УДК 621.391.7 DOI 10.17223/20710410/57/2

О СТРУКТУРНОЙ СТОЙКОСТИ КРИПТОСИСТЕМЫ ТИПА МАК-ЭЛИСА НА СУММЕ ТЕНЗОРНЫХ ПРОИЗВЕДЕНИЙ БИНАРНЫХ КОДОВ РИДА — МАЛЛЕРА

Ю. В. Косолапов, Е. А. Лелюк

Южный федеральный университет, г. Ростов-на-Дону, Россия

E-mail: yvkosolapov@sfedu.ru, lelukevgeniy@mail.ru

Актуальной задачей криптографии является разработка криптосистем, стойких к атакам с использованием квантовых вычислений. Одной из перспективных схем шифрования считается система Мак-Элиса на кодах Гоппы. Однако эта система обладает рядом недостатков, обусловленных структурой кодов Гоппы, что делает актуальным поиск других кодов для схемы Мак-Элиса. Важными требованиями для этих кодов являются наличие быстрого декодера и обеспечение стойкости соответствующей криптосистемы к известным атакам, в том числе с использованием произведения Шура — Адамара. Многие попытки заменить коды Гоппы не привели к успеху, поскольку соответствующие криптосистемы оказались нестойкими к структурным атакам. В настоящей работе в качестве кода предлагается использовать D-конструкцию (D-код) на бинарных кодах Рида — Маллера. Эта конструкция является суммой специального вида тензорных произведений бинарных кодов Рида — Маллера. Для неё имеется быстрый алгоритм декодирования. С целью анализа стойкости схемы Мак-Элиса на D-кодах построена структурная атака с использованием произведения Шура — Адамара D-кода. Для выбора параметров, обеспечивающих стойкость криптосистемы к построенной атаке, исследуется разложимость степени D-кода в прямую сумму кодов Рида — Маллера и делается вывод о множестве стойких ключей криптосистемы.

Ключевые слова: *криптосистема типа Мак-Элиса, структурная стойкость, бинарные коды Рида — Маллера, сумма тензорных произведений, произведение Шура — Адамара.*

ON THE STRUCTURAL SECURITY OF A McELIECE-TYPE CRYPTOSYSTEM BASED ON THE SUM OF TENSOR PRODUCTS OF BINARY REED — MULLER CODES

Yu. V. Kosolapov, E. A. Lelyuk

Southern Federal University, Rostov-on-Don, Russia

The current task of cryptography is the development of cryptosystems resistant to attacks using quantum computing. One of the promising encryption schemes is the McEliece system based on Goppa codes. However, this system has a number of disadvantages due to the structure of Goppa codes, which makes it relevant to search for other codes for the McEliece scheme. Important requirements for these codes are the presence of a fast decoder and ensuring the resistance of the corresponding cryptosystem to known attacks, including attacks with the Schur — Hadamard product. Many attempts to replace Goppa codes have failed because the corresponding cryptosystems

have proven to be unstable against structural attacks. In this paper, it is proposed to use the D-construction (D-code) on binary Reed — Muller codes in the McEliece cryptosystem. This construction is a sum of a special kind of tensor products of binary Reed — Muller codes. There is a fast decoding algorithm for it. To analyze the security of the McEliece scheme on D-codes, we have constructed a structural attack that uses the Schur — Hadamard product of a D-code. To select the parameters that ensure the resistance of the cryptosystem to the constructed attack, we investigate the decomposition of the degree of the D-code into the direct sum of Reed — Muller codes and conclude about the set of strong keys of the cryptosystem.

Keywords: *McEliece-type cryptosystem, structural security, binary Reed — Muller codes, sum of tensor products, Schur —Hadamard product.*

Введение

В 2016 г. Национальным институтом стандартов и технологий США был объявлен конкурс на разработку криптосистем, стойких в постквантовую эпоху [1]. Одним из основных претендентов является кодовая криптосистема Мак-Элиса на кодах Гоппы, стойкость которой основана на сложности декодирования кода в предположении неотличимости его от случайного [2]. Однако её недостатками являются большой размер ключа (от 260 кбайт до 1,3 Мбайт) и относительно высокая (хотя и полиномиальная от размера входных данных) вычислительная сложность алгоритма декодирования [3]. Для уменьшения размера ключа исследователями предлагалось заменить коды Гоппы другими помехоустойчивыми кодами [4 – 7]. Однако эти системы оказались неустойчивы к атакам на ключ [8 – 13], а именно: для предложенных кодов найдены эффективные криптоаналитические алгоритмы структурных атак, которые по публичному ключу находят подходящий секретный ключ. Позднее были предложены некоторые модификации взломанных криптосистем. В частности, в [6] в качестве помехоустойчивого кода используется случайно выбранный подкод известного кода с эффективным алгоритмом декодирования. Однако слабость такого подхода показана в [10, 14]. В [15] для усиления предложено добавлять к порождающей матрице используемого кода случайные столбцы. Эта конструкция также оказалась нестойкой [16, 17].

Заметим, что имеющийся прогресс в области криптоанализа кодовых криптосистем позволяет предположить, что не исключено появление в будущем эффективных структурных атак и на оригинальную криптосистему на кодах Гоппы. Такое предположение подкрепляется, в частности, результатами работы [18], в которой построена эффективная структурная атака для одного класса подпространственных подкодов кодов Рида — Соломона. При этом известно, что коды Гоппы также являются классом подпространственных подкодов кодов Рида — Соломона, и возможно, что идеи, используемые в [18], могут применяться и в случае кодов Гоппы. Поэтому, несмотря на имеющиеся стойкие схемы, актуальна задача поиска других эффективно декодируемых кодов, обеспечивающих высокую стойкость кодовых криптосистем.

Один из подходов построения эффективно декодируемых кодов — комбинирование известных кодов [19]. Однако стоит отметить, что для некоторых известных кодовых конструкций уже получены результаты успешного криптоанализа систем типа Мак-Элиса, основанных на таких конструкциях. В частности, использование в такой криптосистеме прямой суммы известных кодов, как предложено в [20], не усиливает стойкость системы по сравнению со стойкостью системы Мак-Элиса на кодах-слагаемых. Вычислительная эквивалентность структурных атак для таких систем показана

в [21]. Использование повторения [4] и псевдоповторения (соединения) [22] кодов также не позволяет усилить стойкость криптосистемы, что показано в [23].

Представляется, что потенциально стойкой системой типа Мак-Элиса может являться система на произведении кодов. Такие коды и их обобщение — D-коды [24] — относятся к эффективно декодируемым: для некоторых классов этих кодов имеются быстрые алгоритмы мажоритарного декодирования [25, 26]. При этом анализ криптосистемы типа Мак-Элиса на произведении кодов, проведённый в [25], показал её высокую стойкость к структурным атакам. Заметим, что при анализе в [25] не использовалось произведение Шура — Адамара, преобразующее публичный ключ и часто позволяющее получить дополнительную информацию о ключе по свойствам такого преобразования [27, 10, 9, 28]. Позднее для кодов произведения в [29] исследованы некоторые свойства квадрата Шура — Адамара, которые могут быть использованы для построения структурной атаки на соответствующую кодовую криптосистему.

В настоящей работе исследуется стойкость криптосистемы Мак-Элиса на одном обобщении произведения кодов — D-кодах на основе кодов Рида — Маллера. Проводится анализ стойкости этой системы к атаке на основе произведения Шура — Адамара. Для этого исследуются свойства степеней Шура — Адамара D-кодов на основе кодов Рида — Маллера. Соответствующие результаты приводятся в п. 1. В п. 2 строится структурная атака с использованием произведения Шура — Адамара и на основе результатов п. 1 делается вывод о параметрах D-кодов, позволяющих противодействовать построенной атаке.

1. Свойства произведения Шура — Адамара D-конструкции на основе бинарных кодов Рида — Маллера

1.1. Бинарные коды Рида — Маллера

Пусть $\mathbb{F}_q^n$ — векторное пространство над полем Галуа $\mathbb{F}_q$. Для вектора $\mathbf{x} \in \mathbb{F}_q^n$ множество его ненулевых координат называется носителем вектора $\mathbf{x}$ и обозначается $\mathrm{supp}(\mathbf{x})$. Вес $\mathrm{wt}(\mathbf{x})$ вектора $\mathbf{x}$ определяется как $|\mathrm{supp}(\mathbf{x})|$ (здесь и далее символом $|A|$ обозначается мощность множества A). Линейное подпространство C размерности k пространства $\mathbb{F}_q^n$ называется линейным $[n,k]_q$-кодом [30]; $[n,k]_q$-код C с минимальным кодовым расстоянием $d = \min\limits_{\mathbf{c}\in C, \mathbf{c}\neq \mathbf{0}} \{\mathrm{wt}(\mathbf{c})\}$ называется $[n,k,d]_q$-кодом. Порождающую матрицу кода C обозначим через G_C, а двойственный код к коду C — через $\overline{C}$. Коды C и D длины n и размерности k называются перестановочно эквивалентными, если в симметрической группе перестановок $\mathcal{P}_n$, действующей на множестве $\{1,\dots,n\}$, найдётся перестановка σ, такая,что

$$\sigma(C) = \{(c_{\sigma^{-1}(1)},\dots,c_{\sigma^{-1}(n)}) : (c_1,\dots,c_n) \in C\} = D.$$

Напомним, что код C называется *разложимым*, если он перестановочно эквивалентен прямой сумме двух или более кодов ненулевой длины. Для двух векторов $\mathbf{a} = (a_1,\dots,a_n)$ и $\mathbf{b} = (b_1,\dots,b_n)$ из $\mathbb{F}_q^n$ произведением Шура — Адамара называется вектор $\mathbf{a}\star\mathbf{b} = (a_1b_1,\dots,a_nb_n)$; произведением Шура — Адамара $k\times n$-матрицы $A = (\mathbf{a}_i)$ и $l\times n$-матрицы $B = (\mathbf{b}_j)$ называется матрица $A\star B = (\mathbf{a}_i\star\mathbf{b}_j)$, $i = 1,\dots,k$, $j = 1,\dots,l$. Для кодов C и D из $\mathbb{F}_q^n$ их произведение Шура — Адамара определяется следующим образом:

$$C\star D = \mathcal{L}(\{\mathbf{x}\star\mathbf{y} | \mathbf{x}\in C, \mathbf{y}\in D\}).$$

Здесь и далее через $\mathcal{L}(U)$ обозначается линейная оболочка множества U. Известно [27], что $C \star D = \mathcal{L}(G_C \star G_D)$. Произведение $C \star C$ далее обозначается C^2 и называется квадратом кода C.

Для $(k_1 \times n_1)$-матрицы $A = (a_{i,j})$ и $(k_2 \times n_2)$-матрицы B их тензорное произведение $A \otimes B$ определяется как $(k_1 k_2 \times n_1 n_2)$-матрица вида

$$\begin{pmatrix} a_{1,1}B & \cdots & a_{1,n_1}B \\ \vdots & \ddots & \vdots \\ a_{k_1,1}B & \cdots & a_{k_1,n_1}B \end{pmatrix}. \tag{1}$$

Тензорное произведение $C_1 \otimes C_2$ двух $[n_i, k_i, d_i]_q$-кодов $C_i \subset \mathbb{F}_q^{n_i}$, где $i \in \{1, 2\}$, можно определить как $\mathcal{L}(G_{C_1} \otimes G_{C_2})$. Известно, что $C_1 \otimes C_2$ является $[n_1 n_2, k_1 k_2, d_1 d_2]_q$-кодом [19, п. 6.2.3], а из [31, теорема 5] вытекает, что

$$\overline{C_1 \otimes C_2} = \mathbb{F}_q^{n_1} \otimes \overline{C_2} + \overline{C_1} \otimes \mathbb{F}_q^{n_2}. \tag{2}$$

Действительно, согласно [31, формула (7)], порождающая матрица кода $\overline{C_1 \otimes C_2}$ может быть представлена в виде

$$G_{\overline{C_1 \otimes C_2}} = \begin{pmatrix} G_{\overline{C_1}} \otimes G_{\overline{C_2}} \\ A_1 \otimes G_{\overline{C_2}} \\ G_{\overline{C_1}} \otimes A_2 \end{pmatrix},$$

где A_1, A_2 — такие $k_1 \times n_1$- и $k_2 \times n_2$-матрицы, что

$$\mathcal{L}\begin{pmatrix} G_{\overline{C_1}} \\ A_1 \end{pmatrix} = \mathbb{F}_q^{n_1}, \quad \mathcal{L}\begin{pmatrix} G_{\overline{C_2}} \\ A_2 \end{pmatrix} = \mathbb{F}_q^{n_2}.$$

Следовательно,

$$\begin{aligned} \overline{C_1 \otimes C_2} &= \overline{C_1} \otimes \overline{C_2} + \mathcal{L}(A_1) \otimes \overline{C_2} + \overline{C_1} \otimes \mathcal{L}(A_2) = \\ &= \overline{C_1} \otimes \overline{C_2} + \mathcal{L}(A_1) \otimes \overline{C_2} + \overline{C_1} \otimes \mathcal{L}(A_2) + \overline{C_1} \otimes \overline{C_2} = \\ &= (\overline{C_1} + \mathcal{L}(A_1)) \otimes \overline{C_2} + \overline{C_1} \otimes (\overline{C_2} + \mathcal{L}(A_2)) = \\ &= \mathbb{F}_q^{n_1} \otimes \overline{C_2} + \overline{C_1} \otimes \mathbb{F}_q^{n_2}. \end{aligned}$$

Отметим, что порождающая матрица кода $\mathbb{F}_q^n \otimes C$ имеет блочно-диагональный вид: $G_{\mathbb{F}_q^n \otimes C} = \operatorname{diag}(G_C, \ldots, G_C)$. Поэтому код $\mathbb{F}_q^n \otimes C$ можно представить как прямую (внешнюю) сумму n кодов C:

$$\mathbb{F}_q^n \otimes C = \underbrace{C \oplus \ldots \oplus C}_{n}. \tag{3}$$

Широко известным классом линейных кодов является класс бинарных кодов Рида — Маллера. Для их определения и исследования некоторых их свойств рассмотрим $\mathbb{F}_2[x_1, \ldots, x_m]$ — кольцо полиномов от m переменных над полем $\mathbb{F}_2$. Полиномы из $\mathbb{F}_2[x_1, \ldots, x_m]$ будем записывать в виде

$$f(x_1, \ldots, x_m) = \sum_{\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_m) \in \mathbb{F}_2^m} f_{\boldsymbol{\alpha}} \bar{x}^{\boldsymbol{\alpha}},$$

где $\bar{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ — моном степени $\operatorname{wt}(\boldsymbol{\alpha})$. Для вектора $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_2^m$ символом $f(\boldsymbol{\alpha})$ будем обозначать значение полинома $f(x_1, \ldots, x_m)$, вычисленное при $x_i = \alpha_i$, $i = 1, \ldots, m$. Степень полинома f определяется как максимальная степень

его ненулевых мономов. Пусть $\mathbb{F}_2^{(r)}[x_1,\ldots,x_m]$ — линейное пространство полиномов из $\mathbb{F}_2[x_1,\ldots,x_m]$ степени не выше r. Определим оператор $E_{(m,r)}:\mathbb{F}_2^{(r)}[x_1,\ldots,x_m]\to\mathbb{F}_2^n$ следующим образом:

$$E_{(m,r)}(f)=(f(\boldsymbol{\alpha}_1),\ldots,f(\boldsymbol{\alpha}_{2^m})),$$

где $\boldsymbol{\alpha}_i,\boldsymbol{\alpha}_j\in\mathbb{F}_2^m$, $\boldsymbol{\alpha}_i\neq\boldsymbol{\alpha}_j$ для $i\neq j$, $n=2^m$. Бинарный код Рида — Маллера $\mathrm{RM}(m,r)$ с параметрами m и r определяется следующим образом:

$$\mathrm{RM}(m,r)=\{E_{(m,r)}(f):f\in\mathbb{F}_2^{(r)}[x_1,\ldots,x_m]\},$$

при этом $\mathrm{RM}(m,r)=\mathrm{RM}(m,m)=\mathbb{F}_2^n$ для $r\geqslant m$. Известно, что $\overline{\mathrm{RM}(m,r)}=\mathrm{RM}(m,m-r-1)$, а в [9] доказано, что

$$\mathrm{RM}(m,r_1)\star\mathrm{RM}(m,r_2)=\mathrm{RM}(m,r_1+r_2). \tag{4}$$

Из (4) и определения кода Рида — Маллера вытекает, что $\mathrm{RM}(m,r_1)\star\mathrm{RM}(m,r_2)=\mathbb{F}_2^n$ при $r_1+r_2\geqslant m$.

Лемма 1. Пусть $\mathrm{RM}(m_i,r_i)$ — бинарный код Рида — Маллера, $i=1,2$. Тогда

$$\mathrm{RM}(m_1,r_1)\otimes\mathrm{RM}(m_2,r_2)\subset\mathrm{RM}(m_1+m_2,r_1+r_2).$$

Доказательство. Рассмотрим тензорное произведение пространств $\mathbb{F}_2^{(r_1)}[x_1,\ldots,x_{m_1}]$ и $\mathbb{F}_2^{(r_2)}[y_1,\ldots,y_{m_2}]$, которое, по определению, имеет вид

$$\mathbb{F}_2^{(r_1)}[x_1,\ldots,x_{m_1}]\otimes\mathbb{F}_2^{(r_2)}[y_1,\ldots,y_{m_2}]=$$
$$=\{f\cdot g:f\in\mathbb{F}_2^{(r_1)}[x_1,\ldots,x_{m_1}],\ g\in\mathbb{F}_2^{(r_2)}[y_1,\ldots,y_{m_2}]\},$$

где $f\cdot g$ — произведение полиномов в кольце $\mathbb{F}_2[x_1,\ldots,x_{m_1},y_1,\ldots,y_{m_2}]$. Очевидно, что

$$\mathbb{F}_2^{(r_1)}[x_1,\ldots,x_{m_1}]\otimes\mathbb{F}_2^{(r_2)}[y_1,\ldots,y_{m_2}]\subset\mathbb{F}_2^{(r_1+r_2)}[x_1,\ldots,x_{m_1},y_1,\ldots,y_{m_2}].$$

Пусть $f\in\mathbb{F}_2^{(r_1)}[x_1,\ldots,x_{m_1}]$, $g\in\mathbb{F}_2^{(r_2)}[y_1,\ldots,y_{m_2}]$. Покажем, что

$$E_{(m_1+m_2,r_1+r_2)}(f\cdot g)=E_{(m_1,r_1)}(f)\otimes E_{(m_2,r_2)}(g).$$

Так как $(f\cdot g)(\boldsymbol{\alpha},\boldsymbol{\beta})=f(\boldsymbol{\alpha})g(\boldsymbol{\beta})$ для $\boldsymbol{\alpha}\in\mathbb{F}_2^{m_1}$, $\boldsymbol{\beta}\in\mathbb{F}_2^{m_2}$, то, с одной стороны,

$$E_{(m_1+m_2,r_1+r_2)}(f\cdot g)=\big((f\cdot g)(\boldsymbol{\alpha}_i,\boldsymbol{\beta}_j)\big)_{i=1,\ldots,2^{m_1},j=1,\ldots,2^{m_2}}=$$
$$=\big(f(\boldsymbol{\alpha}_i)g(\boldsymbol{\beta}_j)\big)_{i=1,\ldots,2^{m_1},j=1,\ldots,2^{m_2}},$$

с другой стороны, по определению тензорного произведения (1), получаем

$$E_{(m_1,r_1)}(f)\otimes E_{(m_2,r_2)}(g)=\big(f(\boldsymbol{\alpha}_i)g(\boldsymbol{\beta}_j)\big)_{i=1,\ldots,2^{m_1},j=1,\ldots,2^{m_2}},$$

что доказывает утверждение. ■

1.2. D-конструкция на кодах Рида — Маллера

Рассмотрим два семейства двоичных кодов Рида — Маллера:

$$\mathcal{S}_1 = \{C_1(0){=}\mathrm{RM}(m_1, m_1), C_1(1){=}\mathrm{RM}(m_1, m_1-1), \ldots, C_1(m_1){=}\mathrm{RM}(m_1, 0), C_1(J_1){=}\{\bar{0}\}\},$$
$$\mathcal{S}_2 = \{C_2(0){=}\mathrm{RM}(m_2, m_2), C_2(1){=}\mathrm{RM}(m_2, m_2-1), \ldots, C_2(m_2){=}\mathrm{RM}(m_2, 0), C_2(J_2){=}\{\bar{0}\}\},$$

где $J_t = m_t + 1$, $t = 1, 2$. Будем считать, что $C_t(i) = C_t(m_t + 1)$ для $i \geqslant m_t + 1$, $C_t(i) = C_t(0)$ для $i \leqslant 0$, $t = 1, 2$. Эти семейства для $t \in \{1, 2\}$ удовлетворяют условиям

$$C_t(0) \supset C_t(1) \supset C_t(2) \supset \cdots \supset C_t(J_t); \tag{5}$$
$$\overline{C_t(0)} \subset \overline{C_t(1)} \subset \overline{C_t(2)} \subset \cdots \subset \overline{C_t(J_t)}. \tag{6}$$

Поэтому для $i_1 \leqslant i_2$, $j_1 \leqslant j_2$ получаем

$$C_1(i_1) \otimes C_2(j_1) \supseteq C_1(i_2) \otimes C_2(j_2), \tag{7}$$
$$\overline{C_1(i_1)} \otimes \overline{C_2(j_1)} \subseteq \overline{C_1(i_2)} \otimes \overline{C_2(j_2)}.$$

Пусть $D_0 = \{(i, j) : i = 0, \ldots, J_1, j = 0, \ldots, J_2\}$. Для любого $D \subseteq D_0$ определим код

$$C(D) = \mathcal{L}\left(\bigcup_{(i,j)\in D} C_1(i) \otimes C_2(j)\right),\ C_1(i) \in \mathcal{S}_1,\ C_2(j) \in \mathcal{S}_2. \tag{8}$$

Далее будем рассматривать только такие множества $D \subset D_0$, которые удовлетворяют следующему условию: если $(i, j) \in D$ и существует пара $(k, s) \in D_0$, такая, что $k \geqslant i$, $s \geqslant j$, то $(k, s) \in D$. Набор таких множеств D обозначим через $F(D_0)$. Если $D \in F(D_0)$, то *D-кодом* называется код $\overline{C(D)}$, двойственный коду $C(D)$ вида (8). Отметим, что семейства $\mathcal{S}_1, \mathcal{S}_2$ удовлетворяют условиям для построения мажоритарного декодера [26, пример 3], поэтому рассматриваемые D-коды могут быть эффективно декодированы.

Рассмотрим определённые в [24] подмножества D^*, D_b, D_b^* множества D_0, которые строятся по $D \in F(D_0)$:

$$D^* = D_1^* \cup D_2^* \cup D_3^*, \tag{9}$$

где

$$D_1^* = \{(i, j) : (i-1, j-1) \in D_0, (i-1, j-1) \notin D\};$$
$$D_2^* = \begin{cases} \{(i, 0) : i = 0, \ldots, \min\limits_{(v,0)\in D}(v)\}, & \text{если } \min\limits_{(i,j)\in D}(j) = 0, \\ \{(i, 0) : i = 0, \ldots, J_1\} & \text{иначе;} \end{cases}$$
$$D_3^* = \begin{cases} \{(0, j) : j = 0, \ldots, \min\limits_{(0,v)\in D}(v)\}, & \text{если } \min\limits_{(i,j)\in D}(i) = 0, \\ \{(0, j) : j = 0, \ldots, J_2\} & \text{иначе;} \end{cases}$$
$$D_b = \{(i, j) : (i, j) \in D \wedge (i-1, j) \notin D \wedge (i, j-1) \notin D\};$$
$$D_b^* = \{(i, j) : (i, j) \in D^* \wedge (i, j+1) \notin D^* \wedge (i+1, j) \notin D^*\}. \tag{10}$$

Эти подмножества и условия вложенности (5) и (6) для рассматриваемых семейств позволяют определить D-код как сумму тензорных произведений кодов, двойственных к кодам из $\mathcal{S}_1$, $\mathcal{S}_2$, а также использовать простую формулу для вычисления размерности D-кода. Согласно [24, леммы 2 и 3], справедлива следующая

Теорема 1. Пусть $D \in F(D_0)$, $C_1(i) \in \mathcal{S}_1$, $C_2(j) \in \mathcal{S}_2$. Тогда

1) $\dim(C(D)) = \sum\limits_{(i,j)\in D} k_1(i)k_2(j)$, где $k_t(i) = \dim(C_t(i)) - \dim(C_t(i+1))$, $t = 1, 2$;

2) $C(D) = \mathcal{L}\left(\bigcup\limits_{(i,j)\in D_b} C_1(i) \otimes C_2(j)\right)$, $\overline{C(D)} = \mathcal{L}\left(\bigcup\limits_{(i,j)\in D_b^*} \overline{C_1(i)} \otimes \overline{C_2(j)}\right)$.

Замечание 1. Приведённое определение множества D^* немного отличается от оригинального из [24], тем не менее теорема 1 остаётся справедливой. Определение D^* уточняет поведение этого множества на границах D_0, что, в свою очередь, влияет на определение D_b^*. Это множество может отличаться от определённого в [24] в точках (i, j), таких, что $i = 0$ или $j = 0$. В этих точках $\overline{C_1(i)} \otimes \overline{C_2(j)} = \{\overline{0}\} \subset \mathbb{F}_2^{n_1 n_2}$, поэтому в теореме 1 такие точки не влияют на вид кода $\overline{C(D)}$.

Так как $\mathcal{S}_1$, $\mathcal{S}_2$ — семейства кодов Рида — Маллера, то

$$\begin{gathered} k_t(l) = \dim(\mathrm{RM}(m_t, m_t - l)) - \dim(\mathrm{RM}(m_t, m_t - l - 1)) = \\ = \sum_{p=0}^{m_t-l} C_{m_t}^p - \sum_{p=0}^{m_t-l-1} C_{m_t}^p = C_{m_t}^{m_t-l} + \sum_{p=0}^{m_t-l-1} C_{m_t}^p - \sum_{p=0}^{m_t-l-1} C_{m_t}^p = C_{m_t}^{m_t-l} = C_{m_t}^l, \end{gathered} \tag{11}$$

где $l = i$ для $t = 1$ и $l = j$ для $t = 2$. Поэтому в соответствии с п. 1 теоремы 1

$$\dim(C(D)) = \sum_{(i,j)\in D} C_{m_1}^i C_{m_2}^j. \tag{12}$$

Лемма 2. Если $D = \{(i, j) : i + j > \mu\}$, то $C(D) = \mathrm{RM}(m_1 + m_2, m_1 + m_2 - \mu - 1)$, где $\mu \in \{0, \ldots, m_1 + m_2 - 1\}$.

Доказательство. Для заданного D, по формуле (9), $D^* = \{(i, j) : i + j \leqslant \mu + 2\}$. В соответствии с замечанием 1 можно предполагать $i, j > 0$, а по п. 2 теоремы 1 код $\overline{C(D)}$ представим в виде

$$\overline{C(D)} = \mathcal{L}\left(\bigcup_{(i,j)\in D_b^*} \overline{\mathrm{RM}(m_1, m_1 - i)} \otimes \overline{\mathrm{RM}(m_2, m_2 - j)}\right),$$

где $D_b^* = \{(i, j) : i + j = \mu + 2\}$ по определению (10). Из свойства кода, двойственного к коду Рида — Маллера, и леммы 1 для любого $(i, j) \in D_b^*$ выполняется

$$\begin{gathered} \overline{\mathrm{RM}(m_1, m_1 - i)} \otimes \overline{\mathrm{RM}(m_2, m_2 - j)} = \mathrm{RM}(m_1, i - 1) \otimes \mathrm{RM}(m_2, j - 1) \subset \\ \subset \mathrm{RM}(m_1 + m_2, i + j - 2) = \mathrm{RM}(m_1 + m_2, \mu). \end{gathered}$$

Из этого следует, что

$$\overline{C(D)} \subseteq \mathrm{RM}(m_1 + m_2, \mu). \tag{13}$$

Теперь покажем, что

$$\dim(\overline{C(D)}) = \dim(\mathrm{RM}(m_1 + m_2, \mu)). \tag{14}$$

Из [24, формула (30)] с учётом (11) получаем

$$\dim(\overline{C(D)}) = \sum_{(i,j)\notin D} k_1(i)k_2(j) = \sum_{i+j\leqslant\mu} C_{m_1}^i C_{m_2}^j = \sum_{\lambda=0}^{\mu} \sum_{i=0}^{\lambda} C_{m_1}^i C_{m_2}^{\lambda-i}.$$

Из тождества Вандермонда следует формула $\sum\limits_{i=0}^{\lambda} C_{m_1}^i C_{m_2}^{\lambda-i} = C_{m_1+m_2}^{\lambda}$. Следовательно, $\dim(\overline{C(D)}) = \sum\limits_{\lambda=0}^{\mu} C_{m_1+m_2}^{\lambda}$. С другой стороны, $\dim(\mathrm{RM}(m_1 + m_2, \mu)) = \sum\limits_{\lambda=0}^{\mu} C_{m_1+m_2}^{\lambda}$. Отсюда получаем (14). Из (13) и (14) следует, что $\overline{C(D)} = \mathrm{RM}(m_1 + m_2, \mu)$ и $C(D) = \overline{\overline{C(D)}}$. ■

1.3. О разложимости степеней D-конструкции на бинарных кодах Рида — Маллера

Далее нам понадобится следующая техническая лемма:

Лемма 3. Пусть $D_b^* = \{(k_1, l_1), (k_2, l_2), \ldots, (k_s, l_s)\}$ для некоторого $D \in F(D_0)$, где $s \leqslant \min\{m_1, m_2\} + 1$, $k_i \in \{0, \ldots, m_1 + 1\}$, $l_i \in \{0, \ldots, m_2 + 1\}$. Последовательность $(k_i)_{i=1}^s$ — возрастающая тогда и только тогда, когда $(l_i)_{i=1}^s$ — убывающая последовательность.

Доказательство. Пусть $(k_i)_{i=1}^s$ — возрастающая последовательность. Предположим, что последовательность $(l_i)_{i=1}^s$ при этом не является убывающей. Это означает, что для $j > i$ существуют такие точки $(k_i, l_i), (k_j, l_j) \in D_b^*$, что $k_j > k_i$ и $l_j \geqslant l_i$. По определению множества D_b^* имеем $(k_i, l_i), (k_j, l_j) \in D^*$, при этом $(k_i + 1, l_i) \notin D^*$, где $k_i + 1 \leqslant k_j$. По определению множества D^* если $(k_j, l_j) \in D^*$, то $(k_j - 1, l_j - 1) \notin D$, а так как $D \in F(D_0)$, то $(k_p, l_p) \notin D$ для любых $k_p \leqslant k_j - 1$, $l_p \leqslant l_j - 1$. Это означает, что $(k_p, l_p) \in D^*$ для любых $k_p \leqslant k_j$, $l_p \leqslant l_j$ по определению D^*. Поэтому если $(k_j, l_j) \in D^*$, $k_j \geqslant k_i + 1$, $l_j \geqslant l_i$, то и $(k_i + 1, l_i) \in D^*$. Приходим к противоречию, значит, $(l_i)_{i=1}^s$ — убывающая последовательность. Аналогично утверждение доказывается в обратную сторону. ■

Рассмотрим семейства кодов $\mathcal{S}_1$, $\mathcal{S}_2$, определённые в п. 1.2. Пусть

$$D_b^* = \{(k_1, l_1), (k_2, l_2), \ldots, (k_s, l_s)\}, \tag{15}$$

где $s \leqslant \min\{m_1, m_2\}+1$; $k_i \in \{0, \ldots, m_1+1\}$; $l_i \in \{0, \ldots, m_2+1\}$; $(k_i)_{i=1}^s$ — возрастающая последовательность. Тогда по лемме 3 $(l_i)_{i=1}^s$ — убывающая. Поэтому в соответствии с п. 2 теоремы 1

$$\overline{C(D)} = \sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(l_i)}. \tag{16}$$

Для $s \geqslant 2$ и $i < s$ во введённых обозначениях получаем

$$\overline{C_1(k_i)} \subset \overline{C_1(k_{i+1})}, \overline{C_2(l_{i+1})} \subset \overline{C_2(l_i)}. \tag{17}$$

Пусть $r_{k_i}^1 = m_1 - k_i$ — порядок кода Рида — Маллера $C_1(k_i) = \mathrm{RM}(m_1, r_{k_i}^1)$, $r_{l_i}^2 = m_2 - l_i$ — порядок кода Рида — Маллера $C_2(l_i) = \mathrm{RM}(m_2, r_{l_i}^2)$, а

$$\overline{r}_{k_i}^1 = m_1 - (m_1 - k_i) - 1 = k_i - 1, \quad \overline{r}_{l_i}^2 = m_2 - (m_2 - l_i) - 1 = l_i - 1 \tag{18}$$

— порядки двойственных кодов $\overline{C_1(k_i)} = \mathrm{RM}(\overline{r}_{k_i}^1, m_1)$ и $\overline{C_2(l_i)} = \mathrm{RM}(\overline{r}_{l_i}^2, m_2)$ соответственно. Тогда с учётом (4), (16) и (18) получаем

$$\overline{C(D)}^2 = \left(\sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(l_i)}\right)^2 =$$

$$= \sum_{i=1}^{s} \overline{C_1(k_i)}^2 \otimes \overline{C_2(l_i)}^2 + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} (\overline{C_1(k_p)} \star \overline{C_1(k_j)}) \otimes (\overline{C_2(l_p)} \star \overline{C_2(l_j)}) = \tag{19}$$

$$= \sum_{i=1}^{s} \mathrm{RM}(2\overline{r}_{k_i}^1, m_1) \otimes \mathrm{RM}(2\overline{r}_{l_i}^2, m_2) + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \mathrm{RM}(\overline{r}_{k_p}^1 + \overline{r}_{k_j}^1, m_1) \otimes \mathrm{RM}(\overline{r}_{l_p}^2 + \overline{r}_{l_j}^2, m_2) =$$

$$= \sum_{i=1}^{s} \mathrm{RM}(2k_i - 2, m_1) \otimes \mathrm{RM}(2l_i - 2, m_2) + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \mathrm{RM}(k_p + k_j - 2, m_1) \otimes \mathrm{RM}(l_p + l_j - 2, m_2) =$$

$$= \sum_{i=1}^{s} \overline{C_1(2k_i - 1)} \otimes \overline{C_2(2l_i - 1)} + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \overline{C_1(k_p + k_j - 1)} \otimes \overline{C_2(l_p + l_j - 1)}. \tag{20}$$

Таким образом, код $\overline{C(D)}^2$ представляет собой сумму тензорных произведений двойственных кодов к кодам из семейств $\mathcal{S}_1$, $\mathcal{S}_2$. Отметим, что формула для нахождения размерности квадрата произвольного кода неизвестна. Но в случае кода $\overline{C(D)}$ эту формулу можно получить. Перепишем (20) в виде

$$\overline{C(D)}^2 = \sum_{i=1}^{s} C_1(m_1 - 2k_i + 2) \otimes C_2(m_2 - 2l_i + 2) + \\ + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} C_1(m_1 - (k_p + k_j) + 2) \otimes C_2(m_2 - (l_p + l_j) + 2).$$

Пусть $X = \{(m_1 - 2k_i + 2, m_2 - 2l_i + 2) : i \in \{1, \ldots, s\}\} \cup \{(m_1 - (k_p + k_j) + 2, m_2 - (l_p + l_j) + 2) : p, j \in \{1, \ldots, s\}, p \neq j\}$ — множество точек из D_0, которое соответствует коду $\overline{C(D)}^2$. Построим множество $D' \subseteq D_0$ следующим образом. Для каждой точки $(i, j) \in X$ добавим в D' все точки $(k, l) \in D_0$, такие, что $k \geqslant i$ и $l \geqslant j$. Отметим, что $D' \in F(D_0)$. Множеству D' соответствует код $C(D')$ вида (8). При этом коды, соответствующие точкам из D', либо совпадают с кодами, соответствующими точкам из X, либо, согласно (7), являются их подкодами. Следовательно,

$$C(D') = \overline{C(D)}^2.$$

Так как $D' \in F(D_0)$, то, согласно (12), размерность кода $\overline{C(D)}^2$ вычисляется по формуле

$$\dim(\overline{C(D)}^2) = \dim(C(D')) = \sum_{(i,j) \in D'} C^i_{m_1} C^j_{m_2}. \tag{21}$$

Рассмотрим случаи, при которых удаётся упростить представление (19).

Теорема 2. Пусть D^*_b вида (15), $\overline{C(D)}$ вида (16) и $\overline{r}^1_{k_i}, \overline{r}^2_{l_i}$ вида (18).

1) Если $\overline{r}^1_{k_1} \geqslant m_1/2$ и $\overline{r}^2_{l_1} < m_2/2$, то $\overline{C(D)}^2 = \mathbb{F}_2^{n_1} \otimes \overline{C_2(l_1)}^2$.

2) Если $\overline{r}^1_{k_s} < m_1/2$ и $\overline{r}^2_{l_s} \geqslant m_2/2$, то $\overline{C(D)}^2 = \overline{C_1(k_s)}^2 \otimes \mathbb{F}_2^{n_2}$.

Доказательство.

1) Согласно (4), если $\overline{r}^1_{k_1} \geqslant m_1/2$ и $\overline{r}^2_{l_1} < m_2/2$, то $\overline{C_1(k_1)}^2 = \mathbb{F}_2^{n_1}$ и $\overline{C_2(l_1)}^2 \neq \mathbb{F}_2^{n_2}$. Так как $(k_i)_{i=1}^s$ — возрастающая последовательность, из леммы 3 и (18) последовательность $(\overline{r}^1_{k_i})_{i=1}^s$ возрастающая, а $(\overline{r}^2_{l_i})_{i=1}^s$ — убывающая. Поэтому из (19) следует

$$\overline{C(D)}^2 = \sum_{i=1}^{s} \mathbb{F}_2^{n_1} \otimes \overline{C_2(l_i)}^2 + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \mathbb{F}_2^{n_1} \otimes (\overline{C_2(l_p)} \star \overline{C_2(l_j)}) = \\ = \mathbb{F}_2^{n_1} \otimes \left(\sum_{i=1}^{s} \overline{C_2(l_i)}^2 + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \overline{C_2(l_p)} \star \overline{C_2(l_j)} \right) = \mathbb{F}_2^{n_1} \otimes \overline{C_2(l_1)}^2,$$

где последнее равенство вытекает из вложений $\overline{C_2(l_p)} \star \overline{C_2(l_j)} \subseteq \overline{C_2(l_1)}^2$ и $\overline{C_2(l_i)}^2 \subseteq \subseteq \overline{C_2(l_1)}^2$, которые следуют из (4) и (17).

2) Согласно (4), если $\overline{r}^1_{k_s} < m_1/2$ и $\overline{r}^2_{l_s} \geqslant m_2/2$, то $\overline{C_1(k_s)}^2 \neq \mathbb{F}_2^{n_1}$ и $\overline{C_2(l_s)}^2 = \mathbb{F}_2^{n_2}$. Поэтому из (19) следует

$$\overline{C(D)}^2 = \sum_{i=1}^{s} \overline{C_1(k_i)}^2 \otimes \mathbb{F}_2^{n_2} + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} (\overline{C_1(k_p)} \star \overline{C_1(k_j)}) \otimes \mathbb{F}_2^{n_2} =$$

$$= \left(\sum_{i=1}^{s} \overline{C_1(k_i)}^2 + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_1(k_p)} \star \overline{C_1(k_j)} \right) \otimes \mathbb{F}_2^{n_2} = \overline{C_1(k_s)}^2 \otimes \mathbb{F}_2^{n_2}.$$

Теорема 2 доказана. ■

Согласно [23], двоичные коды Рида — Маллера $\mathrm{RM}(m, r)$ для $r < m$ являются неразложимыми. Так как $\overline{C_2(l_1)}^2$ — код Рида — Маллера, не совпадающий со всем пространством при выполнении условий первого утверждения теоремы 2, то, как следует из (3), код $\overline{C(D)}^2$ раскладывается в прямую сумму неразложимых кодов. При выполнении условий второго утверждения теоремы 2 код $\overline{C_1(k_s)}^2$ также является кодом Рида — Маллера, не совпадающим со всем пространством. Согласно [32, формула (10)], для любых двух матриц A и B найдутся такие перестановочные матрицы P и Q подходящих размеров, что $A \otimes B = P(B \otimes A)Q$. Тогда найдётся такая перестановка $\sigma \in \mathcal{P}_{n_1 n_2}$, что $\sigma(\overline{C_1(k_s)}^2 \otimes \mathbb{F}_2^{n_2}) = \mathbb{F}_2^{n_2} \otimes \overline{C_1(k_s)}^2$. Следовательно, в этом случае код $\overline{C(D)}^2$ является перестановочно эквивалентным прямой сумме неразложимых кодов.

Теорема 3. Пусть $\overline{C(D)}$ — код вида (16) и выполняется хотя бы одно из условий:

1) существует $i \in \{1, \ldots, s\}$, что $\overline{r}^1_{k_i} \geqslant m_1/2$ и $\overline{r}^2_{l_i} \geqslant m_2/2$;
2) существуют $p \in \{1, \ldots, s\}$, $j \in \{1, \ldots, s\}$, $p \neq j$, что $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} \geqslant m_1$ и $\overline{r}^2_{l_p} + \overline{r}^2_{l_j} \geqslant m_2$.

Тогда $\overline{C(D)}^2 = \mathbb{F}_2^{n_1 n_2}$.

Доказательство. Пусть выполняется первое условие, тогда из (4) следует, что $\overline{C_1(k_i)}^2 = \mathbb{F}_2^{n_1}$ и $\overline{C_2(l_i)}^2 = \mathbb{F}_2^{n_2}$. Значит, одно из слагаемых в (19) имеет вид $\mathbb{F}_2^{n_1} \otimes \mathbb{F}_2^{n_2}$. В этом случае $\overline{C(D)}^2 = \mathbb{F}_2^{n_1 n_2}$. Пусть теперь выполняется второе условие, тогда из (4) следует, что $\overline{C_1(k_p)} \star \overline{C_1(k_j)} = \mathbb{F}_2^{n_1}$ и $\overline{C_2(l_p)} \star \overline{C_2(l_j)} = \mathbb{F}_2^{n_2}$. Таким образом, одно из слагаемых в (19) имеет вид $\mathbb{F}_2^{n_1} \otimes \mathbb{F}_2^{n_2}$, поэтому $\overline{C(D)}^2 = \mathbb{F}_2^{n_1 n_2}$. ■

Отметим, что при выполнении условий теоремы 3 код $\overline{C(D)}^2$ совпадает с $\mathbb{F}_2^{n_1 n_2}$ и поэтому не эквивалентен прямой сумме нетривиальных кодов Рида — Маллера.

Теорема 4. Пусть $\overline{C(D)}$ — код вида (16) и выполняются условия $\overline{r}^1_{k_1} < m_1/2$, $\overline{r}^2_{l_1} \geqslant m_2/2$ и $\overline{r}^1_{k_j} \geqslant m_1/2$, $\overline{r}^2_{l_j} < m_2/2$ для любых $j \geqslant 2$. Если для любых $p \in \{1, \ldots, s\}$, $j \in \{1, \ldots, s\}$, $p \neq j$, выполняются неравенства $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} \geqslant m_1$ и $\overline{r}^2_{l_p} + \overline{r}^2_{l_j} < m_2$, то

$$\overline{C(D)}^2 = \overline{\tilde{C}_1 \otimes \tilde{C}_2}, \quad \overline{C(D)}^3 = \mathbb{F}_2^{n_1 n_2},$$

где $\tilde{C}_1 = \overline{\overline{C_1(k_1)}^2}$; $\tilde{C}_2 = \overline{\overline{C_2(l_2)}^2 + \sum\limits_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_2(l_p)} \star \overline{C_2(l_j)}}$.

Доказательство. При выполнении условий теоремы, согласно (4), формула (19) примет вид

$$\overline{C(D)}^2 = \overline{C_1(k_1)}^2 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes \overline{C_2(l_2)}^2 + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} (\overline{C_1(k_p)} \star \overline{C_1(k_j)}) \otimes (\overline{C_2(l_p)} \star \overline{C_2(l_j)}) =$$

$$= \overline{\overline{C_1(k_1)}^2} \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes \overline{\overline{C_2(l_2)}^2} + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} \mathbb{F}_2^{n_1} \otimes (\overline{C_2(l_p)} \star \overline{C_2(l_j)}) =$$

$$= \overline{\overline{C_1(k_1)}^2} \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes (\overline{\overline{C_2(l_2)}^2} + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_2(l_p)} \star \overline{C_2(l_j)}).$$

Согласно (2), во введённых в условии теоремы обозначениях получаем доказываемое утверждение. При этом

$$\overline{C(D)}^3 = (\overline{C_1(k_1)}^2 \otimes \mathbb{F}_2^{n_2} + \mathbb{F}_2^{n_1} \otimes (\overline{C_2(l_2)}^2 + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_2(l_p)} \star \overline{C_2(l_j)})) \star \overline{C(D)} =$$

$$= (\overline{C_1(k_1)}^2 \otimes \mathbb{F}_2^{n_2}) \star \left(\sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(l_i)} \right) +$$

$$+ (\mathbb{F}_2^{n_1} \otimes (\overline{C_2(l_2)}^2 + \sum_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_2(l_p)} \star \overline{C_2(l_j)})) \star \left(\sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(l_i)} \right).$$

Рассмотрим первое слагаемое:

$$(\overline{C_1(k_1)}^2 \otimes \mathbb{F}_2^{n_2}) \star \left(\sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(l_i)} \right) = (\overline{C_1(k_1)}^2 \star \overline{C_1(k_s)}) \otimes \mathbb{F}_2^{n_2} = \mathbb{F}_2^{n_1 n_2},$$

где последнее равенство вытекает из $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} \geqslant m_1$. Тогда $\overline{C(D)}^3 = \mathbb{F}_2^{n_1 n_2}$. ■

Следующая теорема доказывается аналогично.

Теорема 5. Пусть $\overline{C(D)}$ — код вида (16) и выполняются условия $\overline{r}^1_{k_j} < m_1/2$, $\overline{r}^2_{l_j} \geqslant m_2/2$ для любых $j < s$ и $\overline{r}^1_{k_s} \geqslant m_1/2$, $\overline{r}^2_{l_s} < m_2/2$. Если для любых $p \in \{1, \ldots, s\}$, $j \in \{1, \ldots, s\}$, $p \neq j$, выполняются неравенства $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} < m_1$ и $\overline{r}^2_{l_p} + \overline{r}^2_{l_j} \geqslant m_2$, то

$$\overline{C(D)}^2 = \overline{\hat{C}_1 \otimes \hat{C}_2}, \ \ \overline{C(D)}^3 = \mathbb{F}_2^{n_1 n_2},$$

где $\hat{C}_1 = \overline{\overline{C_1(k_{s-1})}^2 + \sum\limits_{\substack{p,j=1 \\ p\neq j}}^{s} \overline{C_1(k_p)} \star \overline{C_1(k_j)}}$, $\hat{C}_2 = \overline{C_2(l_s)}^2$.

Отметим, что в теоремах 4 и 5 коды $\tilde{C}_1$, $\tilde{C}_2$, $\hat{C}_1$, $\hat{C}_2$ — коды Рида — Маллера. Поэтому при выполнении условий теорем 4 и 5 код $\overline{C(D)}^2$ является неразложимым и не эквивалентен прямой сумме нетривиальных кодов Рида — Маллера.

В случаях, не рассмотренных в теоремах 2–5, представление (19) пока не удаётся упростить и сделать выводы о разложимости кода $\overline{C(D)}^2$ в прямую сумму кодов Рида — Маллера. Но можно вычислить размерность кода $\overline{C(D)}^2$ с помощью (21) и оценить возможность разложения этого кода в прямую сумму одинаковых кодов Рида — Маллера. Если код $\overline{C(D)}^2$ раскладывается в прямую сумму 2^{m_1} (2^{m_2}) одинаковых

кодов Рида — Маллера K длины 2^{m_2} (2^{m_1}), то, согласно (3), его размерность равна $2^{m_1}\dim(K)$ $(2^{m_2}\dim(K))$. Поэтому если размерность кода $\overline{C(D)}^2$ не делится на 2^{m_1} (2^{m_2}), то этот код не раскладывается в прямую сумму 2^{m_1} (2^{m_2}) одинаковых кодов Рида — Маллера и не является перестановочно эквивалентным такому коду.

2. Криптосистема типа Мак-Элиса на D-кодах и анализ её структурной стойкости

2.1. Криптосистема типа Мак-Элиса на D-кодах

Кодовая криптосистема, предложенная Р. Мак-Элисом в [2], строится на основе порождающей матрицы G_C линейного $[n,k,d]_q$-кода $C \subset \mathbb{F}_q^n$ и случайно выбранных невырожденной $(k\times k)$-матрицы S и перестановочной $(n\times n)$-матрицы P [2]. Пара $(\tilde{G},t)$, где $\tilde{G} = SG_CP$, $t = \lfloor (d-1)/2 \rfloor$, является публичным ключом, с помощью которого вектор $\mathbf{m} \in \mathbb{F}_q^k$ шифруется по правилу $\mathbf{c} = \mathbf{m}\tilde{G} + \mathbf{e}$, где вектор $\mathbf{e}$ обычно выбирается случайно и равновероятно, $\mathrm{wt}(\mathbf{e}) \leqslant t$. Для расшифрования применяется секретный ключ (S,P,C): $\mathbf{m} = S^{-1}\mathsf{Dec}_C(\mathbf{c}P^{-1})$, где $\mathsf{Dec}_C : \mathbb{F}_q^n \to \mathbb{F}_q^k$ — эффективный декодер для кода C. Криптосистему типа Мак-Элиса на коде C обозначим McE(C).

В настоящей работе обобщается криптосистема из [25] путём применения D-конструкции вместо тензорного произведения кодов, а именно: в качестве декодируемого кода используется код $\overline{C(D)}$ с быстрым мажоритарным декодером [26]. Отметим, что этот код может быть секретным для дополнительного усиления стойкости криптосистемы. Другими словами, множество D может быть частью секретного ключа. Перестановочная матрица P имеет размер $n_1n_2 \times n_1n_2$, а невырожденная матрица S — размер $\dim(\overline{C(D)}) \times \dim(\overline{C(D)})$. Матрица публичного ключа тогда имеет вид

$$\tilde{G} = S(G_{\overline{C(D)}})P. \tag{22}$$

Обозначим эту криптосистему McE$(C(D))$.

Отметим, что в соответствии с леммой 2 код $\overline{C(D)}$ может быть кодом Рида — Маллера. Учитывая результаты работ [9, 13], ключи криптосистемы McE$(C(D))$ при таких параметрах D-кода являются слабыми. Для выявления других возможных слабых ключей системы McE$(C(D))$ в настоящей работе используется произведение Шура — Адамара, а именно: строится атака для системы McE$(C(D))$, в которой используется разложимость степени Шура — Адамара D-кода, и на основе результатов п. 1.3 проводится анализ стойкости к разработанной атаке.

2.2. Атака на основе произведения Шура — Адамара

Рассмотрим код $\overline{C(D)}$ вида (16). Пусть $K = \dim(\overline{C(D)})$, $k = \dim(\overline{C_2(l_1)})$. Так как код $\overline{C(D)}$ имеет вид (16), то для $\tau_i = \{(i-1)n_2+1,\ldots,in_2\}$ проекция кода $\overline{C(D)}$ на множество τ_i, получаемая путём отбрасывания в кодовых словах всех координат, за исключением координат из множества τ_i, совпадает с $\overline{C_2(l_1)}$, $i = 1,\ldots,n_1$. Поэтому найдутся такие $(K\times k)$-матрицы M_1, …, M_{n_1} ранга k, что

$$G_{\overline{C(D)}} = (M_1|\ldots|M_{n_1})\mathrm{diag}(G_{\overline{C_2(l_1)}},\ldots,G_{\overline{C_2(l_1)}}). \tag{23}$$

Для кода $\overline{C_2(l_1)}$ и криптосистемы McE$(\overline{C_2(l_1)})$ обозначим через Attack алгоритм, принимающий на вход публичный ключ $\tilde{G}'$ криптосистемы Мак-Элиса на коде Рида — Маллера $\overline{C_2(l_1)}$ с порождающей матрицей $G_{\overline{C_2(l_1)}}$ и возвращающий невырожденную $(k\times k)$-матрицу S' и перестановочную $(n_2\times n_2)$-матрицу P', для которых $\tilde{G}' = S'G_{\overline{C_2(l_1)}}P'$.

Теорема 6. Пусть Attack — алгоритм полиномиальной сложности. Если $\overline{C(D)}^v = \mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v$ для некоторого $v(\in \mathbb{N})$ и код $\overline{C_2(l_1)}^v$ неразложимый, то существует алгоритм полиномиальной сложности, который по публичной матрице $\tilde{G}$ вида (22) находит такую перестановку π, что $\pi(\mathcal{L}(\tilde{G})) \subseteq \mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}$.

Доказательство. Публичная матрица $\tilde{G}$ вида (22), с учётом представления (23), имеет вид

$$\tilde{G} = S(G_{\overline{C(D)}})P = (\mathbf{M}_1 G_{\overline{C_2(l_1)}} | \dots | \mathbf{M}_{n_1} G_{\overline{C_2(l_1)}})P, \tag{24}$$

где $\mathbf{M}_i = SM_i$, $i = 1, \dots, n_1$. Обозначим через $\mathcal{P}_{n_1 n_2}$ симметрическую группу из $n_1 n_2$ элементов. Для удобства перестановку из этой группы, соответствующую матрице P в (24), обозначим ϕ. Вместо P иногда будем писать P_ϕ.

Из условия вытекает, что код с матрицей $\tilde{G}^v$ перестановочно эквивалентен тензорному произведению $\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v$. Так как по условию код $\overline{C_2(l_1)}^v$ неразложимый, то, применяя полиномиальный алгоритм Decomposition из [21] для разложения кода $\mathcal{L}(\tilde{G}^v)$ в прямую сумму подкодов, по матрице $\tilde{G}^v$ можно получить такую перестановку $\sigma(\in \mathcal{P}_{n_1 n_2})$, что

$$\tilde{G}^v P_\sigma \sim \operatorname{diag}(\dot{\mathbf{G}}_1, \dots, \dot{\mathbf{G}}_{n_1}), \tag{25}$$

где матрицы $\dot{\mathbf{G}}_i$ полного ранга порождают коды $C_{2,i} = \mathcal{L}(\dot{\mathbf{G}}_i) \sim \overline{C_2(l_1)}^v$. Тогда

$$\mathcal{L}(\tilde{G}^v P_\sigma) = \sigma(\phi(\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v)) = \sigma(\phi(\underbrace{\overline{C_2(l_1)}^v \oplus \dots \oplus \overline{C_2(l_1)}^v}_{n_1})) = C_{2,1} \oplus \dots \oplus C_{2,n_1}. \tag{26}$$

Из неразложимости кода $\overline{C_2(l_1)}^v$ вытекает, что группа перестановочных автоморфизмов кода $\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v$ в этом случае состоит из перестановок вида

$$\omega = \begin{pmatrix} 1, & \dots, & n_2, & n_2+1, & \dots, & 2n_2, & \dots, & (n_1-1)n_2+1, & \dots, & n_1 n_2 \\ x_1, & \dots, & x_{n_2}, & x_{n_2+1}, & \dots, & x_{2n_2}, & \dots, & x_{(n_1-1)n_2+1}, & \dots, & x_{n_1 n_2} \end{pmatrix} \tag{27}$$

с двумя ограничениями: 1) для каждого $i \in \{0, \dots, n_1 - 1\}$ найдётся единственное $j \in \{0, \dots, n_1 - 1\}$, такое, что $\{x_{in_2+1}, \dots, x_{(i+1)n_2}\} = \{jn_2 + 1, \dots, (j+1)n_2\}$; 2) каждый набор $(x_{in_2+1}, \dots, x_{(i+1)n_2})$ упорядочен так, что проекция кода $\omega(\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v)$, получаемая путём отбрасывания в кодовых словах всех координат, за исключением координат из множества $\{x_{in_2+1}, \dots, x_{(i+1)n_2}\}$, совпадает с $\overline{C_2(l_1)}^v$ [29, лемма 11]. Отсюда вытекает, что перестановка $\xi = \sigma \circ \phi$ в (26) имеет вид (27). Так как алгоритм Decomposition по разложимому коду находит перестановку, переводящую этот код в прямую сумму неразложимых кодов с точностью до перестановки координат в кодах — слагаемых, то для ξ выполняется только ограничение 1.

Учитывая (24), получаем

$$\begin{aligned} \tilde{G}P_\sigma &= S(G_{\overline{C_2(l_1)}})P_\phi P_\sigma = S(G_{\overline{C_2(l_1)}})P_\xi = (\mathbf{M}_1 G_{\overline{C_2(l_1)}} | \dots | \mathbf{M}_{n_1} G_{\overline{C_2(l_1)}})P_\xi = \\ &= (\mathbf{M}_{\theta^{-1}(1)} G_{\overline{C_2(l_1)}} P_{\gamma_1} | \dots | \mathbf{M}_{\theta^{-1}(n_1)} G_{\overline{C_2(l_1)}} P_{\gamma_{n_1}}) = \\ &= [\tilde{\mathbf{G}}_1 | \dots | \tilde{\mathbf{G}}_{n_1}], \quad \gamma_j \in \mathcal{P}_{n_2}, \quad j = 1, \dots, n_1, \end{aligned} \tag{28}$$

где θ — некоторая перестановка из $\mathcal{P}_{n_1}$, соответствующая ξ, а $\tilde{\mathbf{G}}_i = \mathbf{M}_{\theta^{-1}(i)} G_{\overline{C_2(l_1)}} P_{\gamma_i}$. При этом запись $\theta^{-1}(i)$ обозначает порядковый номер j матрицы M_j, которая после действия P_ξ находится в блочном представлении (28) на месте i-го блока.

Очевидно, что $\operatorname{rank}(\tilde{\mathbf{G}}_i) = k$ для всех $i = 1, \ldots, n_1$. По $\tilde{\mathbf{G}}_i$ легко построить соответствующую невырожденную $(k \times n_2)$-матрицу $\hat{\mathbf{G}}_i$, состоящую из k линейно независимых строк матрицы $\tilde{\mathbf{G}}_i$. Обозначим через F_i такую невырожденную $(K \times K)$-матрицу, что

$$F_i \tilde{\mathbf{G}}_i = \left[\frac{\hat{\mathbf{G}}_i}{O}\right],$$

где O — нулевая $((K-k) \times n_2)$-матрица. Матрица $\hat{\mathbf{G}}_i$ может рассматриваться как публичная матрица криптосистемы $\mathrm{McE}(\overline{C_2(l_1)})$. Применяя к каждой матрице $\hat{\mathbf{G}}_i$ алгоритм Attack, можно найти перестановочную матрицу P_{δ_i} ($\delta_i \in \mathcal{P}_{n_2}$) и невырожденную матрицу S'_i, что $\hat{\mathbf{G}}_i = S'_i G_{\overline{C_2(l_1)}} P_{\delta_i}$. Отсюда получаем

$$\tilde{G} P_\sigma \operatorname{diag}(P_{\delta_1}^{-1}, \ldots, P_{\delta_{n_1}}^{-1}) = [\tilde{\mathbf{G}}_1 P_{\delta_1}^{-1} | \ldots | \tilde{\mathbf{G}}_{n_1} P_{\delta_{n_1}}^{-1}] = \left[F_1^{-1}\left[\frac{\hat{\mathbf{G}}_1}{O}\right] P_{\delta_1}^{-1} \middle| \ldots \middle| F_{n_1}^{-1}\left[\frac{\hat{\mathbf{G}}_{n_1}}{O}\right] P_{\delta_{n_1}}^{-1}\right] =$$

$$= \left[F_1^{-1}\left[\frac{S'_1}{O'}\right] G_{\overline{C_2(l_1)}} \middle| \ldots \middle| F_{n_1}^{-1}\left[\frac{S'_{n_1}}{O'}\right] G_{\overline{C_2(l_1)}}\right] =$$

$$= [\hat{\mathbf{S}}_1 G_{\overline{C_2(l_1)}} | \ldots | \hat{\mathbf{S}}_{n_1} G_{\overline{C_2(l_1)}}] = [\hat{\mathbf{S}}_1 | \ldots | \hat{\mathbf{S}}_{n_1}](I_{n_1} \otimes G_{\overline{C_2(l_1)}}),$$

где O' — нулевая $((K-k) \times k)$-матрица; $\hat{\mathbf{S}}_i = F_i^{-1}\left[\frac{S'_i}{O'}\right]$. Следовательно, искомая перестановка имеет вид $\pi = \delta_1^{-1} \circ \ldots \circ \delta_{n_1}^{-1} \circ \sigma$. Так как Decomposition, Attack — алгоритмы полиномиальной сложности, то описанный алгоритм нахождения π также имеет полиномиальную сложность. ■

Отметим, что для произвольных линейных кодов C_1, C_2 над полем $\mathbb{F}_q$ существует такая перестановка σ, зависящая только от длин кодов C_1, C_2, что $C_1 \otimes C_2 = \sigma(C_2 \otimes \otimes C_1)$. Поэтому теорема 6 остаётся справедливой, если вместо $\overline{C(D)}^v = \mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}^v$ рассмотреть произведение $\overline{C(D)}^u = \overline{C_1(k_s)}^u \otimes \mathbb{F}_q^{n_2}$.

Рассмотрим криптосистему Мак-Элиса $\mathrm{McE}(\overline{C(D)})$. Теорема 6 показывает, что в ряде случаев по публичному ключу криптосистемы за полиномиальное время может быть найдена перестановка, позволяющая преобразовать этот ключ к более простому виду. Этот вид даёт возможность, например, использовать для дешифрования сообщений декодер кода $\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}$, заключающийся в применении декодера кода Рида — Маллера $\overline{C_2(l_1)}$ к каждому из n_1 блоков длины n_2. Ясно, что с большой вероятностью такой декодер будет ошибаться, так как кодовое расстояние кода $\mathbb{F}_q^{n_1} \otimes \overline{C_2(l_1)}$ меньше кодового расстояния D-кода, используемого в криптосистеме. Представляется, что уменьшить вероятность неправильного декодирования можно, например, применяя метод декодирования по информационным совокупностям и учитывая структуру кода. Для D-кода $\overline{C(D)}$, удовлетворяющего условиям теоремы 2, выполняются условия теоремы 6. Это позволяет сделать вывод, что коды с такими параметрами не подходят для использования в криптосистеме Мак-Элиса. С другой стороны, D-коды с параметрами, удовлетворяющими условиям одной из теорем 3–5, обеспечивают устойчивость к нахождению перестановки π. Это вытекает из того факта, что их квадрат совпадает со всем пространством или является неразложимым кодом. При этом, в случае неразложимости квадрата D-кода, его третья степень совпадает со всем пространством.

ЛИТЕРАТУРА

1. `http://csrc.nist.gov/projects/post-quantum-cryptography` — National Institute of Standards and Technology (NIST). Post-Quantum Cryptography, 2021.

2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. P. 42–44.
3. `https://classic.mceliece.org/nist/mceliece-20201010.pdf`. 2020.
4. *Sidel'nikov V. M.* Open coding based on Reed — Muller binary codes // Discr. Math. Appl. 1994. V. 4. No. 3. P. 191–207.
5. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Problems Control Inform. Theory. 1986. V. 15. No. 2. P. 159–166.
6. *Berger T. and Loidreau P.* How to mask the structure of codes for a cryptographic use // Des. Codes Cryptogr. 2005. V. 35. No. 1. P. 63–79.
7. *Janwa H. and Moreno O.* McEliece public cryptosystem using algebraic-geometric codes // Des. Codes Cryptogr. 1996. V. 8. P. 293–307.
8. *Couvreur A., Marquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes // IEEE Trans. Inform. Theory. 2017. V. 8. No. 63. P. 5404–5418.
9. *Chizhov I. V. and Borodin M. A.* Effective attack on the McEliece cryptosystem based on Reed — Muller codes // Discr. Math. Appl. 2014. V. 24. No. 5. P. 273–280.
10. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes // LNCS. 2010. V. 6061. P. 61–72.
11. *Sidel'nikov V. M. and Shestakov S. O.* On an encoding system constructed on the basis of generalized Reed — Solomon codes // Discr. Math. Appl. 1992. V. 4. No. 2. P. 439–444.
12. *Деундяк В. М., Дружинина М. А., Косолапов Ю. В.* Модификация криптоаналитического алгоритма Сидельникова — Шестакова для обобщенных кодов Рида — Соломона и ее программная реализация // Изв. вузов. Северо-Кавказский регион. Сер.: Технические науки. 2006. № 4. С. 15–19.
13. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
14. *Бородин М. А., Чижов И. В.* Классификация произведений Адамара подкодов коразмерности 1 кодов Рида — Маллера // Дискретная математика. 2020. Т. 32. № 1. С. 115–134.
15. *Wieschebrink C.* Two NP-complete problems in coding theory with an application in code based cryptography // IEEE Intern. Symp. Inform. Theory. 2006. P. 1733–1737.
16. *Couvreur A., Gaborit P., Gauthier-Umana V., et al.* Distinguisher-based attacks on public-key cryptosystems using Reed — Solomon codes // Des. Codes Cryptogr. 2014. V. 73. P. 641–666.
17. *Otmani A. and Kalachi H.* Square code attack on a modified Sidelnikov cryptosystem // LNCS. 2015. V. 9084. P. 173–183.
18. *Couvreur A. and Lequesne M.* On the security of subspace subcodes of Reed — Solomon codes for public key encryption // IEEE Trans. Inform. Theory. 2022. V. 68. No. 1. P. 632–648.
19. *Morelos-Zaragoza R. H.* The Art of Error Correcting Coding. John Wiley & Sons, Ltd. 2006. 263 p.
20. *Деундяк В. М., Косолапов Ю. В.* Криптосистема на индуцированных групповых кодах // Модел. и анализ информ. систем. 2016. Т. 23. № 2. С. 137–152.
21. *Деундяк В. М., Косолапов Ю. В.* Анализ стойкости некоторых кодовых криптосистем, основанный на разложении кодов в прямую сумму // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2019. Т. 12. № 3. С. 89–101.
22. *Egorova E., Kabatiansky G., Krouk E., and Tavernier C.* A new code-based public-key cryptosystem resistant to quantum computer attacks // J. Phys. Conf. Ser. 2019. V. 1163. P. 1–5.
23. *Deundyak V. M., Kosolapov Yu. V., and Maystrenko I. A.* On the decipherment of Sidel'nikov-type cryptosystems // LNCS. 2020. V. 12087. P. 20–40.

24. *Kasami T. and Lin S.* On the construction of a class of majority-logic decodable codes // IEEE Trans. Inform. Theory. 1971. V. IT-17. No. 5. P. 600–610.
25. *Deundyak V. M., Kosolapov Yu. V., and Lelyuk E. A.* Decoding the tensor product of MLD codes and applications for code cryptosystems // Automatic Control Comput. Sci. 2018. V. 52. No. 7. P. 647–657.
26. *Deundyak V. M. and Lelyuk E. A.* A graph-theoretical method for decoding some group MLD-codes // J. Appl. Industr. Math. 2020. V. 14. No. 2. P. 265–280.
27. *Randriambololona H.* On products and powers of linear codes under componentwise multiplication // Algorithmic Arithmetic Geometry Coding Theory. 2015. V. 637. P. 3–78.
28. *Deundyak V. M. and Kosolapov Yu. V.* On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes // XVI Intern. Symp. Prob. of Redundancy in Information and Control Systems. Russia, 2019. P. 143–148.
29. *Деундяк В. М., Косолапов Ю. В.* О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. № 50. С. 72–86.
30. *Сидельников В. М.* Теория кодирования. М.: Физматлит, 2008.
31. *Grassl M. and Rotteler M.* Quantum block and convolutional codes from self-orthogonal product codes // Proc. IEEE Int. Symp. Inf. Theory. 2005. P. 1018–1022.
32. *Henderson H. V. and Searle S. R.* The vec-permutation matrix, the vec operator and Kronecker products: A review // Linear and Multilinear Algebra. 1981. No. 9. P. 271–288.

REFERENCES

1. `http://csrc.nist.gov/projects/post-quantum-cryptography` — National Institute of Standards and Technology (NIST). Post-Quantum Cryptography, 2021.
2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 1978, pp. 42–44.
3. `https://classic.mceliece.org/nist/mceliece-20201010.pdf`, 2020.
4. *Sidel'nikov V. M.* Open coding based on Reed — Muller binary codes. Discr. Math. Appl., 1994, vol. 4, no. 3, pp. 191–207.
5. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory. Problems Control Inform. Theory, 1986, vol. 15, no. 2, pp. 159–166.
6. *Berger T. and Loidreau P.* How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 2005, vol. 35, no. 1, pp. 63–79.
7. *Janwa H. and Moreno O.* McEliece public cryptosystem using algebraic-geometric codes. Des. Codes Cryptogr., 1996, vol. 8, pp. 293–307.
8. *Couvreur A., Marquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. IEEE Trans. Inform. Theory, 2017, vol. 8, no. 63, pp. 5404–5418.
9. *Chizhov I. V. and Borodin M. A.* Effective attack on the McEliece cryptosystem based on Reed — Muller codes. Discr. Math. Appl., 2014, vol. 24, no. 5, pp. 273–280.
10. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. LNCS, 2010, vol. 6061, pp. 61–72.
11. *Sidel'nikov V. M. and Shestakov S. O.* On an encoding system constructed on the basis of generalized Reed — Solomon codes. Discr. Math. Appl., 1992, vol. 4, no. 2, pp. 439–444.
12. *Deundyak V. M., Druzhinina M. A., and Kosolapov Yu. V.* Modifikatsiya kriptoanaliticheskogo algoritma Sidel'nikova — Shestakova dlya obobshchennykh kodov Rida — Solomona i ee programmnaya realizatsiya [Modification of the Sidelnikov — Shestakov cryptanalytic

algorithm for generalized Reed — Solomon codes and its software implementation]. Izv. Vuzov. Severo-Kavkazskiy Region. Ser. Tekhnicheskie Nauki, 2006, no. 4, pp. 15–19. (in Russian)

13. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem. LNCS, 2007, vol. 4515, pp. 347–360.
14. *Borodin M. A. and Chizhov I. V.* Klassifikatsiya proizvedeniy Adamara podkodov korazmernosti 1 kodov Rida — Mallera [Classification of Hadamard products of codimension 1 subcodes of Reed — Muller codes]. Diskretnaya Matematika, 2020, vol. 32, no. 1, pp. 115–134. (in Russian)
15. *Wieschebrink C.* Two NP-complete problems in coding theory with an application in code based cryptography. IEEE Intern. Symp. Inform. Theory, 2006, pp. 1733–1737.
16. *Couvreur A., Gaborit P., Gauthier-Umana V., et al.* Distinguisher-based attacks on public-key cryptosystems using Reed — Solomon codes. Des. Codes Cryptogr., 2014, vol. 73, pp. 641–666.
17. *Otmani A. and Kalachi H.* Square code attack on a modified Sidelnikov cryptosystem. LNCS, 2015, vol. 9084, pp. 173–183.
18. *Couvreur A. and Lequesne M.* On the security of subspace subcodes of Reed — Solomon codes for public key encryption. IEEE Trans. Inform. Theory, 2022, vol. 68, no. 1, pp. 632–648.
19. *Morelos-Zaragoza R. H.* The Art of Error Correcting Coding. John Wiley & Sons, Ltd, 2006. 263 p.
20. *Deundyak V. M. and Kosolapov Yu. V.* Kriptosistema na indutsirovannykh gruppovykh kodakh [Cryptosystem on induced group codes]. Model. i Analiz Inform. Sistem, 2016, vol. 23, no. 2, pp. 137–152. (in Russian)
21. *Deundyak V. M. and Kosolapov Yu. V.* Analiz stoykosti nekotorykh kodovykh kriptosistem, osnovannyy na razlozhenii kodov v pryamuyu summu [Analysis of the stability of some code cryptosystems based on the decomposition of codes into a direct sum]. Vestn. YuUrGU. Ser. Matem. Modelirovanie i Programmirovanie, 2019, vol. 12, no. 3, pp. 89–101. (in Russian)
22. *Egorova E., Kabatiansky G., Krouk E., and Tavernier C.* A new code-based public-key cryptosystem resistant to quantum computer attacks. J. Phys. Conf. Ser., 2019, vol. 1163, pp. 1–5.
23. *Deundyak V. M., Kosolapov Yu. V., and Maystrenko I. A.* On the decipherment of Sidel'nikov-type cryptosystems. LNCS, 2020, vol. 12087, pp. 20–40.
24. *Kasami T. and Lin S.* On the construction of a class of majority-logic decodable codes. IEEE Trans. Inform. Theory, 1971, vol. IT-17, no. 5, pp. 600–610.
25. *Deundyak V. M., Kosolapov Yu. V., and Lelyuk E. A.* Decoding the tensor product of MLD codes and applications for code cryptosystems. Automatic Control Comput. Sci., 2018, vol. 52, no. 7, pp. 647–657.
26. *Deundyak V. M. and Lelyuk E. A.* A graph-theoretical method for decoding some group MLD-codes. J. Appl. Industr. Math., 2020, vol. 14, no. 2, pp. 265–280.
27. *Randriambololona H.* On products and powers of linear codes under componentwise multiplication. Algorithmic Arithmetic Geometry Coding Theory, 2015, vol. 637, pp. 3–78.
28. *Deundyak V. M. and Kosolapov Yu. V.* On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes. XVI Intern. Symp. Prob. of Redundancy in Information and Control Systems. Russia, 2019, pp. 143–148.
29. *Deundyak V. M. and Kosolapov Yu. V.* O nekotorykh svoystvakh proizvedeniya Shura — Adamara dlya lineynykh kodov i ikh prilozheniyakh [On some properties of the Schur — Hadamard product for linear codes and their applications]. Prikladnaya Diskretnaya Matematika, 2020, no. 50, pp. 72–86.
30. *Sidel'nikov V. M.* Teoriya kodirovaniya [Coding Theory]. Moscow, Fizmatlit Publ., 2008.

31. *Grassl M. and Rotteler M.* Quantum block and convolutional codes from self-orthogonal product codes. Proc. IEEE Int. Symp. Inf. Theory, 2005, pp. 1018–1022.
32. *Henderson H. V. and Searle S. R.* The vec-permutation matrix, the vec operator and Kronecker products: A review. Linear and Multilinear Algebra, 1981, no. 9, pp. 271–288.