МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чижов Иван Владимирович

Ключевое пространство криптосистемы Мак-Элиса–Сидельникова

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Научный руководитель:
Карпунин Г.А., доцент кафедры ИБ, канд.физ.-мат. наук

Москва, 2006

Оглавление

Введение

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 Р. Дж. Мак-Элисом [1]. Данная криптосистема основывается на $\mathbb{NP}$-трудной проблеме в теории кодирования. Основная идея её 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. Эта криптосистема обладает одним важным преимуществом — высокой скоростью зашифрования и расшифрования. Однако, у неё имеется серьёзный недостаток — относительно низкая скорость передачи (R). Обычно у кодовых криптосистем $R < 1$, тогда как у криптосистемы RSA скорость в точности равна 1.

В этой работе рассматривается обобщение криптосистемы Мак-Элиса, предложенное в 1994 коду В.М. Сидельниковым [2]. В этой работе модификация, предложенная В. М. Сидельниковым, называется криптосистемой Мак-Элиса–Сидельникова. Криптосистема Мак-Элиса–Сидельникова строится на основе u-кратного использования кодов Рида–Маллера $RM(r, m)$. Она имеет высокую криптографическую стойкость, скорость передачи близкую к 1 и сравнительно невысокую сложность шифрования секретных сообщений и расшифрования криптограмм этих сообщений.

В работе исследуются вопросы, связанные с пространством эквивалентных секретных ключей, то есть секретных ключей, порождающих одинаковые открытые ключи, новой криптосистемы. Опишем краткое содержание разделов работы.

В § 1 даётся определение криптосистемы Мак-Элиса, описываются её секретный и открытый ключи. Приводятся алгоритмы зашифрования и расшифрования.

В § 2 изучается ключевое пространство криптосистемы Мак-Элиса. Устанавливается связь классов эквивалентностей секретных ключей с группой автоморфизмов линейного кода, лежащего в основе этой криптосистемы.

В § 3 описывается криптосистема Мак-Элиса–Сидельникова: секретный и открытый ключи, алгоритмы зашифрования и расшифрования.

§ 4 посвящён ключевому пространству новой криптосистемы. В нём

вводятся множества, необходимые для описания классов эквивалентности секретных ключей. Получаются нижние и верхние оценки на мощности введённых множеств и на число открытых ключей криптосистемы Мак-Элиса–Сидельникова.

В § 5 изучается криптосистема Мак-Элиса–Сидельникова в случае двух блоков ($u = 2$).

В настоящей работе получаются нижние оценки на мощность множества открытых ключей криптосистемы Мак-Элиса–Сидельникова (теорема 4.3) при использовании произвольного числа блоков u. Для кодов Рида–Маллера с u-кратным повторением строится множество, которое, в некотором смысле, является аналогом группы автоморфизмов обычного кода Рида–Маллера, и устанавливается связь этого множества с классами эквивалентности секретных ключей.

Для случая двух блоков ($u = 2$) полностью описывается указанное множество при использовании кодов Рида–Маллера $RM(r, m)$ ($r \leqslant 2, r < m$) и матриц определённого вида (теоремы 5.1, 5.2). Тем самым при $u = 2, r \geqslant 2, r < m$ описываются все классы эквивалентности секретных ключей с представителями особого вида и вычисляются их мощности. Для некоторых классов эквивалентности секретных ключей приводятся нижние оценки на их мощность (теоремы 5.1 и 5.2).

1. Криптосистема Мак-Элиса

Опишем устройство криптосистемы с открытым ключом, предложенной Р. Дж. Мак-Элисом [1].

Пусть $\mathscr{C}$ — некоторый линейный код с параметрами $[n, k, d]$ над конечным полем F_q, который имеет эффективные алгоритмы декодирования, G — его порождающая матрица размера $k \times n$, H — невырожденная $k \times k$ матрица и Γ — перестановочная матрица размера $n \times n$. Секретным ключом в данной схеме является тройка (H, G, Γ), а открытым ключом — матрица $G' = H \cdot G \cdot \Gamma$. В оригинальной криптосистеме Мак-Элиса [1] матрица G выбирается случайно из множества всех порождающих матриц некоторого класса линейных кодов, например кодов Гоппы, с заданными параметрами. Следует отметить, что иногда в секретный ключ не включается матрица G, а она фиксируется и сообщается всем абонентам по открытому каналу. Это связано с тем, что используемый класс линейных кодов, например код Рида–Маллера RM(r,m), состоит из одного единственного кода. Именно такая криптосистема рассматривается в работах В. М. Сидельникова [2] и В. М. Сидельникова, С. О. Шестакова [3]. Везде в этой работе предполагается, что матрица G — фиксированная.

Опишем алгоритм зашифрования. На его вход подаётся открытое сообщение m, которое является k-мерным вектором над полем F_q. На выходе алгоритма образуется n-мерный вектор c, который и является криптограммой открытого сообщения.

Алгоритм Зашифрования.

1. Вычислить $c' = mH \cdot G \cdot \Gamma = mG'$.
2. Выбрать случайный n–мерный вектор e веса $wt(\mathrm{e}) = \lfloor \frac{d-1}{2} \rfloor$.
3. Вычислить $c = c' + \mathrm{e}$.

Опишем устройство алгоритма расшифрования. На его вход подаётся криптограмма c — n-мерный вектор над полем F_q, а выходом является вектор m — зашифрованное сообщение.

Алгоритм Расшифрования.

1. Вычислить $c' = c\Gamma^{-1}$;

2. Декодировать c', то есть представить его в виде $c' = aG + e'$, где $a = mH \in \mathscr{C},\ wt(e') = \lfloor \frac{d-1}{2} \rfloor$;

3. Вычислить секретное сообщение $m = aH^{-1}$.

Шаг 2 возможно выполнить в силу того, что перестановочная матрица Г не изменяет веса вектора e, участвующего в алгоритме шифрования, а только переставляет его координаты.

Злоумышленнику же проделать шаги алгоритма расшифрования сложно, так как он не знает матриц H и Г, поэтому ему трудно декодировать код $\mathscr{C}$ с порождающей матрицей G, который для него является кодом общего положения, а задача декодирования такого кода является $\mathbb{NP}$-трудной.

Известно [4, 5], что сложность N декодирования линейного кода общего положения имеет вид $N = 2^{c \cdot min(k, n-k)}$. Откуда видно, что, даже при сравнительно небольших параметрах k и $n - k$, вычислительная сложность декодирования таких кодов является неприемлемо высокой.

В оригинальной криптосистеме Мак-Элиса в качестве матрицы G была выбрана порождающая матрица двоичного кода Гоппы с параметрами $[n = 1024, k \geqslant 524, d \geqslant 101]$ над полем $\mathbb{F}_2$. Однако, можно использовать порождающие матрицы любого другого кода, имеющего быстрые и эффективные алгоритмы декодирования. Но не все коды могут обеспечить необходимую стойкость криптосистемы Мак-Элиса. Так, например, В. М. Сидельников и С. О. Шестаков [3] построили эффективный алгоритм поиска секретного ключа по известному открытому в случае использования порождающей матрицы обобщённого кода Рида–Соломона.

2. Ключевое пространство криптосистемы Мак-Элиса.

В исследованиях криптосистем с открытым ключом возникает вопрос о числе открытых ключей, так как некоторые разные секретные ключи могут порождать одинаковые открытые ключи. Если этих ключей достаточно мало, то злоумышленник сможет эффективно строить по открытому ключу некоторого легального абонента свой секретный ключ. Что даст ему возможность читать все секретные сообщения, приходящие в адрес абонента. Идеально, когда в криптосистеме любые два различных секретных ключа порождают неравные друг другу открытые ключи. Однако, часто в кодовых криптосистемах это не так. В связи с чем возникает естественный вопрос, а сколько всего открытых ключей.

Везде в этом параграфе предполагается, что в криптосистеме Мак-Элиса в качестве порождающей матрицы кода $\mathscr{C}$ была выбрана матрица G, а сам код имеет длину равную n, размерность — k и кодовое расстояние — d. Легальный абонент в качестве своего секретного ключа выбрал тройку (H, G, Γ) (здесь G включается в секретный ключ для удобства, на самом деле, G — общедоступная матрица, выбираемая заранее), тогда соответствующий открытый ключ будет равен произведению этих матриц $H \cdot G \cdot \Gamma$. Введём отношение эквивалентности секретных ключей следующим способом

Определение 2.1. Два секретных ключа (H', G, Γ') и (H'', G, Γ'') назовём *эквивалентными*, если и только если выполняется соотношение

$$H' \cdot G \cdot \Gamma' = H'' \cdot G \cdot \Gamma'',$$

то есть порождаемые ими открытые ключи совпадают.

Легко видеть, что данное отношение — отношение эквивалентности. Тем самым всё множество секретных ключей разбивается на классы эквивалентности. В дальнейшем класс с представителем (H, G, Γ) будем обозначать как $[(H, G, \Gamma)]$

Важную роль в исследовании классов эквивалентности $[(H, G, \Gamma)]$ играет группа автоморфизмов кода $\mathscr{C}$, напомним ее определение.

Определение 2.2. *Группой автоморфизмов* кода $\mathscr{C}$ называется множество

$$Aut(\mathscr{C}) = \{\Gamma \in S_n | \exists\, A \in GL_k(F_q) : G\Gamma = AG\},$$

где S_n — симметрическая группа степени n, $GL_k(F_q)$ — группа всех невырожденных $k \times k$-матриц над полем F_q, а перестановка $\Gamma \in S_n$ представляется перестановочной $k \times k$-матрицей, которая действует на G как соответствующая перестановка столбцов.

С группой автоморфизмов неразрывно связано множество $\mathscr{A}(\mathscr{C})$ невырожденных $k \times k$-матриц, задающих перестановки из группы автоморфизмов, то есть

$$\mathscr{A}(\mathscr{C}) = \{A \in GL_k(F_q) | \exists\, \Gamma \in Aut(G) : AG = G\Gamma\}.$$

Утверждение 2.1. *Пусть кодовое расстояние кода $\mathscr{C}^\perp$, дуального к коду $\mathscr{C}$, строго больше двух. Тогда для любой матрицы $A \in GL_k(F_q)$, принадлежащей множеству $\mathscr{A}(\mathscr{C})$, существует и единственная перестановка Γ из группы автоморфизмов $Aut(\mathscr{C})$. И для любой перестановки $\Gamma \in Aut(\mathscr{C})$ существует и единственная матрица $A \in \mathscr{A}(\mathscr{C})$.*

Доказательство. Пусть A принадлежит $\mathscr{A}(\mathscr{C})$, тогда найдётся перестановка Γ такая, что

$$AG = G\Gamma.$$

Очевидно, что $\Gamma \in Aut(\mathscr{C})$. Докажем, что такая Γ единственна. Пусть существуют две перестановки Γ' и Γ'' такие, что

$$AG = G\Gamma' \quad AG = G\Gamma''.$$

Тогда

$$G\Gamma'\Gamma''^{-1} = G.$$

В силу того, что кодовое расстояние $\mathscr{C}^\perp$ строго больше двух, то в матрице G нет двух одинаковых столбцов. Поэтому из последнего соотношения следует, что

$$\Gamma'\Gamma''^{-1} = E.$$

Полученное соотношение, означает, что $\Gamma' = \Gamma''$.

Докажем, что для $\Gamma \in Aut(\mathscr{C})$ найдётся единственная матрица $A \in \mathscr{A}(\mathscr{C})$. В силу того, что $\Gamma \in Aut(\mathscr{C})$, то существует A, с которой

$$AG = G\Gamma.$$

Понятно, что $A \in \mathscr{A}(\mathscr{C})$. Если найдутся две матрицы A' и A'' такие, что

$$A'G = G\Gamma \quad A''G = G\Gamma,$$

то $A'G = A''G$. Ранг матрицы G равен k, поэтому $A' = A''$.

Утверждение полностью доказано. □

Известно следующее утверждение, устанавливающее связь между группой автоморфизмов кода $\mathscr{C}$ с порождающей матрицей G и эквивалентными ключами криптосистемы Мак-Элиса.

Утверждение 2.2. *Пусть в качестве порождающей матрицы кода $\mathscr{C}$ в криптосистеме Мак-Элиса взята матрица G. Тогда существует взаимно однозначное соответствие между множеством $Aut(\mathscr{C})$ и классом эквивалентности $[(H, G, \Gamma)]$ множества секретных ключей криптосистемы Мак-Элиса.*

Доказательство. Действительно, поставим секретному ключу $(H', G, \Gamma') \in [(H, G, \Gamma)]$ в соответствие перестановку $\Gamma'\Gamma^{-1}$. Докажем, что это перестановка принадлежит группе автоморфизмов кода $\mathscr{C}$. В силу того, что (H', G, Γ') принадлежит классу $[(H, G, \Gamma)]$, то выполняется соотношение

$$HG\Gamma = H'G\Gamma'.$$

Умножая правую и левую его части справа на матрицу Γ^{-1}, а слева на H'^{-1}, получаем, что для перестановки $\Gamma'\Gamma^{-1}$ справедливо соотношение

$$H'^{-1}HG = G\Gamma'\Gamma^{-1}.$$

Последнее и означает, что $\Gamma'\Gamma^{-1}$ принадлежит группе автоморфизмов кода $\mathscr{C}$. Очевидно, данное отображение сюръективно. Покажем, что оно инъективно. Пусть существуют два секретных ключа (H', G, Γ') и (H'', G, Γ'') из класса эквивалентности $[(H, G, \Gamma)]$, для которых $\Gamma'\Gamma^{-1} = \Gamma''\Gamma^{-1}$. Тогда, $\Gamma' = \Gamma''$. И, так как $H'G\Gamma' = H''G\Gamma''$, то равны матрицы H' и H''. Из всего сказанного следует, что ключи (H', G, Γ') и (H'', G, Γ'') совпадают.

Утверждение полностью доказано. □

Утверждение 2.3. *Класс эквивалентности* $[(H, G, \Gamma)]$ *состоит из всех троек вида* $(H \cdot D_{\Gamma_A}, G, \Gamma_A^{-1} \cdot \Gamma)$, *где* $\Gamma_A \in Aut(\mathscr{C})$, *а* $D_{\Gamma_A} G = G\Gamma_A$.

Доказательство. При доказательстве утверждения 2.2 было получено, что для любого элемента $(H', G, \Gamma') \in [(H, G, \Gamma)]$ матрица $H'^{-1}H$ принадлежит множеству $\mathscr{A}(\mathscr{C})$, а $\Gamma'\Gamma^{-1}$ — соответствующая перестановка из группы автоморфизмов кода $\mathscr{C}$, то есть $\Gamma'\Gamma^{-1} \in Aut(\mathscr{C})$. Если теперь положить $D_{\Gamma_A} = H'^{-1}H$ и $\Gamma_A = \Gamma'\Gamma^{-1}$, то получим требуемое. □

Из этого утверждения немедленно получаем формулу для мощности множества открытых ключей, которая совпадает с числом классов эквивалентности секретных ключей.

Утверждение 2.4. *Пусть* $\mathscr{C}$ *— множество всех открытых ключей криптосистемы Мак–Элиса. Тогда справедлива формула*

$$|\mathscr{C}| = \frac{n! h_k(q)}{|Aut(\mathscr{C})|},$$

здесь $h_k(q) = |GL_k(F_q)| = (q^k - 1)(q^k - q) \dots (q^k - q^{k-1})$ *— число невырожденных матриц порядка* k *над полем* F_q.

Доказательство. Из утверждения 2.2 следует, что каждый класс эквивалентности состоит из одного и того же числа элементов, а именно из $|Aut(\mathscr{C})|$ элементов, поэтому число классов, а значит и число открытых ключей, будет равно отношению общего числа секретных ключей к мощности класса эквивалентности. Всего секретных ключей столько сколько пар (H, Γ), где H — невырожденная $k \times k$-матрица, а Γ — перестановочная $n \times n$-матрица. Число матриц H равно $h_k(q)$, а число всех перестановок — $n!$, поэтому общее число пар (H, Γ) в точности равно $n! h_k(q)$. Учитывая всё сказанное, получаем требуемую формулу. □

Заметим, что формула утверждения 2.4 даёт также общее число классов эквивалентности секретных ключей криптосистемы Мак-Элиса.

Тем самым вопрос изучения классов эквивалентности секретных ключей криптосистемы Мак-Элиса сводится к известной и трудной задаче теории кодирования — описание группы автоморфизмов кода.

Одним из примеров кодов, для которых полностью вычислена группа автоморфизмов, является двоичный код Рида–Маллера $RM(r, m)$, см. например [6]. Его группа автоморфизмов $Aut(RM(r, m))$ представляет из себя

полную аффинную группу пространства F_2^m. Мощность этой группы равна $2^m h_m(2)$. Поэтому справедливо утверждение.

Утверждение 2.5. *Общее число открытых ключей в криптосистеме Мак-Элиса, в которой в качестве матрицы G была выбрана порождающая матрица двоичного кода Рида–Маллера, вычисляется по формуле*

$$|\mathscr{E}| = \frac{n! h_k}{2^m h_m},$$

здесь $h_k = h_k(2)$ и $h_m = h_m(2)$.

Информацию о группах автоморфизмов других известных кодов можно найти в [7].

3. Криптосистема Мак-Элиса–Сидельникова

В. М. Сидельников в работе [2] провёл криптографический анализ криптосистемы Мак-Элиса, в которой в качестве кода $\mathscr{C}$ выбирался двоичный код Рида–Маллера $RM(r,m)$ с порождающей матрицей R. В результате криптоанализа В. М. Сидельников пришёл к выводу, что на сегодняшний день данная криптосистема не обеспечивает необходимого уровня стойкости. В этой же работе автор предложил некоторую её модификацию. Опишем конструкцию, предложенную В. М. Сидельниковым.

Определение 3.1. *Кодом Рида–Маллера* $RM(r,m)$, называется множество векторов значений Ω_f всех булевых функций $f(y_1,\ldots,y_m)$, степень нелинейности (максимальная длина монома, входящего в полином Жегалкина функции f) которых не превосходит r, то есть

$$RM(r,m) = \{\Omega_f = (x_1,\ldots,x_n), n = 2^m | \\ f(y_1,\ldots,y_m) = a_0 \oplus \bigoplus_{s=1}^{t} \bigoplus_{1\leqslant i_1<\ldots<i_s\leqslant m} a_{i_1,\ldots,i_s} y_{i_1}\ldots y_{i_s},\ t \leqslant r\}$$

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]. Обозначим через R порождающую матрицу кода Рида–Маллера $RM(r,m)$, которая состоит из единичного вектора и векторов-значений всех мономов от m переменных степени нелинейности не превосходящей r.

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

где $G_0 = (1,1\ldots,1)$,

$$G_1 = \begin{pmatrix} \Omega_{y_m} \\ \vdots \\ \Omega_{y_2} \\ \Omega_{y_1} \end{pmatrix}, G_2 = \begin{pmatrix} \Omega_{y_{m-1}y_m} \\ \vdots \\ \Omega_{y_1y_3} \\ \Omega_{y_1y_2} \end{pmatrix}, G_r = \begin{pmatrix} \Omega_{y_{m-r+1}y_{m-r+2}\cdots y_m} \\ \vdots \\ \Omega_{y_1y_2\ldots y_{r-1}y_{r+1}} \\ \Omega_{y_1y_2\ldots y_{r-1}y_r} \end{pmatrix}$$

Матрицу R ещё будем называть *стандартной формой* порождающей матрицы кода Рида–Маллера $RM(r,m)$.

Секретным ключом криптосистемы уже являются не две матрицы, а кортеж

$$(H_1, H_2, \ldots, H_u, \Gamma).$$

Здесь $H_1, H_2, \ldots, H_u$ — невырожденные $k \times k$-матрицы над полем $F_2 = \{0, 1\}$, которые выбираются случайно и равновероятно из множества всех двоичных невырожденных $k \times k$-матриц. Матрица Γ имеет размеры $u \cdot n \times u \cdot n$ и является перестановочной, то есть в каждой её строчке и в каждом столбце стоит ровно одна единица. Заметим, что в секретный ключ не включается матрица R, так как это не имеет смысла в силу единственности кода Рида–Маллера $RM(r, m)$.

Открытым ключом криптосистемы Мак-Элиса–Сидельникова является матрица

$$G' = (H_1 R \| H_2 R \| \ldots \| H_u R) \cdot \Gamma,$$

где символом $\|$ обозначена конкатенация матриц. Алгоритм зашифрования в такой криптосистеме почти не отличается от классического. Для зашифрования секретного сообщения m, длины k нужно

Алгоритм Зашифрования.

1. Вычислить $c' = mG'$.
2. Выбрать случайный $(u \cdot n)$–мерный вектор e такой, что для его веса выполняется $wt(\mathrm{e}) \leqslant u \cdot \lfloor \frac{d-1}{2} \rfloor + u - 1$.
3. Вычислить $c = c' + \mathrm{e}$.

Следует заметить, что длина криптограммы c равна un. Из алгоритма зашифрования видно, что в криптосистеме Мак-Элиса–Сидельникова каждое открытое сообщение имеет большее число возможных криптограмм, чем в оригинальной криптосистеме. Опишем теперь алгоритм расшифрования криптограммы c.

Алгоритм Расшифрования.

1. Вычислить $c' = c\Gamma^{-1}$.
2. Представить вектор c' в виде $c' = (c'_1 \| \ldots \| c'_u)$, где $c'_i \in F_2^n$.
3. Каждый вектор c'_i попытаться представить в виде $c'_i = a_i R + e'_i$, для некоторого $a_i \in F_2^k$ и некоторого вектора ошибок $e'_i \in F_2^n$ веса, не превосходящего $\lfloor \frac{d-1}{2} \rfloor$.

4. Взять любое c'_i, которое удалось представить в виде, указанном в пункте 3.

5. Вычислить $m = a_i H_i^{-1}$.

Заметим, что алгоритм расшифрования корректен. Действительно, вектор c' отстоит от кода с порождающей матрицей $(H_1 R \| \ldots \| H_u R)$ на расстояние не превосходящее $u \cdot \lfloor \frac{d-1}{2} \rfloor + u - 1$. Следовательно, найдётся вектор c'_i, отличающийся от некоторого вектора кода $RM(r, m)$ не более, чем в $\lfloor \frac{d-1}{2} \rfloor$ позициях. Именно для этого вектора и удастся получить разложение из пункта 3 алгоритма зашифрования.

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]. Очевидный недостаток — низкая скорость передачи, которая здесь хуже, чем в оригинальной схеме на основе тех же самых кодов.

Одно из самых первых направлений исследования новой криптосистемы — изучение множества открытых ключей. Обозначим через $\mathscr{E}$ множество всех открытых ключей криптосистемы Мак-Элиса–Сидельникова. Возникает вопрос о мощности множества $\mathscr{E}$. В. М. Сидельников в своей работе [2] предложил следующую гипотезу

$$|\mathscr{E}| = \frac{(un)!(h_k)^u}{u!|Aut(RM(r,m))|^u},$$

где $h_k = (2^k - 1)(2^k - 2) \ldots (2^k - 2^{k-1})$ — число невырожденных матриц размерности k над полем F_2; $|Aut(RM(r,m))| = 2^m(2^m - 1) \ldots (2^m - 2^{m-1})$ — мощность группы автоморфизмов кода Рида-Маллера $RM(r,m)$.

Эта гипотеза оказалась ошибочной. Г. А. Карпунин доказал [9], что

$$|\mathscr{E}| < \frac{(un)!(h_k)^u}{u!|Aut(RM(r,m))|^u}.$$

Он также полностью описал множество открытых ключей $\mathscr{E}$ для случая кода $RM(1,m)$ при $u = 2$ и вычислил его мощность.

4. Множество открытых ключей криптосистемы Мак-Элиса—Сидельникова

Дадим следующее определение эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова.

Определение 4.1. Секретные ключи $(H_1, H_2, \ldots, H_u, \Gamma)$ и $(H'_1, H'_2, \ldots, H'_u, \Gamma')$ назовём *эквивалентными*, если соответствующие им открытые ключи совпадают, то есть выполняется соотношение

$$(H_1R\|H_2R\|\ldots\|H_uR)\cdot\Gamma = (H'_1R\|H'_2R\|\ldots\|H'_uR)\cdot\Gamma'.$$

Заметим, что данное отношение действительно является отношение эквивалентности. Тем самым всё множество секретных ключей разбивается на классы эквивалентности и число классов эквивалентности совпадает с числом открытых ключей. Рассмотрим множество

$$\begin{aligned}\mathcal{G}(H_1, H_2, \ldots, H_u) \;=\; &\{\Gamma \in S_{un} : \exists H'_1, H'_2, \ldots H'_u \text{ такие, что}\\ &(H_1R\|H_2R\|\ldots\|H_uR)\Gamma = (H'_1R\|H'_2R\|\ldots\|H'_uR)\}\end{aligned}$$

Как и раньше класс эквивалентности с представителем $(H_1, \ldots, H_u, \Gamma)$ будем обозначать так: $[(H_1, \ldots, H_u, \Gamma)]$.

Справедлива следующая теорема.

Теорема 4.1. *Существует взаимно однозначное отображение между классом* $[(H_1, H_2, \ldots, H_u, \Gamma)]$ *и множеством* $\mathcal{G}(H_1, H_2, \ldots, H_u)$.

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

$$(H_1R\|H_2R\|\ldots\|H_uR)\Gamma = (M_1R\|M_2R\|\ldots\|M_uR)\Gamma'$$

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

Докажем, что f — инъекция. Пусть два ключа

$$(A_1, A_2, \ldots, A_u, \Gamma_1) \text{ и } (B_1, B_2, \ldots, B_u, \Gamma_2)$$

из рассматриваемого класса эквивалентности переводятся с помощью f в перестановки $\Gamma\Gamma_1^{-1}$ и $\Gamma\Gamma_2^{-1}$ соответственно, так, что $\Gamma\Gamma_1^{-1} = \Gamma\Gamma_2^{-1}$. Тогда $\Gamma_1 = \Gamma_2$, а значит и

$$A_1 = B_1, A_2 = B_2, \ldots, A_u = B_u,$$

то есть ключи совпадают.

Теперь рассмотрим перестановку Γ_g из множества $\mathcal{G}(H_1, H_2, \ldots, H_u)$. Тогда для Γ_g найдутся такие матрицы $H_1', H_2', \ldots, H_u'$, что

$$(H_1R\|H_2R\|\ldots\|H_uR)\cdot\Gamma_g = (H_1'R\|H_2'R\|\ldots\|H_u'R).$$

Положим

$$\Gamma' = \Gamma_g^{-1}\Gamma, M_1 = H_1', \ldots, M_1 = H_u'.$$

В этом случае

$$(H_1'R\|H_2'R\|\ldots\|H_u'R)\cdot\Gamma_g^{-1}\Gamma = (H_1R\|H_2R\|\ldots\|H_uR)\Gamma,$$

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

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

Следствие 4.1. *Справедлива формула для мощности класса эквивалентности*

$$|[(H_1, H_1, \ldots, H_u, \Gamma)]| = |\mathcal{G}(H_1, H_2, \ldots, H_u)|$$

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

Далее установим связь множества $\mathcal{G}(H_1, \ldots, H_u)$ с множеством

$$\begin{aligned}\mathcal{L}(H_1, \ldots, H_u) \;=\; &\{(A_1, \ldots, A_u) - \text{кортеж невырожденных матриц,}\\ &\text{для которых существует перестановка } \Gamma \in S_{un} :\\ &(H_1R\|\ldots\|H_uR)\Gamma = (A_1R\|\ldots\|A_uR).\}\end{aligned}$$

Утверждение 4.1. *Зафиксируем некоторые невырожденные двоичные $k \times k$-матрицы $H_1, \ldots, H_u$. Тогда множество $\mathcal{G}(H_1, \ldots, H_u)$ можно представить в виде объединения непересекающихся множеств*

$$\mathcal{G}(H_1, \ldots, H_u) = \bigcup_{(A_1,\ldots,A_u)\in\mathcal{L}(H_1,\ldots,H_u)} \{\gamma_\varphi\Gamma_{A_1,\ldots,A_u} | \gamma_\varphi \in \Gamma_\varphi(H_1, \ldots, H_u)\}.$$

здесь $\Gamma_{A,\ldots,A_u}$ *— некоторая перестановка из* S_{un}*, для которой*

$$(H_1R\| \ldots \|H_uR)\Gamma_{A_1,\ldots,A_u} = (A_1R\| \ldots \|A_uR).$$

Символом $\Gamma_\varphi(H_1, \ldots, H_u)$ *обозначено множество таких перестановок* $\gamma_\varphi \in S_{un}$*, что*

$$(H_1R\|H_2R\| \ldots \|H_uR)\gamma_\varphi = (H_1R\|H_2R\| \ldots \|H_uR).$$

Доказательство. Из определения множества $\mathcal{G}(H_1, \ldots, H_u)$ следует, что

$$\mathcal{G}(H_1, \ldots, H_u) = \bigcup_{A_1,\ldots,A_u} \{\Gamma \in S_{un} : (H_1|| \ldots ||H_u)\Gamma = (A_1R|| \ldots ||A_uR)\}.$$

Очевидно, что множества, стоящие под знаком объединения не пересекаются. Далее, пусть существуют две перестановки $\Gamma_1, \Gamma_2 \in S_{un}$ такие, что

$$\begin{aligned}(H_1R\| \ldots \|H_uR)\Gamma_1 &= (H'_1R\| \ldots \|H'_uR)\\ (H_1R\| \ldots \|H_uR)\Gamma_2 &= (H'_1R\| \ldots \|H'_uR).\end{aligned}$$

Тогда

$$(H_1R\| \ldots \|H_uR)\Gamma_2\Gamma_1^{-1} = (H_1R\| \ldots \|H_uR).$$

Тем самым перестановка $\Gamma_2\Gamma_1^{-1}$ принадлежит множеству $\Gamma_\varphi(H_1, \ldots, H_u)$. Обратно, если для перестановки Γ_1 выполнено соотношение

$$(H_1R\| \ldots \|H_uR)\Gamma_1 = (H'_1R\| \ldots \|H'_uR), \tag{4.1}$$

то для любой $\gamma_\varphi \in \Gamma_\varphi(H_1, \ldots, H_u)$ перестановка $\Gamma_2 = \gamma_\varphi\Gamma_1$ также удовлетворяет (4.1). Тем самым доказано, что любое непустое множество $\{\Gamma \in S_{un} : (H_1|| \ldots ||H_u)\Gamma = (A_1R|| \ldots ||A_uR)\}$, стоящее под знаком объединения равно следующему множеству $\{\gamma_\varphi\Gamma_{A_1,\ldots,A_u} | \gamma_\varphi \in \Gamma_\varphi(H_1, \ldots, H_u)\}$, где $\Gamma_{A,\ldots,A_u}$ — некоторая перестановка из S_{un}, для которой

$$(H_1R\| \ldots \|H_uR)\Gamma_{A_1,\ldots,A_u} = (A_1R\| \ldots \|A_uR).$$

Для завершения доказательства осталось заметить, что множества, стоящие под знаком объединения не пустые, если и только если кортеж $(A_1, \ldots, A_u)$ принадлежит множеству $\mathcal{L}(H_1, \ldots, H_u)$.

Утверждение полностью доказано. □

Следствием предыдущего утверждения является формула, связывающая мощности множеств $\mathcal{G}(H_1, \ldots, H_u)$ и $\mathcal{L}(H_1, \ldots, H_u)$.

Утверждение 4.2. *Справедлива формула*

$$|\mathcal{G}(H_1, \ldots, H_u)| = |\Gamma_\varphi(H_1, \ldots, H_u)| \cdot |\mathcal{L}(H_1, \ldots, H_u)|.$$

Занумеруем все столбцы матрицы $(H_1R\| \ldots \|H_uR)$ числами от 1 до un. Обозначим через $\mathcal{N}^u$ множество всех номеров от 1 до un, то есть $\mathcal{N}^u = \{1, 2, \ldots, un\}$. Пусть также для любого $i \in \mathcal{N}^u$ $(H_1R\| \ldots \|H_uR)_i$ — i-тый столбец матрицы $(H_1R\| \ldots \|H_uR)$.

Следующее утверждение описывает строение множества $\Gamma_\varphi(H_1, \ldots, H_u)$.

Утверждение 4.3. *Перестановка* Γ *принадлежит множеству* $\Gamma_\varphi(H_1, \ldots, H_u)$*, если и только если для любых* $i, j \in \mathcal{N}^u$*, таких что* $\Gamma(i) = j$*, выполняется равенство*

$$(H_1R\| \ldots \|H_uR)_i = (H_1R\| \ldots \|H_uR)_j.$$

Доказательство. Немедленно следует из того, что Γ принадлежит множеству $\Gamma_\varphi(H_1, \ldots, H_u)$ тогда и только тогда, когда верно равенство

$$(H_1R\| \ldots \|H_uR)\Gamma = (H_1R\| \ldots \|H_uR).$$

□

Выясним некоторые свойства множества $\mathcal{L}(H_1, \ldots, H_u)$. Обозначим через
$\mathcal{A}(RM(r, m))$ множество матриц, которые задают перестановки, принадлежащие группе автоморфизмов кода $RM(r, m)$ с порождающей матрицей R, то есть

$$\mathcal{A}(RM(r, m)) = \{A | \exists \Gamma \in Aut(RM(r, m)) : AR = R\Gamma\}.$$

Утверждение 4.4. *Пусть кортеж* $(A_1, \ldots, A_u)$ *принадлежит множеству* $\mathcal{L}(H_1, \ldots, H_u)$*. Тогда для любых матриц* $D_1, \ldots, D_u \in \mathcal{A}(RM(r, m))$ *и любой перестановки* $\Gamma \in S_u$ *кортеж*

$$(A_{\Gamma(1)}D_1, \ldots, A_{\Gamma(u)}D_u)$$

также принадлежит множеству $\mathcal{L}(H_1, \ldots, H_u)$*.*

Доказательство. Зафиксируем любые матрицы $D_1, \ldots, D_u \in \mathcal{A}(RM(r,m))$ и любую перестановку $\Gamma \in S_u$. Тогда для матриц $D_1, \ldots, D_u$ найдутся перестановки $\Gamma_1, \ldots, \Gamma_u$, принадлежащие S_n, такие что

$$D_i R = R\Gamma_i, \ \forall i = 1, \ldots, u.$$

Далее, по перестановке Γ построим перестановку $\widetilde{\Gamma} \in S_{un}$, которая моделирует действие перестановки Γ, то есть $\widetilde{\Gamma}$ переставляет конкатенируемые блоки $A_i R$ так, что $(A_1 R || \ldots || A_u R)\widetilde{\Gamma} = (A_{\Gamma(1)} R || \ldots || A_{\Gamma(u)} R)$. Так как кортеж $(A_1, \ldots, A_u)$ принадлежит множеству $\mathcal{L}(H_1, \ldots, H_u)$, то найдётся перестановка $P \in S_{un}$ такая, что

$$(H_1 R \| \ldots \| H_u R)P = (A_1 R \| \ldots \| A_u R).$$

Теперь построим перестановку $\Gamma_P = P\widetilde{\Gamma}(\Gamma_1 \| \ldots \| \Gamma_u)$. Легко проверить, что кортеж $(A_{\Gamma(1)} D_1, \ldots, A_{\Gamma(u)} D_u)$ будет удовлетворять соотношению, задающему множество $\mathcal{L}(H_1, \ldots, H_u)$ именно с перестановкой Γ_P. □

Утверждение 4.4 позволяет разбить всё множество $\mathcal{L}(H_1, \ldots, H_u)$ на классы эквивалентности.

Определение 4.2. Назовём два кортежа $(A_1, \ldots, A_u)$ и $(B_1, \ldots, B_u)$ из множества $\mathcal{L}(H_1, \ldots, H_u)$ *эквивалентными*, если

$$\exists \Gamma \in S_u : \forall i = 1, \ldots, u \ A_i^{-1} B_{\Gamma(i)} \in \mathcal{A}(RM(r,m)).$$

В дальнейшем класс эквивалентности в множестве $\mathcal{L}(H_1, \ldots, H_u)$ будем называть *A-классом*. *A*-класс с представителем $(H_1, \ldots, H_u)$ будем обозначать следующим образом: $A[(H_1, \ldots, H_u)]$.

Для выяснения дальнейших свойств множества $\mathcal{L}(H_1, \ldots, H_u)$ потребуется следующая лемма.

Лемма 4.1. *Рассмотрим $H_1, \ldots, H_u$ — последовательность невырожденных матриц. Если существует номер i такой, что для любого $j = 1, \ldots, u$ матрица $H_i^{-1} H_j$ принадлежит $\mathcal{A}(RM(r,m))$, то для любых $k, l = 1, 2, \ldots, u$ матрица $H_k^{-1} H_l$ принадлежит $\mathcal{A}(RM(r,m))$.*

Доказательство. Заметим, что множество $\mathcal{A}(RM(r,m))$ является группой в силу того, что $Aut(RM(r,m))$ — группа. Возьмём две любые матрицы H_k

и H_l из кортежа, по условию существует матрица H_i такая, что $H_i^{-1}H_k \in \mathscr{A}(RM(r,m))$ и $H_i^{-1}H_l \in \mathscr{A}(RM(r,m))$. Это означает, что найдутся две матрицы $D_1, D_2 \in \mathscr{A}(RM(r,m))$, для которых

$$H_k = H_i D_1,\ H_l = H_i D_2.$$

Вычислим $H_k^{-1}H_l$:

$$H_k^{-1}H_l = D_1^{-1}H_i^{-1}H_i D_2 = D_1^{-1}D_2.$$

Так как $\mathscr{A}(RM(r,m))$ группа, то $D_1^{-1}D_2 \in \mathscr{A}(RM(r,m))$, а значит и $H_k^{-1}H_l \in \mathscr{A}(RM(r,m))$. □

Утверждение 4.5. *Пусть матрицы $H_1, \ldots, H_u$ таковы, что существует номер i, с которым выполняется условие*

$$\forall j = 1, 2, \ldots, u \quad H_i^{-1}H_j \in \mathscr{A}(RM(r,m)).$$

Тогда

1) *в множестве $\mathscr{L}(H_1, \ldots, H_u)$ существует единственный A-класс $A[(H_1, \ldots, H_u)]$;*

2) *мощность этого A-класса равна $|Aut(RM(r,m))|^u$.*

Доказательство. Для начала заметим, что в множестве $\mathscr{L}(H_1, \ldots, H_u)$ существует A-класс с представителем $(H_1, \ldots, H_u)$. Возьмём теперь любой кортеж матриц $(A_1, \ldots, A_u)$ из множества $\mathscr{L}(H_1, \ldots, H_u)$. Для него найдётся перестановка Γ такая, что

$$(H_1R\|H_2R\|\ldots\|H_uR)\Gamma = (A_1R\|A_2R\|\ldots\|A_uR).$$

Умножим левую и правую часть равенства на невырожденную матрицу H_i^{-1}. Тогда получим

$$(H_i^{-1}H_1R\|\ldots\|H_i^{-1}H_{i-1}R\|ER\|H_i^{-1}H_{i+1}R\|\ldots\|H_i^{-1}H_uR)\Gamma = \\ = (H_i^{-1}A_1R\|\ldots\|H_i^{-1}A_uR).$$

В силу того, что $H_i^{-1}H_j \in \mathscr{A}(RM(r,m))$, то существуют перестановки из $\Gamma_1, \ldots, \Gamma_u \in S_n$, для которых

$$(R\|\ldots\|R)(\Gamma_1\|\ldots\|\Gamma_{i-1}\|E\|\Gamma_{i+1}\|\ldots\|\Gamma_u)\Gamma = (H_i^{-1}A_1R\|\ldots\|H_i^{-1}A_uR).$$

Г. А. Карпунин доказал [9], что перестановку, стоящую в левой части последнего равенства можно представить в виде $g_\varphi\widetilde{\Gamma}$, где $\widetilde{\Gamma}$ — блоковая перестановка, составленная из автоморфизмов кода $RM(r,m)$, g_φ — некоторая перестановка из множества $\Gamma_\varphi(E,E,\ldots,E)$. Учитывая всё сказанное, получаем

$$(D_1R\|\ldots\|D_uR) = (H_i^{-1}A_1R\|\ldots\|H_i^{-1}A_uR)$$

для некоторых матриц $D_1,\ldots,D_u \in \mathscr{A}(RM(r,m))$. Откуда следует, что

$$A_j = H_iD_j, \forall\ j = 1,2,\ldots,u.$$

Осталось заметить, что любая матрица H_j может быть представлена в виде $H_j = H_iB_j$, где $B_j \in \mathscr{A}(RM(r,m))$. Тем самым любой кортеж $(A_1,\ldots,A_u) \in \mathscr{L}(H_1,\ldots,H_u)$ принадлежит A-классу $A[(H_1,\ldots,H_u)]$.

Вычислим теперь мощность A-класса с представителем $(H_1,\ldots,H_u)$. Для этого возьмём два набора матриц $D'_1,\ldots,D'_u$ и $D''_1,\ldots,D''_u$ из множества $\mathscr{A}(RM(r,m))$. Пусть существует номер i такой, что $D'_i \neq D''_i$, тогда $H_iD'_i \neq H_iD''_i$. Итак, если два набора матриц из множества $\mathscr{A}(RM(r,m))$ различны, то и различны наборы $(H_1D'_1,\ldots,H_uD'_u)$, $(H_1D''_1,\ldots,H_uD''_u)$. Возьмём теперь любую перестановку Γ из множества S_u. Рассмотрим два набора $(H_1,\ldots,H_u)$ и $(H_{\Gamma(1)},\ldots,H_{\Gamma(u)})$. В силу леммы 4.1 $H_k^{-1}H_{l=\Gamma(k)} \in \mathscr{A}(RM(r,m))$. Тогда рассмотрим такой кортеж $(H_1D_1,\ldots,H_uD_u)$, что $D_k = H_k^{-1}H_{l=\Gamma(k)} \in \mathscr{A}(RM(r,m))$. Этот кортеж совпадает с $(H_{\Gamma(1)},\ldots,H_{\Gamma(u)})$. Тем самым для любой перестановки Γ найдётся набор матриц $D_1,\ldots,D_u \in \mathscr{A}(RM(r,m))$ такой, что

$$H_{\Gamma(j)} = H_jD_j.$$

Итак, все элементы A-класса $A[(H_1,\ldots,H_u)]$ получаются только умножением каждой H_i на некоторую матрицу из $\mathscr{A}(RM(r,m))$. Откуда следует, что мощность класса эквивалентности $[(H_1,\ldots,H_u)]$ равна $|Aut(RM(r,m))|^u$. □

Из утверждения 4.2 и 4.5 следует теорема.

Теорема 4.2. *Пусть матрицы $H_1,\ldots,H_u$ таковы, что существует номер i, с которым выполняется условие*

$$\forall j = 1,2\ldots,u \quad H_i^{-1}H_j \in \mathscr{A}(RM(r,m)).$$

Тогда

$$|\mathscr{G}(H_1,\ldots,H_u)| = (u!)^n|Aut(RM(r,m))|^u.$$

Доказательство. Из утверждений 4.2 и 4.5 следует, что

$$|\mathcal{G}(H_1, \ldots, H_u)| = |\Gamma_\varphi(H_1, \ldots, H_u)||Aut(RM(r,m))|^u. \quad (2)$$

По условию найдётся такая матрица H_i, что $H_i^{-1}H_j$ для любого номера $j = 1, 2, \ldots, u$ принадлежит множеству $\mathcal{A}(RM(r,m))$. В силу этого все матрицы H_jR, $j = 1, 2, \ldots, u$, состоят из одних и тех же столбцов.

Напомним, см. утверждение 4.3, что в множестве $\Gamma_\varphi(H_1, \ldots, H_u)$ лежат только перестановки меняющие местами блоки одинаковых столбцов. Значит, в нашем случае мощность этого множества будет равна $(u!)^n$. Учитывая соотношение (2), получаем требуемую формулу. □

Из последнего утверждения можно получить важное следствие — оценку снизу на мощность множества открытых ключей криптосистемы Мак-Элиса–Сидельникова.

Утверждение 4.6. *Справедлива оценка снизу на мощность множества открытых ключей*

$$\frac{h_k(u \cdot n)!}{(u!)^n} \leqslant |\mathcal{C}|.$$

Доказательство. Рассмотрим следующее множество $\mathcal{H}$ секретных ключей:

$$\mathcal{H} = \{(HD_1, HD_2, \ldots, HD_u, \Gamma)| \\ H \in GL_k(F_2)\ D_1, D_2, \ldots, D_u \in \mathcal{A}(RM(r,m)), \Gamma \in S_{un}\}.$$

Множество $\mathcal{H}$ замкнуто относительно эквивалентности секретных ключей. Действительно, пусть ключи $(HD_1, \ldots, HD_u, \Gamma)$ и $(H'_1, \ldots, H'_u, \Gamma')$ эквивалентны, то есть

$$(HD_1R\| \ldots \|HD_uR)\Gamma = (H'_1R\| \ldots \|H'_uR)\Gamma'.$$

Рассмотрим перестановки $\Gamma_1, \Gamma_2, \ldots, \Gamma_u \in Aut(RM(r,m))$, для которых

$$D_1R = R\Gamma_1 \quad D_2R = R\Gamma_2\ , \ldots,\ D_uR = R\Gamma_u.$$

Тогда

$$(R\| \ldots \|R)(\Gamma_1\| \ldots \|\Gamma_u)\Gamma\Gamma'^{-1} = (H^{-1}H'_1R\| \ldots \|H^{-1}H'_uR).$$

Как и в утверждении 4.5, отсюда немедленно следует, что найдутся матрицы $D'_1, \ldots, D'_u \in \mathcal{A}(RM(r,m))$ такие, что

$$H'_1 = HD'_1,\ \ldots,\ H'_u = HD'_u.$$

Что означает принадлежность ключа $(H'_1, \ldots, H'_u, \Gamma')$ множеству $\mathscr{H}$.

Таким образом, множество $\mathscr{H}$ разбивается на классы эквивалентности. Из следствия 4.1 и теоремы 4.2 вытекает, что эти классы будут иметь одинаковую мощность, равную $(u!)^n |Aut(RM(r,m))|^u$. Но тогда число классов эквивалентности в этом множестве будет в точности равно отношению мощности $\mathscr{H}$, которая очевидно равна $h_k |Aut(RM(r,m))|^u (u \cdot n)!$, к мощности класса эквивалентности, то есть

$$\frac{h_k |Aut(RM(r,m))|^u (u \cdot n)!}{(u!)^n |Aut(RM(r,m))|^u} = \frac{h_k (u \cdot n)!}{(u!)^n}.$$

Осталось заметить, что $\mathscr{H}$ — подмножество секретных ключей, поэтому число классов эквивалентности, а значит и число открытых ключей, будет не меньше чем число классов в множестве $\mathscr{H}$, то есть

$$\frac{h_k (u \cdot n)!}{(u!)^n} \leqslant |\mathscr{C}|.$$

Что и требовалось доказать. □

Учитывая результат, полученный Г . А . Карпуниным [9], можно сформулировать теорему

Теорема 4.3. *Справедливы неравенства для числа открытых ключей криптосистемы Мак-Элиса–Сидельникова*

$$\frac{h_k (u \cdot n)!}{(u!)^n} \leqslant |\mathscr{C}| < \frac{(u \cdot n)! (h_k)^u}{u! |Aut(RM(r,m))|^u}.$$

Следует отметить, что результаты данного параграфа можно без изменений переформулировать для любого линейного кода на любым конечным полем F_q.

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

Для случая $u = 2$ задача поиска эквивалентных ключей криптосистемы Мак-Элиса–Сидельникова основывается на изучении множеств $\mathcal{G}(H_1, H_2)$, которые определяются так:

$$\begin{aligned}\mathcal{G}(H_1, H_2) \ = \{\Gamma \in S_{2n} | \exists A_1, A_2 &- \text{невырожденные } k \times k\text{-матрицы такие, что} \\ &(H_1 R \| H_2 R)\Gamma = (A_1 R \| A_2 R)\}\end{aligned}$$

Как указывалось в предыдущем параграфе вопрос описания множеств $\mathcal{G}(H_1, \ldots, H_u)$ тесно связан с множествами $\mathcal{L}(H_1, \ldots, H_u)$. Сформулируем их определение для случая $u = 2$.

$$\begin{aligned}\mathcal{L}(H_1, H_2) \ = \ &\{(A_1, A_2) - \text{кортеж невырожденных матриц,} \\ &\text{для которых существует перестановка } \Gamma \in S_{2n} : \\ &(H_1 R \| H_2 R)\Gamma = (A_1 R \| A_2 R).\}\end{aligned}$$

Если матрица $H_1^{-1} H_2$ (или $H_2^{-1} H_1$) принадлежит множеству $\mathcal{A}(RM(r, m))$, то описание данного множества даёт утверждение 4.5. Интересен случай, когда эта матрица не принадлежит множеству $\mathcal{A}(RM(r, m))$.

Перепишем соотношение, задающее множества $\mathcal{G}(H_1, H_2)$ и $\mathcal{L}(H_1, H_2)$, в следующем виде

$$(R \| H_1^{-1} H_2 R)\Gamma = (H_1^{-1} A_1 R \| H_1^{-1} A_2 R).$$

Введём новые матрицы: $T = H_1^{-1} H_2$, $X = H_1^{-1} A_1$, $Y = H_1^{-1} A_2$. В новых обозначения последнее соотношение перепишется так

$$(R \| TR)\Gamma = (XR \| YR) \qquad (\star).$$

Если в этом соотношении фиксировать матрицу T, то можно получить матричное уравнение относительно X, Y, Γ. Следующее утверждение устанавливает связь решений уравнения $(\star)$ с множествами $\mathcal{G}(H_1, H_2)$ и $\mathcal{L}(H_1, H_2)$.

Утверждение 5.1. *Пусть тройка* (X, Y, Γ), $X, Y \in GL_k(F_2)$, Γ — *перестановка на множестве из* $2n$ *элементов, является решением уравнения*

$$(R\|TR)\Gamma = (XR\|YR).$$

Тогда для любой невырожденной матрицы H *размера* $k \times k$ *пара* $(HX, HY) \in \mathscr{L}(H, HT)$ *и* $\Gamma \in \mathscr{G}(H, HT)$.

Справедливо и обратное. Если пара (A_1, A_2) *принадлежит множеству* $\mathscr{L}(H_1, H_2)$, *а* $\Gamma \in \mathscr{G}(H_1, H_2)$, *причём*

$$(H_1R\|H_2R)\Gamma = (A_1R\|A_2R),$$

то тройка $(H_1^{-1}A_1, H_1^{-1}A_2, \Gamma)$ *является решением уравнения*

$$(R\|TR)\Gamma = (XR\|YR), \text{ при } T = H_1^{-1}H_2.$$

Доказательство. Справедливость данного утверждения следует из определения соответствующих множеств. □

Утверждение 5.1 позволяет сводить задачу описания множеств $\mathscr{L}(H_1, H_2)$ к решению уравнения

$$(R\|TR)\Gamma = (XR\|YR).$$

Рассмотрим матрицы $T_{\widetilde{\alpha}}$ следующего типа:

$$T_{\widetilde{\alpha}} = \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_{k-1} \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

здесь $\widetilde{\alpha} = (\alpha_1, \dots, \alpha_{k-1})$. Очевидно, что для любого набора $\widetilde{\alpha}$ матрица $T_{\widetilde{\alpha}}$ невырождена, поэтому можно рассмотреть уравнение $(\star)$ с матрицей T равной $T_{\widetilde{\alpha}}$. Отметим также, что матрица $T_{\widetilde{\alpha}}$ при $\widetilde{\alpha} \neq 0$ не принадлежит множеству $\mathscr{A}(RM(r, m))$, поскольку при $\widetilde{\alpha} \neq 0$ в матрицах R и $T_{\widetilde{\alpha}}R$ веса их первых строчек будут отличаться.

Занумеруем всё множество столбцов порождающей матрицы R кода Рида–Маллера $RM(r, m)$ числами от 1 до n. Обозначим символом $\mathcal{N}$ множество $\{1, 2, \dots, n\}$.

Определение 5.1. *Носителем* n-мерного вектора x над полем F_2 называется множество всех тех номеров координат, в которых у вектора x стоит 1, то есть

$$\mathrm{supp}(x) = \{i \in \mathcal{N} | x_i = 1\}.$$

Множество дополнительное к носителю вектора x будем обозначать символом $\overline{\mathrm{supp}}(x)$, то есть

$$\overline{\mathrm{supp}}(x) = \mathcal{N} \setminus \mathrm{supp}(x).$$

Заметим, что множество $\overline{\mathrm{supp}}(x)$ состоит из тех номеров $i = 1, \ldots, n$, для которых $x_i = 0$.

Определение 5.2. Пусть $I \subset \mathcal{N}$, тогда *укороченным кодом* Рида–Маллера $RM_I(r, m)$ будем называть множество кодовых слов $RM(r, m)$, у которых на местах с номерами из множества I стоят нули, то есть

$$RM_I(r, m) = \{x \in RM(r, m) | \forall i \in I \; x_i = 0\}.$$

Легко проверить, что данное множество действительно является кодом, то есть линейным подпространством пространства F_2^n.

Определение 5.3. Обозначим через R^i для некоторого i матрицу, получающуюся из матрицы R выкидыванием i-той строки. Кодом Рида–Маллера $RM^i(r, m)$ *с выбрасыванием* назовём код, порождающей матрицей которого является R^i.

Везде далее $RM^i_I(r, m) = (RM^i)_I(r, m)$, то есть $RM^i_I(r, m)$ — код, получающийся из кода Рида–Маллера $RM(r, m)$ сначала выбрасыванием i-той строки из порождающей матрицы, а потом укорачиванием нового кода в множестве координат I.

Утверждение 5.2. *Перестановка* Γ *принадлежит множеству* $\mathcal{G}(E, T_{\widetilde{\alpha}})$*, если и только если её можно представить в виде* $\widetilde{\Gamma}(\Gamma_1 \| \Gamma_2)$*, где* $\Gamma_1, \Gamma_2 \in Aut(RM(r, m))$*, а перестановка* $\widetilde{\Gamma}$

1) *выделяет блоки одинаковых столбцов и переводит их друг в друга;*

2) *выбирает некоторый вектор* x *из кода* $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r, m)$ *и переводит столбцы* R_i *в* $T_{\widetilde{\alpha}} R_i$ *для любого* $i \in \mathrm{supp}(x)$.

Доказательство. Рассмотрим уравнение $(\star)$:

$$(R \| T_{\widetilde{\alpha}} R)\Gamma = (XR \| YR).$$

В силу того, что R является стандартной формой порождающей матрицы кода $RM(r, m)$, то первая её строка состоит из всех единиц, поэтому любой столбец можно представить в виде $\binom{1}{R'_i}$, $i = 1, 2, \ldots, n$.

Для начала заметим, что матрица $T_{\widetilde{\alpha}} R$ состоит из столбцов двух видов. Первый тип — такие же столбцы как и в матрице R, то есть они имеют вид $\binom{1}{R'_i}$. Таких столбцов будет столько, сколько единиц в первой строке матрицы $T_{\widetilde{\alpha}} R$, то есть $|\operatorname{supp}((1, \widetilde{\alpha})R)|$. Второй тип — столбцы, которые отличаются от какого-нибудь столбца в матрице R только в первой координате. Их число, очевидно, равно числу нулей в первой строке, то есть $|\overline{\operatorname{supp}}((1, \widetilde{\alpha})R)|$. Такие столбцы имеют вид $\binom{0}{R'_i}$.

Возьмём какое нибудь решение (X, Y, Γ) уравнения $(\star)$. После действия перестановки Γ никакие столбцы из $T_{\widetilde{\alpha}} R$ первого типа не могут оказаться в одной матрице (XR или YR) с точно такими же столбцами из матрицы R, в силу того, что ни в одной порождающей матрице кода Рида–Маллера нет двух одинаковых столбцов.

Докажем теперь, что в матрицах XR и YR не могут лежать сразу столбцы следующих видов: $\binom{0}{R'_i}$, $\binom{1}{R'_i}$. Действительно, пусть это имеет место. В матрицах R и $T_{\widetilde{\alpha}} R$ первый столбец одинаковый и равен $\binom{1}{0}$, поэтому и в матрице XR и в матрице YR обязательно должен быть столбец $\binom{1}{0}$. Но тогда, сложив $\binom{0}{R'_i}$, $\binom{1}{R'_i}$ и $\binom{1}{0}$, получим:

$$\binom{0}{R'_i} \oplus \binom{1}{R'_i} \oplus \binom{1}{0} = 0.$$

Но последнее означает, что данная система столбцов линейно зависимая. Откуда немедленно следует, что кодовое расстояние дуального к коду с порождающей матрицей XR или YR меньше, либо равно 3. Но XR и YR — суть коды Рида–Маллера $RM(r, m)$, $r \geqslant 2$. Известно [6], что кодовое расстояние кода $RM^{\perp}(r, m)$ в точности равно 2^{r+1}. Учитывая это получаем, что $2^{r+1} \leqslant 3$. Что невозможно при $r \geqslant 2$. Получили противоречие.

Из всего выше сказанного следует, что перестановка Γ лишь может

1) менять порядок следования столбцов внутри матриц R и $T_{\widetilde{\alpha}} R$;

2) выделять группы столбцов в одной матрице и перекидывать их в те же самые столбцы в другой матрице;

3) выделять группы столбцов второго типа $\binom{0}{R'_{i_1}}$, $\binom{0}{R'_{i_2}}$,…,$\binom{0}{R'_{i_s}}$ в матрице $T_{\widetilde{\alpha}}R$ и менять её с группой столбцов $\binom{1}{R'_{i_1}}$,$\binom{1}{R'_{i_2}}$,…,$\binom{1}{R'_{i_s}}$ матрицы R.

Итак, предполагая что (X, Y, Γ) — решение уравнения $(\star)$, мы получили необходимые условия на перестановку Γ. В этих же предположениях уточним условие 3). Возьмём перестановку Γ, которая обязательно реализует 3). Пусть после применения Γ из матрицы $(R\|T_{\widetilde{\alpha}}R)$ образовалась матрица $(XR\|YR)$. XR — задаёт код Рида–Маллера $RM(r, m)$, значит существует вектор β такой, что $\beta XR = 1 = (1, 1, \ldots, 1)$. Докажем, что первая координата вектора β обязательно равна 1. Действительно, в силу вида перестановки Γ, матрицу XR можно представить в виде

$$XR = \begin{pmatrix} 1 & 1 & \ldots & 0 & \ldots & 0 & \ldots & 1 \\ R'_{j_1} & R'_{j_2} & \ldots & R'_{i_1} & \ldots & R'_{i_s} & \ldots & R'_{j_n} \end{pmatrix}.$$

Здесь столбцы $R_{i_1}, \ldots, R_{i_s}$ стоят на местах с номерами $j_{i_1}, \ldots, j_{i_s}$ соответственно. Причём матрица $(R'_{j_1}R'_{j_2}\ldots R'_{i_1}\ldots R'_{i_s}\ldots R'_{j_n})$ получается из матрицы $(R'_1R'_2\ldots R'_{i_1}\ldots R'_{i_s}\ldots R'_n)$ применением некоторой перестановки $\Gamma_1 \in S_n$. Но никакая сумма строк матрицы $(R'_1\ldots R'_n)$ не может равняться единичной строчке 1. Следовательно, сумма строк матрицы XR, дающая единичную строчку, должна обязательно содержать строку с первым номером, то есть $\beta_1 = 1$. Учитывая, что $\beta_1 = 1$, получаем

$$1 = \beta XR = \\ = (1\ 1\ \ldots\ 0\ \ldots\ 0\ \ldots\ 1) \oplus (\beta_2, \ldots, \beta_k)(R'_{j_1}\ R'_{j_2}\ \ldots\ R'_{i_1}\ \ldots\ R'_{i_s}\ \ldots\ R'_{j_n}).$$

Откуда

$$(\beta_2, \ldots, \beta_k)(R'_{j_1}\ R'_{j_2}\ \ldots\ R'_{i_1}\ \ldots\ R'_{i_s}\ \ldots\ R'_{j_n}) = (0\ 0\ \ldots\ 1\ \ldots\ 1\ \ldots\ 0).$$

Здесь в векторе $(0\ 0\ \ldots\ 1\ \ldots\ 1\ \ldots\ 0)$ единицы стоят на позициях с номерами $j_{i_1}, j_{i_2}, \ldots, j_{i_s}$. Умножим левую и правую часть этого равенства на перестановку Γ_1^{-1}, тогда

$$(\beta_2, \ldots, \beta_k)(R'_1\ \ldots\ R'_n) = (0\ 0\ \ldots\ 1\ \ldots\ 1\ \ldots\ 0). \qquad (\divideontimes)$$

Здесь уже в векторе $(0\ 0\ \ldots\ 1\ \ldots\ 1\ \ldots\ 0)$ единицы стоят на позициях с номерами $i_1, \ldots, i_s$. Обозначим через x вектор, стоящий в правой части последнего равенства, то есть

$$x = (0\ 0\ \ldots\ 1\ \ldots\ 1\ \ldots\ 0),\ x_j = 1 \Leftrightarrow j = i_p (p = 1, \ldots, s).$$

Введя такое обозначение, соотношение (⋇) можно записать так:

$$(0, \beta_2, \ldots, \beta_k)R = x.$$

Откуда немедленно следует, что вектор x, принадлежит коду $RM^1(r, m)$. Заметим, что $i_1, \ldots, i_s \in \overline{\mathrm{supp}}((1, \widetilde{\alpha})R)$, то есть $i_1, \ldots, i_s \notin \mathrm{supp}((1, \widetilde{\alpha})R)$. Этот факт означает, что вектор $x \in RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r, m)$.

Введём матрицу K:

$$K = \begin{pmatrix} 1 & \beta_2 & \ldots & \beta_k \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

В результате матрицы XR и YR можно представить в виде

$$XR = K \cdot R\Gamma_1;\ YR = K \cdot T_{\widetilde{\alpha}} R\Gamma_2. \tag{3}$$

Последнее верно, так как строчки с номерами $2, \ldots, k$ матрицы $T_{\widetilde{\alpha}}R$ не отличаются от соответствующих строчек матрицы R. В силу этого, строчки $2, \ldots, k$ матрицы $K \cdot T_{\widetilde{\alpha}}R$ также будут совпадать с соответствующими строками матрицы R. Первая же строка в $K \cdot T_{\widetilde{\alpha}}R$ будет получаться прибавлением вектора x к первой строке матрицы $T_{\widetilde{\alpha}}R$. В векторе x единицы стоят только на тех местах, на которых в первой строке матрицы $T_{\widetilde{\alpha}}R$ стоят нули, поэтому замена столбцов вида $\binom{0}{R_{i_p}}$ на столбцы $\binom{1}{R_{i_p}}(p = 1, \ldots, s)$ в матрице $T_{\widetilde{\alpha}}R$ эквивалентна прибавлению вектора $x(x_j = 1 \Leftrightarrow j = i_p(p = 1, \ldots, s))$ к первой строке матрицы $T_{\widetilde{\alpha}}R$. Поэтому матрица $K \cdot T_{\widetilde{\alpha}}R$ будет состоять из тех же столбцов, что и матрица YR. И для некоторой перестановки Γ_2 будет выполняться

$$YR = K \cdot T_{\widetilde{\alpha}} R\Gamma_2.$$

Из соотношения (3) следует, что каждая из перестановок Γ_1, Γ_2 является автоморфизмов кода $RM(r, m)$, а матрицы X и Y имеют вид

$$X = KD_1,\ Y = KD_2,\ D_1, D_2 \in \mathcal{A}(RM(r, m)).$$

Итак, из всей цепочки рассуждений видно, что матрицу Γ можно разложить в произведение некоторой матрицы $\widetilde{\Gamma}$ на блоковую перестановку $(\Gamma_1\|\Gamma_2)$, состоящую из автоморфизмов кода $RM(r,m)$. Тем самым можно не только уточнить условия 1),2),3), но и сформулировать их уже для перестановки $\widetilde{\Gamma}$. В итоге, $\widetilde{\Gamma}$ может только

1') выделять группы столбцов в одной матрице и перекидывать их в те же самые столбцы в другой матрице;

2') выделять группы столбцов второго типа $\binom{0}{R'_{i_1}}$, $\binom{0}{R'_{i_2}},\dots,\binom{0}{R'_{i_s}}$ в матрице TR и менять её с группой столбцов $\binom{1}{R'_{i_1}},\binom{1}{R'_{i_2}},\dots,\binom{1}{R'_{i_s}}$ матрицы R, при условии, что существует вектор x из кода $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$ такой, что для любого $j=1,\dots,s$ $x_{i_j}=1$.

3') выполнять 1') и 2') одновременно.

Докажем обратное. Пусть перестановку Γ можно представить в виде произведения перестановок $\widetilde{\Gamma}(\Gamma_1\|\Gamma_2)$, где Γ_1,Γ_2 — автоморфизмы кода Рида–Маллера $RM(r,m)$, а $\widetilde{\Gamma}$ удовлетворяет условиям 1'),2'),3'). Если $\widetilde{\Gamma}$ удовлетворяет только условию 1'), то, очевидно, что (D_1,D_2,Γ) (здесь $D_1R=R\Gamma_1$ и $D_2R=R\Gamma_2$) — решение уравнения $(\star)$, то есть $\Gamma\in\mathcal{G}(E,T_{\widetilde{\alpha}})$. Пусть она реализует ещё и 2'). Тогда существует кодовое слово $x\in RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$ такое, что перестановка $\widetilde{\Gamma}$ переводит друг в друга столбцы R_i и $T_{\widetilde{\alpha}}R_i$ для любого номера $i\in\mathrm{supp}(x)$. Так как $x\in RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$, то, по определению кода $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$, существует $(k-1)$-мерный вектор $\beta=(\beta_2,\dots,\beta_k)$ такой, что $(0,\beta)R=x$ и $(0,\beta)T_{\widetilde{\alpha}}R=x$. Построим матрицу X следующим образом

$$X=\begin{pmatrix}1&\beta_2&\dots&\beta_k\\0&1&\dots&0\\\vdots&\vdots&\dots&\vdots\\0&0&\dots&1\end{pmatrix},\qquad(*)$$

и пусть $Y=XT_{\widetilde{\alpha}}$. Тогда, очевидно, $(X,Y,\widetilde{\Gamma})$ — решение уравнения $(\star)$, а значит и тройка (XD_1,YD_2,Γ) (здесь $D_1R=R\Gamma_1$ и $D_2R=R\Gamma_2$) тоже решение уравнения $(\star)$, поэтому $\Gamma\in\mathcal{G}(E,T_{\widetilde{\alpha}})$.

Тем самым утверждение полностью доказано. □

Из утверждения 5.2 как следствие можно получить утверждение 5.3.

Утверждение 5.3. *Пусть код Рида–Маллера $RM(r,m)$ имеет параметры: $r \geqslant 2$, $r < m$. Обозначим через R стандартную форму его порождающей матрицы. Тогда число A-классов в множестве $\mathscr{L}(E, T_{\widetilde{\alpha}})(\widetilde{\alpha} \neq \widetilde{0})$ равно*

$$2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]-1}.$$

Доказательство. В силу утверждения 5.2 любую перестановку $\Gamma \in \mathscr{G}(E, T_{\widetilde{\alpha}})$ можно представить в виде $\widetilde{\Gamma}(\Gamma_1 \| \Gamma_2)$, где Γ_1, Γ_2 — автоморфизмы кода Рида–Маллера $RM(r,m)$, а $\widetilde{\Gamma}$ задаётся некоторым словом из $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$. Тем самым число перестановок в множестве $\mathscr{G}(E, T_{\widetilde{\alpha}})$ равно произведению числа кодовых слов в $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$ на $|Aut(RM(r,m))|^2$ и на

$$|\Gamma_\varphi(E, T_{\widetilde{\alpha}})| = 2^{|\,\mathrm{supp}((1,\widetilde{\alpha})R)|}.$$

Из утверждения 4.2 следует, что мощность множества $\mathscr{L}(E, T_{\widetilde{\alpha}})$ в $\mathscr{L}(E, T_{\widetilde{\alpha}}) \geqslant 2^{|\,\mathrm{supp}((1,\widetilde{\alpha})R)|}$ раз меньше, чем $|\mathscr{G}(E, T_{\widetilde{\alpha}})|$. Значит

$$|\mathscr{L}(E, T_{\widetilde{\alpha}})| = 2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]}|Aut(RM(r,m))|^2.$$

Осталось заметить, что, так как $T_{\widetilde{\alpha}}$ не принадлежит множеству $\mathscr{A}(RM(r,m))$, мощность каждого A-класса равна $2|Aut(RM(r,m))|^2$. Итак, число A-классов в $\mathscr{L}(E, T_{\widetilde{\alpha}})$ равно

$$\frac{2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]}|Aut(RM(r,m))|^2}{2|Aut(RM(r,m))|^2} = 2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]-1}.$$

Что и требовалось доказать. □

Пример. Возьмём код Рида–Маллера с параметрами $r = 2$, $m = 3$. В качестве матрицы T выберем следующую:

$$T = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Тогда уравнение $(\star)$ примет вид:

$$\left\|\begin{array}{cccccccc|cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right\| \Gamma = \|XR|YR\|.$$

Вектор $\widetilde{\alpha}$ будет равен $(1, 1, 0, 1, 0, 0)$. Множество

$$\mathrm{supp}((1, 1, 1, 0, 1, 0, 0)R = (1, 1, 0, 0, 0, 0, 0, 0))$$

состоит из двух координат 1 и 2. Код $RM^1_{1,2}$ будет иметь порождающую матрицу $R_{1,2}$:

$$R_{1,2} = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}$$

Построим, например, перестановки $\widetilde{\Gamma}_1$ и $\widetilde{\Gamma}_2$,$\widetilde{\Gamma}_3$ которые будут соответствовать первому, второму и последнему вектору матрицы $R_{1,2}$.

$$\widetilde{\Gamma}_1 = (1)(2)(3)(4)(9)(10)(11)(12)(5\ 13)(6\ 14)(7\ 15)(8\ 16).$$

$$\widetilde{\Gamma}_2 = (1)(2)(3)(4)(5)(6)(9)(10)(11)(12)(13)(14)(7\ 15)(8\ 16).$$

$$\widetilde{\Gamma}_3 = (1)(2)(3)(5)(6)(8)(9)(10)(11)(13)(14)(4\ 12)(8\ 16).$$

Соответствующие матрицы (X_1, Y_1), (X_2, Y_2), (X_3, Y_3) будут выглядеть так

$$X_1 = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} Y_1 = X_1T = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

$$X_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} Y_2 = X_2T = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$X_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} Y_3 = X_3T = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

При этом

$$X_1R = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} Y_1R = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$X_2R = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} Y_2R = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$X_3R = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad Y_3R = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Нетрудно видеть, что все эти матрицы задают различные A-классы.

Следствием предыдущих утверждений являются утверждения 5.4 и 5.5.

Утверждение 5.4. *Для любой невырожденной матрицы H перестановка Γ принадлежит множеству $\mathcal{G}(H, HT_{\widetilde{\alpha}})$, если и только если её можно представить в виде $\widetilde{\Gamma}(\Gamma_1 \| \Gamma_2)$, где $\Gamma_1, \Gamma_2 \in Aut(RM(r,m))$, а перестановка $\widetilde{\Gamma}$*

1) *выделяет блоки одинаковых столбцов и переводит их друг в друга;*

2) *выбирает некоторый вектор x из кода $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$ и переводит столбцы HR_i и $HT_{\widetilde{\alpha}}R_i$ друг в друга для любого $i \in \mathrm{supp}(x)$.*

Утверждение 5.5. *Пусть код Рида–Маллера $RM(r,m)$ имеет параметры: $r \geqslant 2$, $r < m$. Обозначим через R стандартную форму его порождающей матрицы. Тогда для любой невырожденной матрицы H число A-классов в множестве $\mathcal{L}(H, HT_{\widetilde{\alpha}})$ равно*

$$2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]-1}.$$

Рассмотрим теперь матрицу $T^i_{\widetilde{\alpha}}(i > 1)$ вида

$$T^i_{\widetilde{\alpha}} = \begin{pmatrix} & & & & i & & \\ & & & & \downarrow & & \\ & 1 & 0 & \dots & 0 & \dots & 0 \\ & 0 & 1 & \dots & 0 & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ i \to & \alpha_1 & \alpha_2 & \dots & 1 & \dots & \alpha_{k-1} \\ & \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & 0 & \dots & 1 \\ & & & & & & \end{pmatrix}.$$

Для неё справедливо следующее утверждение.

Утверждение 5.6. *Пусть* $I = \overline{\mathrm{supp}}(\overrightarrow{R}_i \oplus \overrightarrow{T^i_{\widetilde{\alpha}} R_i})$, *здесь* $\overrightarrow{R}_i$ *и* $\overrightarrow{T^i_{\widetilde{\alpha}} R_i}$ — i*-тые строки матриц* R *и* $T^i_{\widetilde{\alpha}} R$ *соответственно. Тогда для любого* $x \in RM^i_I$ *перестановка* $\Gamma = \Gamma'\Gamma''(\Gamma_1 \| \Gamma_2)$, *где*

1) Γ' *переводит одинаковые столбцы друг в друга;*

2) Γ'' *переводит друг в друга столбцы* $T^i_{\widetilde{\alpha}} R_j$ *и* R_j *для любого* $j \in \mathrm{supp}(x)$*;*

3) Γ_1, Γ_2 — *автоморфизмы кода Рида–Маллера* $RM(r, m)$*;*

принадлежит множеству $\mathcal{G}(E, T^i_{\widetilde{\alpha}})$.

Доказательство. Действительно, рассмотрим любое $x \in RM^i_I$. Из определения кода RM^i_I следует, что существует k-мерный вектор $\beta = (\beta_1, \ldots, \beta_k)$ такой, что $\beta_i = 0$ и $x = \beta R$. Рассмотрим матрицу K:

$$K = \begin{pmatrix} & & & i & & \\ & & & \downarrow & & \\ & 1 & 0 \ \ldots & 0 & \ldots & 0 \\ & 0 & 1 \ \ldots & 0 & \ldots & 0 \\ & \vdots & \vdots \ \ldots & \vdots & \ldots & \vdots \\ i \to & \beta_1 & \beta_2 \ \ldots & 1 & \ldots & \beta_k \\ & \vdots & \vdots \ \ldots & \vdots & \ldots & \vdots \\ & 0 & 0 \ \ldots & 0 & \ldots & 1 \end{pmatrix}.$$

Теперь пусть перестановка Γ'' переводит друг в друга столбцы $T^i_{\widetilde{\alpha}} R_j$ и R_j для любого $j \in \mathrm{supp}(x)$. Пусть после применения Γ'' матрица R перешла в матрицу R', а матрица $T^i_{\widetilde{\alpha}} R$ — в R''. Отметим, что столбцы $T^i_{\widetilde{\alpha}} R_j$ и R_j для любого $j \in \mathrm{supp}(x)$ отличаются только в i-той координате. Тем самым матрица R' будет состоят из тех же строк, за исключением i-той, что и R, а i-тая координата получается прибавлением вектора x к i-той строке матрицы R. Аналогичное будет выполняться и для матрицы R'', то есть всё её строки, кроме i-той, будут совпадать с соответствующими строками матрицы $T^i_{\widetilde{\alpha}} R$, а в силу структуры $T^i_{\widetilde{\alpha}}$ и со строками R. Строчка же с номером i получается в результате суммы вектора x и i-той строки матрицы $T^i_{\widetilde{\alpha}} R$. Поэтому действие перестановки Γ'' можно промоделировать матрицей K следующим образом:

$$(R \| T^i_{\widetilde{\alpha}})\Gamma'' = (R' \| R'') = K(R \| T^i_{\widetilde{\alpha}} R).$$

А это и означает, что $\Gamma'' \in \mathcal{G}(E, T^i_{\widetilde{\alpha}})$.

Осталось заметить, что перестановки Γ' и $(\Gamma_1 \| \Gamma_2)$ принадлежат множеству $\mathcal{G}(E, T^i_{\widetilde{\alpha}})$ очевидным образом, и к тому же

$$(R \| T^i_{\widetilde{\alpha}} R)\Gamma' = (R \| T^i_{\widetilde{\alpha}} R).$$

Утверждение полностью доказано. □

Утверждение 5.7. *Пусть код Рида–Маллера $RM(r, m)$ имеет параметры: $r \geqslant 2$, $r < m$. И пусть $T^i_{\widetilde{\alpha}} \notin \mathcal{A}(RM(r, m))$. Обозначим через R стандартную форму его порождающей матрицы. Пусть также $I = \overline{\operatorname{supp}}(\overrightarrow{R}_i \oplus \overrightarrow{T^i_{\widetilde{\alpha}} R_i})$, здесь $\overrightarrow{R}_i$ и $\overrightarrow{T^i_{\widetilde{\alpha}} R_i}$ — i-тые строки матриц R и $T^i_{\widetilde{\alpha}} R$ соответственно. Тогда число A-классов в множестве $\mathcal{L}(E, T^i_{\widetilde{\alpha}})$ не меньше, чем*

$$2^{\dim\left[RM^i_I(r,m)\right]-1}.$$

Доказательство. Из утверждения 5.6 следует, что

$$|\mathcal{G}(E, T^i_{\widetilde{\alpha}})| \geqslant |\Gamma_\varphi(E, T^i_{\widetilde{\alpha}})| 2^{\dim\left[RM^i_I(r,m)\right]} |Aut(RM(r, m))|^2.$$

Откуда

$$|\mathcal{L}(E, T^i_{\widetilde{\alpha}})| = \frac{|\mathcal{G}(E, T^i_{\widetilde{\alpha}})|}{|\Gamma_\varphi(E, T^i_{\widetilde{\alpha}})|} \geqslant 2^{\dim\left[RM^i_I(r,m)\right]} |Aut(RM(r, m))|^2.$$

Так как по условию $T^i_{\widetilde{\alpha}} \notin \mathcal{A}(RM(r, m))$, то мощность каждого A-класса равна $2|Aut(RM(r, m))|^2$. Учитывая это, получаем требуемое неравенство. □

Для матриц H и $HT^i_{\widetilde{\alpha}}$ можно сформулировать утверждения, аналогичные утверждениям 5.6 и 5.7. Их справедливость является прямым следствием утверждений 5.6 и 5.7.

Утверждение 5.8. *Пусть $I = \overline{\operatorname{supp}}(\overrightarrow{R}_i \oplus \overrightarrow{T^i_{\widetilde{\alpha}} R_i})$, здесь $\overrightarrow{R}_i$ и $\overrightarrow{T^i_{\widetilde{\alpha}} R_i}$ — i-тые строки матриц R и $T^i_{\widetilde{\alpha}} R$ соответственно. Тогда для любого $x \in RM^i_I$ и любой невырожденной матрицы H перестановка $\Gamma = \Gamma'\Gamma''(\Gamma_1 \| \Gamma_2)$, где*

1) *Γ' переводит одинаковые столбцы друг в друга;*

2) *Γ'' переводит друг в друга столбцы $HT^i_{\widetilde{\alpha}} R_j$ и HR_j для любого $j \in \operatorname{supp}(x)$;*

3) *Γ_1, Γ_2 — автоморфизмы кода Рида–Маллера $RM(r, m)$;*

принадлежит множеству $\mathcal{G}(H, HT^i_{\widetilde{\alpha}})$.

Утверждение 5.9. *Пусть код Рида–Маллера* $RM(r,m)$ *имеет параметры:* $r \geqslant 2, r < m$. *И пусть* $T^i_{\widetilde{\alpha}} \notin \mathcal{A}(RM(r,m))$. *Обозначим через* R *стандартную форму его порождающей матрицы. Пусть также* $I = \overline{\mathrm{supp}}(\overrightarrow{R}_i \oplus \overrightarrow{T^i_{\widetilde{\alpha}} R_i})$, *здесь* $\overrightarrow{R}_i$ *и* $\overrightarrow{T^i_{\widetilde{\alpha}} R_i}$ — i*-тые строки матриц* R *и* $T^i_{\widetilde{\alpha}} R$ *соответственно. Тогда для любой невырожденной матрицы* H *число* A*-классов в множестве* $\mathcal{L}(H, HT^i_{\widetilde{\alpha}})$ *не меньше, чем*

$$2^{\dim\left[RM^i_I(r,m)\right]-1}.$$

Из всех утверждений данного параграфа следует справедливость двух основных теорем.

Теорема 5.1. *Пусть* R *— стандартная форма порождающей матрицы кода* $RM(r,m)$ $(r \leqslant 2, r < m)$. *Тогда для любой невырожденной матрицы* H *справедливо:*

1) *каждое множество* $\mathcal{L}(H, HD)$ $(D \in \mathcal{A}(RM(r,m)))$ *содержит только один* A*-класс* $A[(H, HD)]$. *Причём мощность этого класса равна* $|Aut(RM(r,m)|^2$, *если* H *принадлежит множеству* $A(RM(r,m)))$, *и —* $2|Aut(RM(r,m))|^2$ *иначе;*

2) *каждое множество* $\mathcal{L}(H, HT_{\widetilde{\alpha}})$ *содержит в точности*

$$2^{\dim\left[RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)\right]-1}$$

A-классов мощности $2|Aut(RM(r,m))|^2$;

3) *каждое множество* $\mathcal{L}(H, HT^i_{\widetilde{\alpha}})(T^i_{\widetilde{\alpha}} \notin \mathcal{A}(RM(r,m)))$ *содержит не менее*

$$2^{\dim\left[RM^i_I(r,m)\right]-1}$$

A-классов мощности $2|Aut(RM(r,m))|^2$; *здесь под* I *понимается множество* $\overline{\mathrm{supp}}(\overrightarrow{R_i} \oplus \overrightarrow{T^i_{\widetilde{\alpha}} R_i})$, *а* $\overrightarrow{R_i}$ *и* $\overrightarrow{T^i_{\widetilde{\alpha}} R_i}$ *—* i*-тые строки матриц* R *и* $T^i_{\widetilde{\alpha}} R$ *соответственно.*

Теорема 5.2. *Пусть* R *— стандартная форма порождающей матрицы кода* $RM(r,m)$ $(r \leqslant 2, r < m)$. *Представим некоторую перестановку* Γ *в виде произведения перестановок* $\widetilde{\Gamma}(\Gamma_1 \| \Gamma_2)$, *где* $\widetilde{\Gamma} \in S_{2n}$, $\Gamma_1, \ldots, \Gamma_2 \in S_n$. *Тогда для любой невырожденной матрицы* H *справедливо:*

1) *каждое множество* $\mathcal{G}(H, HD)$ $(D \in \mathcal{A}(RM(r,m)))$ *содержит перестановку* Γ*, если и только если* $\Gamma_1, \Gamma_2 \in Aut(RM(r,m))$*, а перестановка* $\widetilde{\Gamma}$ *выделяет блоки одинаковых столбцов и переводит их друг в друга;*

2) *каждое множество* $\mathcal{G}(H, HT_{\widetilde{\alpha}})$ *содержит перестановку* Γ*, если и только если* $\Gamma_1, \Gamma_2 \in Aut(RM(r,m))$*, а перестановка* $\widetilde{\Gamma}$ *либо*

   i) *выделяет блоки одинаковых столбцов и переводит их друг в друга, либо*

   ii) *выбирает некоторый вектор* x *из кода* $RM^1_{\mathrm{supp}((1,\widetilde{\alpha})R)}(r,m)$ *и переводит столбцы* HR_i *и* $HT_{\widetilde{\alpha}}R_i$ *друг в друга для любого* $i \in \mathrm{supp}(x)$*, либо*

   iii) *i) и ii) вместе;*

3) *Если перестановка* Γ *такова, что* $\Gamma_1, \Gamma_2 \in Aut(RM(r,m))$*, а* $\widetilde{\Gamma}$

   i) *выделяет блоки одинаковых столбцов и переводит их друг в друга, либо*

   ii) *выбирает некоторый вектор* x *из кода* $RM^i_I(r,m)$ *и переводит столбцы* HR_j *и* $HT^i_{\widetilde{\alpha}}R_j$ *друг в друга для любого* $j \in \mathrm{supp}(x)$*, здесь под* I *понимается множество* $\overline{\mathrm{supp}}(\overrightarrow{R_i} \oplus \overrightarrow{T^i_{\widetilde{\alpha}}R_i})$*, а* $\overrightarrow{R_i}$ *и* $\overrightarrow{T^i_{\widetilde{\alpha}}R_i}$ *— i-тые строки матрицы* R *и* $T^i_{\widetilde{\alpha}}R$ *соответственно; либо*

   iii) *i) и ii) вместе,*

то множество $\mathcal{G}(H, HT^i_{\widetilde{\alpha}})$ *содержит перестановку* Γ*.*

Итак, теоремы 5.1 и 5.2 дают полное описание множеств $\mathcal{G}(H_1, H_2)$ для всех матриц H_1, H_2 таких, что $H_1^{-1}H_2$ — либо автоморфизм кода $RM(r,m)$, либо одна из матриц $T_{\widetilde{\alpha}}$. А для $\mathcal{G}(H, HT^i_{\widetilde{\alpha}})$ описывается некоторое его подмножество.

Список литературы

1. *Mceliece R.* A Public-Key Cryptosystem Based on Algebraic Coding Theory // JPL DSN Progress Report. — 1978. — Т. 44. — С. 123—125.
2. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискрет. матем. — 1994. — Т. 6, № 2. — С. 3—20.
3. *Сидельников В., Шестаков С.* О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона // Дискретная математика. — 1992. — Т. 4, № 3. — С. 57—63.
4. *Евсеев Г. С.* О сложности декодирования линейных кодов // Пробл. передачи информ. — 1983. — Т. 19, № 1. — С. 3—8.
5. *Крук Е. А.* Граница для сложности декодирования линейных блоковых кодов // Пробл. передачи информ., — 1989. — Т. 25, № 3. — С. 103—107.
6. *Мак-Вильямс Ф. Д., Слоэн Н. Д. А.* Теория кодов, исправляющих ошибки. — Связь, 1979.
7. *Huffman W. C., Brualdi R. A., Pless V. S.* Handbook of Coding Theory. — Elsevier Science Inc., 1998.
8. *Сидельников В. М., Першаков А. С.* Декодирование кодов Рида–Маллера при большом числе ошибок // Пробл. передачи информ., — 1992. — Т. 28, № 3. — С. 80—94.
9. *Карпунин Г. А.* О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида - Маллера // Дискретная математика. — 2004. — Т. 16, № 2. — С. 79—84. — DOI: 10.4213/dm153.