m) = \begin{pmatrix} \tilde{\alpha}_1 & & \tilde{\alpha}_{2^{t'-1}+1} & \\ 1 & v_1 & 1 & v_1 \\ 1 & v_2 & 1 & v_2 \\ \dots & \dots & \dots & \dots \\ 1 & v_{k_1} & 1 & v_{k_1} \\ 0 & \tilde{0} & 1 & w_1 \\ 0 & \tilde{0} & 1 & w_2 \\ \dots & \dots & \dots & \dots \\ 0 & \tilde{0} & 1 & w_{k_2} \end{pmatrix}.$$

Здесь k_1 и k_2 — размерности кодов $RM(m-r-1, m-1)$ и $RM(m-r-2, m-1)$ соответственно, а v_i и w_j , $1 \leq i \leq k_1$, $1 \leq j \leq k_2$ — базисы выколотых кодов Рида-Маллера $RM^*(m-r-1, m-1)$ и $RM^*(m-r-2, m-1)$ соответственно, а $\tilde{0}$ — вектор из нулей соответствующей длины.

Столбцы с номерами $|\tilde{\alpha}_1|_2$ и $|\tilde{\alpha}_{2^{t'-1}+1}|_2$ образуют подматрицу

$$\mathcal{A}_1 = \begin{pmatrix} \mathbf{1}^\downarrow & \mathbf{1}^\downarrow \\ \mathbf{0}^\downarrow & \mathbf{1}^\downarrow \end{pmatrix},$$

где символом $\mathbf{1}^\downarrow$ обозначен вектор-столбец из единиц соответствующей длины (либо k_1 , либо k_2), а символом $\mathbf{0}^\downarrow$ — вектор-столбец из нулей.

Вернемся теперь к представлению (6). К каждой из матриц $G(m-r-1, m-1)$ и $G(m-r-2, m-1)$ этого представления опять можно применить то же самое представление. В итоге получим

$$G(m-r-1, m) = (G(m-r-1, m)_{L_1} \parallel G(m-r-1, m)_{L_2} \parallel G(m-r-1, m)_{L_3} \parallel G(m-r-1, m)_{L_4}),$$

где

$$\begin{aligned} G(m-r-1, m)_{L_1} &= \begin{pmatrix} G(m-r-1, m-2) \\ \mathbb{O} \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix}, \\ G(m-r-1, m)_{L_2} &= \begin{pmatrix} G(m-r-1, m-2) \\ G(m-r-2, m-2) \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix}, \\ G(m-r-1, m)_{L_3} &= \begin{pmatrix} G(m-r-1, m-2) \\ \mathbb{O} \\ G(m-r-2, m-2) \\ \mathbb{O} \end{pmatrix}, \\ G(m-r-1, m)_{L_4} &= \begin{pmatrix} G(m-r-1, m-2) \\ G(m-r-2, m-2) \\ G(m-r-2, m-2) \\ G(m-r-3, m-2) \end{pmatrix}. \end{aligned}$$

При этом первый столбец подматрицы $G(m-r-1, m)_{L_1}$ во всей матрице имеет номер $|\tilde{\alpha}_1|_2 = 1$, первый столбец подматрицы $G(m-r-1, m)_{L_2}$ имеет номер $|\tilde{\alpha}_{2^{t'-3}+1}|_2 = 2^{m-2}$,

первый столбец подматрицы $G(m-r-1, m)_{L_3}$ имеет номер $|\tilde{\alpha}_{2^t-2+1}|_2 = 2 \cdot 2^{m-2}$, первый столбец подматрицы $G(m-r-1, m)_{L_4}$ имеет номер $|\tilde{\alpha}_{2^t-1+1}|_2 = 3 \cdot 2^{m-2}$. Как и раньше, выберем в качестве базиса кодов $RM(m-r-1, m-2)$, $RM(m-r-2, m-2)$ и $RM(m-r-3, m-2)$ базис, состоящий из векторов минимального веса этих кодов. Следовательно, исходную порождающую матрицу $G(m-r-1, m)$ можно представить в виде:

$$G(m-r-1, m) = \begin{pmatrix} \tilde{\alpha}_1 & & \tilde{\alpha}_{2^t-3+1} & & \tilde{\alpha}_{2^t-2+1} & & \tilde{\alpha}_{2^t-1+1} & \\ 1 & v_1 & 1 & v_1 & 1 & v_1 & 1 & v_1 \\ 1 & v_2 & 1 & v_2 & 1 & v_2 & 1 & v_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & v_{k_1} & 1 & v_{k_1} & 1 & v_{k_1} & 1 & v_{k_1} \\ 0 & \tilde{0} & 1 & w_1 & 0 & \tilde{0} & 1 & w_1 \\ 0 & \tilde{0} & 1 & w_2 & 0 & \tilde{0} & 1 & w_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \tilde{0} & 1 & w_{k_2} & 0 & \tilde{0} & 1 & w_{k_2} \\ 0 & \tilde{0} & 0 & \tilde{0} & 1 & w_1 & 1 & w_1 \\ 0 & \tilde{0} & 0 & \tilde{0} & 1 & w_1 & 1 & w_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \tilde{0} & 0 & \tilde{0} & 1 & w_{k_2} & 1 & w_{k_2} \\ 0 & \tilde{0} & 0 & \tilde{0} & 0 & \tilde{0} & 1 & h_1 \\ 0 & \tilde{0} & 0 & \tilde{0} & 0 & \tilde{0} & 1 & h_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \tilde{0} & 0 & \tilde{0} & 0 & \tilde{0} & 1 & h_{k_3} \end{pmatrix}.$$

Столбцы с номерами $|\tilde{\alpha}_1|_2$, $|\tilde{\alpha}_{2^t-3+1}|_2$, $|\tilde{\alpha}_{2^t-2+1}|_2$ и $|\tilde{\alpha}_{2^t-1+1}|_2$ образуют подматрицу

$$\mathcal{A}_2 = \begin{pmatrix} \mathbf{1}^\downarrow & \mathbf{1}^\downarrow & \mathbf{1}^\downarrow & \mathbf{1}^\downarrow \\ \mathbf{0}^\downarrow & \mathbf{1}^\downarrow & \mathbf{0}^\downarrow & \mathbf{1}^\downarrow \\ \mathbf{0}^\downarrow & \mathbf{0}^\downarrow & \mathbf{1}^\downarrow & \mathbf{1}^\downarrow \\ \mathbf{0}^\downarrow & \mathbf{0}^\downarrow & \mathbf{0}^\downarrow & \mathbf{1}^\downarrow \end{pmatrix}.$$

В терминах произведения Кронекера матрицу $\mathcal{A}_2$ можно выразить следующим образом. Рассмотрим матрицы A_1 и A_2 , которые получаются из матриц $\mathcal{A}_1$ и $\mathcal{A}_2$ формальным снятием с элементов символа $\downarrow$. Тогда

$$A_2 = A_1 \otimes A_1.$$

Далее, применяя рекурсивно представление (6) t раз, получим, что порождающую матрицу кода $RM(m-r-1, m)$ можно представить в таком виде, что столбцы с номерами $|\tilde{\alpha}_1|_2$, $|\tilde{\alpha}_2|_2, \dots, |\tilde{\alpha}_{2^t}|_2$ будут образовывать подматрицу $\mathcal{A}_t$ такую, что

$$A_t = A_1 \underbrace{\otimes \dots \otimes}_{t \text{ раз}} A_1.$$

Матрица A_t является верхнетреугольной матрицей с единицами на главной диагонали, следовательно, матрицу A_t можно привести к виду

$$A_t = \begin{pmatrix} 1 & \tilde{\mathbf{1}} \\ \mathbf{0}^\downarrow & E \end{pmatrix},$$

где E — единичная матрица.

Это означает, что порождающая матрица кода Рида–Маллера $RM(m - r - 1, m)$ может быть представлена в виде

$$G(m - r - 1, m) = \begin{pmatrix} \tilde{\alpha}_1 & & \tilde{\alpha}_2 & & \tilde{\alpha}_3 & & & \tilde{\alpha}_{2^t} \\ 1 & v_1 & 1 & v_1 & 1 & v_1 & \dots & 1 & v_1 \\ 1 & v_2 & 1 & v_2 & 1 & v_2 & \dots & 1 & v_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & v_{k_1} & 1 & v_{k_1} & 1 & v_{k_1} & \dots & 1 & v_{k_1} \\ 0 & f_1^1 & 1 & f_2^1 & 0 & f_3^1 & \dots & 0 & f_t^1 \\ 0 & f_1^2 & 1 & f_2^2 & 0 & f_3^2 & \dots & 0 & f_t^2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & f_1^{k_2} & 1 & f_2^{k_2} & 0 & f_3^{k_2} & \dots & 0 & f_t^{k_2} \\ 0 & g_1^1 & 0 & g_2^1 & 1 & g_3^1 & \dots & 0 & g_t^1 \\ 0 & g_1^2 & 0 & g_2^2 & 1 & g_3^2 & \dots & 0 & g_t^2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & g_1^{k_3} & 0 & g_2^{k_3} & 1 & g_3^{k_3} & \dots & 0 & g_t^{k_3} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & h_1^1 & 0 & h_2^1 & 0 & h_3^1 & \dots & 1 & h_t^1 \\ 0 & h_1^2 & 0 & h_2^2 & 0 & h_3^2 & \dots & 1 & h_t^2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & h_1^{k_t} & 0 & h_2^{k_t} & 0 & h_3^{k_t} & \dots & 1 & h_t^{k_t} \end{pmatrix}.$$

При этом первые k_1 строк являются словами минимального веса. Остальные строки, возможно, имеют больший вес Хэмминга. Полученную матрицу $G(m - r - 1, m)$ обозначим через $M(t)$.

Вернемся к доказательству второй части предложения. По теореме Мак-Элиса, вес любого кодового слова кода Рида–Маллера $RM(m - r - 1, m)$ должен делиться на $2^{\lceil (m-1)/(m-r-1) \rceil}$. Но если $m = 2r$ или $m = 2r + 1$, то

$$\left\lceil \frac{m-1}{m-r-1} \right\rceil \geq \frac{m-1}{m-r-1} \geq 2,$$

поэтому вес любого кодового слова кода $RM(m - r - 1, m)$ при $m = 2r$ или $m = 2r + 1$ должен делиться на 4.

Рассмотрим действие перестановки σ на порождающую матрицу $M(t)$ кода Рида–Маллера $RM(m - r - 1, m)$. Первые k_1 строк матрицы имеют вид $F_j = (1v_j1v_j \dots 1v_j)$, при этом $wt(F_j) = 2^{r+1}$. Под действием подстановки σ вектор F_j переходит в вектор $F'_j = (1v'_{j1}1v'_{j2} \dots 1v'_{jt})$. Если вектор F'_j не принадлежит коду Рида–Маллера $RM(m - r - 1, m)$, то, в силу представления (5) этому коду должен принадлежать вектор $F'_j \oplus w = (0v'_{j1}0v'_{j2} \dots 0v'_{jt})$, но это невозможно, так как вектор $F'_j \oplus w$ имеет вес $2^{r+1} - 2^t$, меньший кодового расстояния $d^\perp = 2^{r+1}$ кода $RM(m - r - 1, m)$. Все оставшиеся строки имеют вид $G_j = (0g_10g_20g_3 \dots 1g_j \dots 0g_t)$. Введем обозначение $g = (g_1g_2 \dots g_t)$. Очевидно, что $wt(G_j) = wt(g) + 1$. Под действием перестановки σ вектор G переходит в вектор $G'_j = (0g'_10g'_20g'_3 \dots 1g'_j \dots 0g'_t)$. Через g' обозначим вектор $g' = (g'_1g'_2 \dots g'_t)$. Тогда $wt(g') = wt(g) = wt(G_j) - 1$. Если G'_j не принадлежит коду Рида–Маллера $RM(m - r - 1, m)$, то, в силу представления (5) этому коду принадлежит вектор $w = w \oplus G'_j = (1g'_11g'_21g'_3 \dots 0g'_j \dots 1g'_t)$. Вес вектора w равен

$$wt(w) = 2^t - 1 + wt(g') = 2^t - 1 + wt(G_j) - 1 = wt(G_j) + 2^t - 2.$$

При $t > 1$ вес w не делится на 4, что невозможно в коде $RM(m - r - 1, m)$ при $m = 2r$ или $m = 2r + 1$. Полученное противоречие доказывает, что G'_j должен быть вектором кода Рида–Маллера $RM(m - r - 1, m)$.

Итак, все строки порождающей матрицы $M(t)$ кода $RM(m - r - 1, m)$ под действием σ переходят в слова кода $RM(m - r - 1, m)$, следовательно, σ — автоморфизм кода $RM(m - r - 1, m)$, а значит, и кода $RM^\perp(m - r - 1, m) = RM(r, m)$. Этим полностью доказано, что $\sigma \in \text{Aut}(w, RM(r, m))$. Обратное следует из предложения 14. Предложение 15 полностью доказано.

Теорема 7. Пусть $2r \leq m$, $0 < t \leq r$, $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$, и пусть $(k - 1)$ -мерное подпространство Π_w кода Рида–Маллера $RM(r, m)$ задается вектором w . Тогда σ переводит Π_w в подпространство кода Рида–Маллера $RM(r, m)$, если и только если $\sigma \in I(\Pi_w) \times \text{Aut}(RM(r, m))$. Если $\Gamma(\Pi_w)$ — множество перестановок, переводящих код Π_w в подкод кода $RM(r, m)$, то $\Gamma(\Pi_w) = I(\Pi_w) \times \text{Aut}(RM(r, m))$.

Доказательство. Рассмотрим следующие случаи.

Случай 1: $2r + 1 < m$ и $1 < t \leq r$. В этом случае $I(\Pi_w) = \{e\}$ в силу леммы 2. Применяя предложение 12 и учитывая, что для любой аффинной γ множество Π'_w — подкод кода $RM(r, m)$, получаем требуемое.

Случай 2: $2r \leq m$, $t = 1$, или $m = 2r$ и $t > 1$, или $m = 2r + 1$ и $t > 1$. Применяя предложение 13, получаем, что σ представима в виде $\sigma = \sigma' \gamma$, где σ' — автоморфизм кода Π_w , причем $w^{\sigma'} = w$, а γ — аффинная перестановка. Из предложения 15 следует, что σ' — перестановка из множества $I(\Pi_w) \times \text{Aut}(w, RM(r, m))$. Тем самым σ — произведение перестановки из $I(\Pi_w)$ и аффинных перестановок, и поэтому $\sigma \in I(\Pi_w) \times \text{Aut}(RM(r, m))$. Для завершения доказательства в этом случае достаточно заметить, что любая перестановка σ из множества $I(\Pi_w) \times \text{Aut}(RM(r, m))$ переводит Π_w в подкод кода $RM(r, m)$.

Предложение полностью доказано.

5. Классы эквивалентных ключей в случае $u = 2$: продолжение

После изучения подпространств кода Рида–Маллера вернемся к задаче описания классов эквивалентных ключей криптосистемы Мак–Элиса–Сидельникова.

Как было замечено ранее, задача поиска эквивалентных ключей криптосистемы Мак–Элиса–Сидельникова для случая $u = 2$ основывается на изучении множеств $\mathcal{G}(E, H)$. Напомним, что множества $\mathcal{G}(E, H)$ определяются как множества перестановок, сохраняющих структуру матрицы $(R \parallel HR)$, где R — порождающая матрица кода Рида–Маллера $RM(r, m)$ или, более формально,

$$\mathcal{G}(E, H) = \{\Gamma \in S_{2n} \mid \exists H_1, H_2 : (R \parallel HR)\Gamma = (H_1 R \parallel H_2 R)\}.$$

Далее предполагается, что матрица H имеет специальный вид $H = T_\alpha^i$. Предложение 8 сводит изучение множества $\mathcal{G}(E, H)$ к изучению перестановок P , которые переводят подпространство кода Рида–Маллера $RM(r, m)$, порождаемое матрицей R' , в некоторое другое подпространство кода Рида–Маллера $RM(r, m)$. Предложение 11 дает возможность изучать вместо перестановок P такие перестановки π , которые переводят специальный подкод Π_w , $w = \bar{x}_1 \bar{x}_2 \dots \bar{x}_{m-t}$, кода Рида–Маллера $RM(r, m)$ в любой другой подкод кода Рида–Маллера. Полное описание перестановок π получено в теореме 7. Все это позволяет доказать теорему о строении множества $\mathcal{G}(H, HT_\alpha^i)$ при $i > 1$.

Теорема 8. Пусть $RM(r, m)$ — код Риды–Маллера такой, что $2r \leq m$ и $r > 1$, i — натуральное число, большее единицы, H — любая невырожденная двоичная матрица, α — произвольный двоичный вектор, у которого в координате с номером i стоит единица. Тогда множество $\mathcal{G}(H, HT_{\alpha}^i)$ содержит те и только те перестановки Γ , которые могут быть представлены в виде $\Gamma = \Gamma' \cdot \sigma_L[1]\sigma_R[2]$, где σ_L, σ_R — автоморфизмы кода Риды–Маллера $RM(r, m)$, а для перестановки Γ' выполняются два условия:

- (1) Если $R' = (k-1) \times n$ матрица, получающаяся исключением строки с номером i из матрицы R , то $(R' \parallel R')\Gamma' = (R' \parallel R')$,
- (2) Если r_i — строка матрицы R с номером i , то $(r_i \parallel \tilde{\alpha}R)\Gamma' \in RM(r, m) \times RM(r, m)$.

Доказательство. В силу предложения 5, верно равенство $\mathcal{G}(H, HT_{\alpha}^i) = \mathcal{G}(E, T_{\alpha}^i)$. Опишем множество $\mathcal{G}(E, T_{\alpha}^i)$.

Предположим, что Γ принадлежит множеству $\mathcal{G}(E, T_{\alpha}^i)$. В силу предложения 8, найдутся две перестановки Γ' и P такие, что, во-первых, $\Gamma = \Gamma'P$, и во-вторых, $P = \sigma_L[1]\sigma_R[2]$, $\sigma_L, \sigma_R \in S_n$, и $(R' \parallel R')\Gamma' = (R' \parallel R')$. Матрица R' получается из матрицы R исключением строки с номером i . Из рассуждений, следующих после доказательства предложения 8, вытекает, что, к тому же, $(R')^{\sigma_L}$ и $(R')^{\sigma_R}$ являются подпространствами кода Риды–Маллера $RM(r, m)$.

Из предложения 11 следует, что существует аффинная перестановка π такая, что $(R')^{\pi} = \Pi_w$, где $w = \bar{x}_1\bar{x}_2 \dots \bar{x}_{m-i}$ и t — степень булевой функции с вектором значений, равным строке r_i матрицы R . Теорема 7 позволяет заключить, что $\pi^{-1}\sigma_L$ и $\pi^{-1}\sigma_R$ лежат в множестве $I(\Pi_w) \times \text{Aut}(RM(r, m))$, или, что то же самое, $\sigma_L, \sigma_R \in \pi I(\Pi_w) \times \text{Aut}(RM(r, m))$. Заметим, что $\pi I(\Pi_w)\pi^{-1} = I(R')$. Действительно, рассмотрим $\gamma = \pi\sigma\pi^{-1}$, $\sigma \in I(\Pi_w)$. Так как $(R')^{\pi} = \Pi_w$, справедливо включение $\gamma \in I(R')$. Докажем обратное. Рассмотрим $\gamma \in I(R')$. Справедлива цепочка равенств

$$(R')^{\gamma} = R' \Rightarrow (\Pi_w)^{\pi^{-1}\gamma} = (\Pi_w)^{\pi^{-1}} \Rightarrow (\Pi_w)^{\pi^{-1}\gamma\pi} = \Pi_w.$$

Тем самым $\pi^{-1}\gamma\pi \in I(\Pi_w)$, то есть $\gamma \in \pi I(\Pi_w)\pi^{-1}$. Итак, $\pi I(\Pi_w)\pi^{-1} = I(R')$. Заметив, что $\text{Aut}(RM(r, m)) = \pi^{-1} \text{Aut}(RM(r, m))$, поскольку π — аффинная перестановка, а значит, и автоморфизм кода $\text{Aut}(RM(r, m))$, получаем, что справедливы включения $\sigma_L, \sigma_R \in I(R') \times \text{Aut}(RM(r, m))$.

Итак, любая перестановка $\Gamma \in \mathcal{G}(E, T_{\alpha}^i)$ представима в виде

$$\Gamma = \Gamma'\delta'_L[1]\delta'_R[2]\sigma'_L[1]\sigma'_R[2].$$

Здесь $\delta'_R, \delta'_L \in I(R')$, а σ'_L и σ'_R являются автоморфизмами кода $RM(r, m)$. Теперь заметим, что

$$(R' \parallel R')\Gamma'\delta'_L[1]\delta'_R[2] = (R' \parallel R').$$

Для того, чтобы не вводить новых обозначений, будем далее понимать под Γ' произведение $\Gamma'\delta'_L[1]\delta'_R[2]$, а под σ_L и σ_R соответственно σ'_L и σ'_R , тогда перестановка Γ будет представима в виде $\Gamma = \Gamma'\sigma_L[1]\sigma_R[2]$, где $(R' \parallel R')\Gamma' = (R' \parallel R')$, а σ_L и σ_R — автоморфизмы кода Риды–Маллера $RM(r, m)$.

Осталось заметить, что Γ' должна переводить строку матрицы $(R \parallel T_{\alpha}^i R)$ с номером i в множество $RM(r, m) \times RM(r, m)$, в противном же случае Γ не может лежать в множестве $\mathcal{G}(E, T_{\alpha}^i)$, так как σ_L и σ_R — аффинные перестановки. Этим полностью доказана первая часть предложения.

Непосредственной проверкой легко убедиться, что все перестановки Γ , для которых справедливо разложение $\Gamma = \Gamma' \sigma_L[1] \sigma_R[2]$ и выполняются условия 1 и 2 теоремы, принадлежат множеству $\mathcal{G}(E, T_{\alpha}^i)$.

Теорема полностью доказана.

Отметим особенности рассмотренного случая. Во-первых, если в матрице R' нет одинаковых столбцов, то Γ' сохраняет матрицу $(R \parallel R)$, а значит, сама перестановка Γ принадлежит множеству $\mathcal{G}(E, E)$. Во-вторых, если в матрице R' все-таки есть два одинаковых столбца, а такое возможно, например, в случае $i = 2$, то в множестве $\mathcal{G}(H, HT_{\alpha}^i)$ возможно появление перестановок принципиально нового типа. Если до этого момента все перестановки принадлежали множеству $\mathcal{G}(E, E)$ (см., например, теоремы 2 и 4), то в множестве $\mathcal{G}(H, HT_{\alpha}^i)$ могут быть перестановки, не лежащие в множестве $\mathcal{G}(E, E)$.

Осталось привести теорему, описывающую класс эквивалентности $[(H, HT_{\alpha}^i, \Gamma)]$.

Теорема 9. Пусть $RM(r, m)$ — код Риды–Маллера такой, что $2r \leq m$ и $r > 1$, i — натуральное число, большее единицы, H — любая невырожденная двоичная матрица, α — произвольный двоичный вектор, у которого в координате с номером i стоит единица. Тогда класс эквивалентности $[(H, HT_{\alpha}^i, \Gamma)]$ состоит из кортежей вида $(HT_{\beta}^i D_1, HT_{\gamma}^i D_2, \sigma_L^{-1}[1] \sigma_R^{-1}[2] (\Gamma')^{-1} \Gamma)$. Здесь σ_L, σ_R — автоморфизмы кода Риды–Маллера $RM(r, m)$, соответствующие матрицам D_1 и D_2 , а для перестановки Γ' выполняются два условия:

- (1) Если $R' = (k-1) \times n$ матрица, получающаяся исключением строки с номером i из матрицы R , то $(R' \parallel R') \Gamma' = (R' \parallel R)$;
- (2) Если r_i — строка матрицы R с номером i , то

$$(r_i \parallel \tilde{\alpha} R) \Gamma' = (\tilde{\beta} R \parallel \tilde{\gamma} R) \in RM(r, m) \times RM(r, m).$$

Доказательство. Согласно предложению 4, класс эквивалентности $[(H, HT_{\alpha}^i, \Gamma)]$ состоит из кортежей $(H'_1, H'_2, \Gamma_g \Gamma)$, где $\Gamma_g^{-1} \in \mathcal{G}(H, HT_{\alpha}^i)$ и $(HR \parallel HT_{\alpha}^i R) \Gamma_g^{-1} = (H'_1 R \parallel H'_2 R)$. Из теоремы 8 следует, что $\Gamma_g^{-1} = \Gamma' \cdot \sigma_L[1] \cdot \sigma_R[2]$, причем для перестановки Γ' выполняются условия 1 и 2. Осталось найти матрицы H'_1 и H'_2 . Поиск этих матриц проводится так же, как и в теореме 5.

Теорема доказана.

6. Заключение

В настоящей работе рассматривалась криптосистема Мак–Элиса–Сидельникова с открытым ключом, которая является модификацией кодовой криптосистемы Мак–Элиса. Криптосистема Мак–Элиса–Сидельникова строится на основе u -кратного использования кода Риды–Маллера $RM(r, m)$. В статье исследовались вопросы структуры множества открытых ключей криптосистемы Мак–Элиса–Сидельникова.

Теорема 3 дает описание некоторых классов эквивалентности секретных ключей криптосистемы для произвольного числа блоков.

Когда криптосистема Мак–Элиса–Сидельникова строится с помощью двукратного использования ($u = 2$) кода Риды–Маллера $RM(r, m)$, задача описания некоторых множеств открытых ключей сводится к задаче изучения эквивалентных $(k-1)$ -мерных подпространств кода Риды–Маллера $RM(r, m)$. Теорема 7 описывает все подпространства

кода Рида–Маллера, эквивалентные некоторому специальному классу подпространств. Используя теорему 7, в теореме 9 получено полное описание класса эквивалентности секретных ключей криптосистемы Мак–Элиса–Сидельникова с представителями особого вида.

Список литературы

1. McEliece R. J., *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42–44. Jet Prop. Lab., Calif. Inst. Technol., Pasadena, CA, 1978.
2. Сидельников В. М., Открытое шифрование на основе двоичных кодов Рида–Маллера. *Дискретная математика* (1994) **6**, №3, 3–20.
3. Сидельников В. М., Шестаков С. О., О безопасности системы шифрования, построенной на основе обобщенных кодов Рида–Соломона. *Дискретная математика* (1992) **4**, №3, 57–63.
4. Евсеев Г. С., О сложности декодирования линейных кодов. *Проблемы передачи информации* (1983) **19**, №1, 3–8.
5. Крук Е. А., Граница для сложности декодирования линейных кодов. *Проблемы передачи информации* (1989) **25**, №3, 103–107.
6. Мак–Вильямс Ф. Дж., Слоэн Н. Дж., *Теория кодов, исправляющих ошибки*. Связь, Москва, 1979.
7. *Handbook of coding theory, I–II* (Pless V. S., Huffman W. C., eds.). Elsevier, Amsterdam, 1998.
8. Сидельников В. М., Першаков А. С., Декодирование кодов Рида–Маллера при большом числе ошибок. *Проблемы передачи информации* (1992) **28**, №3, 80–94.
9. Карпунин Г. А., О ключевом пространстве криптосистемы Мак–Элиса на основе двоичных кодов Рида–Маллера. *Дискретная математика* (2004) **16**, №2, 79–84.
10. Касами Т., Токура Н., Ивадари Е., Инагаки Я., *Теория кодирования*. Мир, Москва, 1978.
11. Kasami T., Tokura N., On the weight structure of Reed–Muller codes. *IEEE Trans. Inform. Theory* (1970) **16**, 752–759.

Статья поступила 20.08.2009.