ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 621.391.7

О НЕКОТОРЫХ СВОЙСТВАХ ПРОИЗВЕДЕНИЯ ШУРА — АДАМАРА ДЛЯ ЛИНЕЙНЫХ КОДОВ И ИХ ПРИЛОЖЕНИЯХ

В. М. Деундяк, Ю. В. Косолапов

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

Произведение Шура — Адамара активно используется при криптоанализе асимметричных кодовых криптосистем типа Мак-Элиса, основанных на линейных кодах. Именно, это произведение успешно применяется при криптоанализе кодовых систем на подкодах обобщённых кодов Рида — Соломона, на двоичных кодах Рида — Маллера и их подкодах коразмерности 1, на соединении некоторых известных кодов. В качестве способа усиления стойкости криптосистемы авторами ранее предложена система на тензорном произведении линейных кодов. С целью анализа стойкости этой системы в настоящей работе исследуются свойства произведения Шура — Адамара для тензорного произведения произвольных линейных кодов. В результате получены необходимые и достаточные условия, когда s-я степень тензорного произведения кодов перестановочно эквивалентна прямой сумме кодов. Этот результат позволяет, в частности, выбирать параметры линейных кодов так, чтобы произведение Шура — Адамара для тензорного произведения совпадало со всем пространством, в котором это произведение определено. Таким образом, могут быть определены параметры линейных кодов, при которых атака на основе произведения Шура — Адамара, применённого к публичному ключу, не проходит. Получены некоторые новые свойства произведения Шура — Адамара для линейных кодов, которые позволили, в частности, доказать неразложимость двоичных кодов Рида — Маллера. Как следствие, доказана теорема о структуре группы перестановочных автоморфизмов прямой суммы неразложимых кодов.

Ключевые слова: *тензорное произведение, разложимость кодов, криптосистемы типа Мак-Элиса.*

DOI 10.17223/20710410/50/5

ON SOME PROPERTIES OF THE SCHUR — HADAMARD PRODUCT FOR LINEAR CODES AND THEIR APPLICATIONS

V. M. Deundyak, Yu. V. Kosolapov

Southern Federal University, Rostov-on-Don, Russia

E-mail: vl.deundyak@gmail.com, itaim@mail.ru

The Shur — Hadamard product is actively used in the cryptanalysis of asymmetric code cryptosystems like McEliece based on linear codes. Namely, this product is successfully used in cryptanalysis of code systems on subcodes of generalized Reed — Solomon codes, on binary Reed — Muller codes and their subcodes of codimension 1, on the combination of some well known codes. As a way to enhance the security of

a cryptosystem, the authors have previously proposed a system based on the tensor product of linear codes. In order to analyze the security of this system, in this paper we study the properties of the Schur — Hadamard product for the tensor product of arbitrary linear codes. As a result, necessary and sufficient conditions are obtained when the sth power of the tensor product of codes is permutationally equivalent to the direct sum of codes. This result allows, in particular, to choose the parameters of linear codes so that the Schur — Hadamard product for the tensor product coincides with the entire space in which this product is defined. Thus, the parameters of linear codes can be determined, at which the attack based on the Shur — Hadamard product applied to the public key fails. Also, some new results on the Schur — Hadamard product for linear codes were obtained, which made it possible, in particular, to prove the indecomposability of binary Reed — Muller codes. A theorem on the structure of the group of permutation automorphisms of a direct sum of indecomposable codes is proved.

Keywords: *tensor product codes, decomposability of codes, McEliece type systems.*

Введение

Асимметричные кодовые криптосистемы типа Мак-Элиса [1] характеризуются более высокой скоростью операций шифрования и расшифрования по сравнению с соответствующими операциями используемых в настоящее время асимметричных криптосистем. Это связано с тем, что в операциях шифрования и расшифрования кодовых систем используются, как правило, только матричная арифметика и алгоритмы решения систем линейных уравнений над полями небольшой мощности. В системах RSA или Эль-Гамаля выполняются операции с большими числами, что в вычислительном отношении более затратно. Кодовые криптосистемы устойчивы также к атакам с использованием квантовых компьютеров [2], поэтому они рассматриваются как альтернатива современным асимметричным криптосистемам [3].

Многие успешные атаки на кодовые криптосистемы основаны на применении произведения Шура — Адамара к публичному ключу [4 – 11]. В [12] предложена кодовая криптосистема типа Мак-Элиса, основанная на тензорном произведении кодов $C_1 \otimes C_2$. Настоящая работа посвящена исследованию свойств произведения Шура — Адамара для тензорного произведения линейных кодов. Работа имеет следующую структуру. В п. 1 исследуются свойства произведения Шура — Адамара для тензорного произведения кодов, в частности получены необходимые и достаточные условия того, что s-я степень тензорного произведения кодов перестановочно эквивалентна прямой сумме кодов. В п. 2 на основе некоторых результатов из п. 1 доказана неразложимость бинарных кодов Рида — Маллера, а также вычислена группа перестановочных автоморфизмов прямой суммы неразложимых кодов.

1. Свойства произведения Шура — Адамара для тензорного произведения кодов

Пусть $\mathbb{F}_q$ — поле Галуа мощности q. Под линейным $[n, k, d]_q$-кодом будем понимать подпространство размерности k пространства $\mathbb{F}_q^n$ над конечным полем $\mathbb{F}_q$, имеющее кодовое расстояние d. Такой код иногда будем называть $[n, k]_q$-кодом. Тензорное произведение $A \otimes B$ для $(k_1 \times n_1)$-матрицы A и $(k_2 \times n_2)$-матрицы B определяется равенством

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,n_1}B \\ \vdots & \ddots & \vdots \\ a_{k_1,1}B & \dots & a_{k_1,n_1}B \end{pmatrix}.$$

Для векторов $\mathbf{a} = (a_1, \dots, a_n)$ и $\mathbf{b} = (b_1, \dots, b_n)$ из $\mathbb{F}_q^n$ рассмотрим покоординатное умножение $\mathbf{a} \star \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$, также называемое произведением Шура или произведением Адамара [13]. Произведением Шура — Адамара $(k_A \times n)$-матрицы $A = (\mathbf{a}_i)_{i=1}^{k_A}$ и $(k_B \times n)$-матрицы $B = (\mathbf{b}_i)_{i=1}^{k_B}$ называется $(k_A k_B \times n)$-матрица вида

$$A \star B = \begin{pmatrix} \mathbf{a}_1 \star \mathbf{b}_1 \\ \vdots \\ \mathbf{a}_1 \star \mathbf{b}_{k_B} \\ \mathbf{a}_2 \star \mathbf{b}_1 \\ \vdots \\ \mathbf{a}_{k_A} \star \mathbf{b}_{k_B} \end{pmatrix}. \tag{1}$$

Произведение $A \star A$ будем обозначать A^2. Для натурального n симметрическую группу перестановок множества $\underline{n} = \{1, \dots, n\}$ обозначим $\mathcal{S}_n$. Под действием перестановки $\sigma \in \mathcal{S}_n$ на вектор $\mathbf{a} = (a_1, \dots, a_n)$ будем понимать перестановку координат этого вектора в соответствии с σ:

$$\sigma(\mathbf{a}) = (a_{\sigma(1)}, \dots, a_{\sigma(n)});$$

$\sigma(U) = \{\sigma(\mathbf{u}) : \mathbf{u} \in U\}$, где U — множество векторов длины n. Композицию перестановок $\sigma, \delta \in \mathcal{S}_n$ обозначим $\sigma \circ \delta$, причём $(\sigma \circ \delta)(i) = \sigma(\delta(i))$. Пусть $r(A)$ — ранг матрицы A. Единичную $(n \times n)$-матрицу обозначим I_n.

Лемма 1. Произведение Шура — Адамара обладает следующими свойствами:

1) $\forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \, (\mathbf{a} \star \mathbf{b} = \mathbf{b} \star \mathbf{a})$;
2) $\forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \, \forall \sigma \in \mathcal{S}_n \, \forall a, b \in \mathbb{F} \, \big(\sigma(a\mathbf{a} \star b\mathbf{b}) = ab(\sigma(\mathbf{a}) \star \sigma(\mathbf{b}))\big)$;
3) $\forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n \, \big((\mathbf{a} + \mathbf{b}) \star \mathbf{c} = (\mathbf{a} \star \mathbf{c}) + (\mathbf{b} \star \mathbf{c})\big)$;
4) для любых матриц A и B размера $(k_A \times n)$ и $(k_B \times n)$ соответственно

$$r(A \star B) \leqslant k_A k_B;$$

5) $\forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \, \forall \mathbf{c}, \mathbf{d} \in \mathbb{F}_q^m \, \big((\mathbf{a} \otimes \mathbf{c}) \star (\mathbf{b} \otimes \mathbf{d}) = (\mathbf{a} \star \mathbf{b}) \otimes (\mathbf{c} \star \mathbf{d})\big)$;
6) для любых матриц A и B размера $(k_A \times n)$ и $(k_B \times n)$ соответственно и любой $(n \times n)$-матрицы перестановки Q выполняется равенство

$$(AQ) \star (BQ) = (A \star B)Q.$$

Доказательство. Свойства 1–4 вытекают из определения произведения Шура — Адамара для векторов и матриц.

Докажем свойство 5. Пусть $\mathbf{a} = (a_1, \dots, a_n)$, $\mathbf{b} = (b_1, \dots, b_n)$. По определению тензорного произведения и произведения Шура — Адамара получаем

$$\begin{aligned}(\mathbf{a} \otimes \mathbf{c}) \star (\mathbf{b} \otimes \mathbf{d}) &= (a_1\mathbf{c}, \dots, a_n\mathbf{c}) \star (b_1\mathbf{d}, \dots, b_n\mathbf{d}) = \\ &= (a_1 b_1 \mathbf{c} \star \mathbf{d}, \dots, a_n b_n \mathbf{c} \star \mathbf{d}) = (\mathbf{a} \star \mathbf{b}) \otimes (\mathbf{c} \star \mathbf{d}),\end{aligned}$$

где запись $(\mathbf{x}, \mathbf{y})$ означает приписывание вектора $\mathbf{y}$ справа к вектору $\mathbf{x}$.

Докажем свойство 6. Из определения (1) произведения Шура — Адамара для матриц получаем, что

$$(AQ) \star (BQ) = ((\mathbf{a}_i Q) \star (\mathbf{b}_j Q))_{i \in \underline{k_A}, j \in \underline{k_B}},$$

где $\mathbf{a}_i$ и $\mathbf{b}_j$ — строки матриц A и B соответственно. Из свойства 2 вытекает, что $(\mathbf{a}_i Q) \star \star (\mathbf{b}_j Q) = (\mathbf{a}_i \star \mathbf{b}_j)Q$. Отсюда получаем требуемое равенство. ■

Множество всех порождающих матриц кода C обозначим $\mathcal{G}(C)$. Отметим, что $C = \mathcal{L}(G_C)$ для всех G_C из $\mathcal{G}(C)$, где $\mathcal{L}(A)$ — линейная оболочка, натянутая на строки матрицы A. Для $[n, k_1]_q$-кода C_1 и $[n, k_2]_q$-кода C_2 их произведение Шура — Адамара определяется как линейная оболочка, натянутая на множество векторов $\{\mathbf{a} \star \mathbf{b} : \mathbf{a} \in C_1, \mathbf{b} \in C_2\}$:

$$C_1 \star C_2 = \mathcal{L}\left(\{\mathbf{a} \star \mathbf{b} : \mathbf{a} \in C_1, \mathbf{b} \in C_2\}\right). \tag{2}$$

Квадратом кода C называется пространство (код) $C \star C = C^2$. Аналогично может быть определена любая степень s кода C: $C^s = C^{s-1} \star C$. Для $\tau \subseteq \underline{n}$ через $\mathbb{F}_q^n(\tau)$ обозначим $|\tau|$-мерное координатное подпространство пространства $\mathbb{F}_q^n$, полагая, что все векторы из $\mathbb{F}_q^n(\tau)$ на координатах из $\underline{n} \setminus \tau$ имеют нулевые значения.

Носителем вектора $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ назовём множество $\mathrm{supp}(\mathbf{x}) = \{i \in \underline{n} : x_i \neq 0\}$, а носителем $A \subseteq \mathbb{F}_q^n$ — множество $\mathrm{supp}(A) = \bigcup\limits_{\mathbf{a} \in A} \mathrm{supp}(\mathbf{a})$. Говорят, что $[n, k, d]_q$-код C не имеет фиктивных или нулевых координат, если $\mathrm{supp}(C) = \underline{n}$. Заметим, что $[n, k, d]_q$-код C для $n > 1$ не имеет фиктивных координат тогда и только тогда, когда кодовое расстояние кода $C^\perp$, дуального к коду C, не менее двух.

Лемма 2. Пусть C — $[n, k]_q$-код, $\tau \subseteq \underline{n}$ — множество ненулевых координат кода. Тогда $C \star \mathbb{F}_q^n = \mathbb{F}_q^n \star C = \mathbb{F}_q^n(\tau)$.

Доказательство. Пусть M_C и $M_{\mathbb{F}_q^n}$ — матрицы, строками которых являются все кодовые слова кода C и пространства $\mathbb{F}_q^n$ соответственно. По условию в матрице M_C столбцы с номерами из τ ненулевые, а остальные нулевые, следовательно, в матрице $M_C \star M_{\mathbb{F}_q^n}$ все столбцы с номерами из $\underline{n} \setminus \tau$ нулевые, а с номерами из τ — ненулевые, причём в $M_C \star M_{\mathbb{F}_q^n}$ найдутся $|\tau|$ строк, образующих базис пространства $\mathbb{F}_q^n(\tau)$. Последнее следует из того, что для каждого $i \in \tau$ в матрице M_C найдётся строка с ненулевой i-й координатой и найдётся строка в матрице $M_{\mathbb{F}_q^n}$ веса один также с ненулевой i-й координатой. Поэтому из (2) имеем $C \star \mathbb{F}_q^n = \mathbb{F}_q^n \star C = \mathcal{L}(M_C \star M_{\mathbb{F}_q^n}) = \mathbb{F}_q^n(\tau)$. ■

Из леммы 2 получаем, что если $[n, k]_q$-код C не имеет фиктивных координат, то

$$C \star \mathbb{F}_q^n = \mathbb{F}_q^n \star C = \mathbb{F}_q^n. \tag{3}$$

В соответствии с [14] введём определение внешней (прямой) и внутренней суммы двух кодов. Для этого понадобятся понятия проекции вектора и проекции пространства. Под проекцией вектора $\mathbf{x} = (x_1, \ldots, x_n)$ на множество $\tau \subseteq \underline{n}$ будем понимать n-мерный вектор $\mathbf{y} = \Pi_\tau(\mathbf{x})$, такой, что $y_i = x_i$ для $i \in \tau$, и $y_i = 0$, если $i \notin \tau$. Проекцию кода C на множество номеров τ определим по правилу

$$\Pi_\tau(C) = \{\Pi_\tau(\mathbf{c}) : \mathbf{c} \in C\}. \tag{4}$$

Отметим, что $\mathrm{supp}(\Pi_\tau(\mathbf{x})) \subseteq \tau$. Прямой суммой кодов $C \subseteq \mathbb{F}_q^n$ и $D \subseteq \mathbb{F}_q^m$ назовём код

$$C \oplus D = \{(\mathbf{c}, \mathbf{d}) : \mathbf{c} \in C, \mathbf{d} \in D\} \subseteq \mathbb{F}_q^{n+m}. \tag{5}$$

Порождающая матрица $G_{C\oplus D}$ кода $C \oplus D$ может быть представлена в блочно-диагональном виде:

$$G_{C\oplus D} = \operatorname{diag}(G_C, G_D) = \begin{pmatrix} G_C & 0 \\ 0 & G_D \end{pmatrix}.$$

Пусть $\tau = \{1, \ldots, n\}$, $\nu = \{n+1, \ldots, n+m\}$. Коду C сопоставим подкод $\tilde{C} = \Pi_\tau(C \oplus D)$ кода $C \oplus D$, а коду D — подкод $\tilde{D} = \Pi_\nu(C \oplus D)$. Тогда

$$C \oplus D = \tilde{C} + \tilde{D},\ \operatorname{supp}(\tilde{C}) \cap \operatorname{supp}(\tilde{D}) = \varnothing,\ \dim(\tilde{C}) = \dim(C),\ \dim(\tilde{D}) = \dim(D), \quad (6)$$

где

$$\tilde{C} + \tilde{D} = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in \tilde{C}, \mathbf{b} \in \tilde{D}\} \subseteq \mathbb{F}_q^{n+m} \quad (7)$$

— внутренняя сумма кодов. Таким образом, прямая сумма $C \oplus D$ кодов C и D представима в виде внутренней суммы подкодов $\tilde{C} \subseteq C \oplus D$ и $\tilde{D} \subseteq C \oplus D$ с непересекающимися носителями. При этом заметим, что могут найтись два подкода $\tilde{C}' \subseteq C \oplus D$ и $\tilde{D}' \subseteq C \oplus D$ с пересекающимися носителями, такие, что $\tilde{C}' + \tilde{D}' = C \oplus D$.

По аналогии с (5) и (7) определяется внешняя и внутренняя сумма u кодов, $u \in \mathbb{N}$.

Лемма 3 [13]. Для кодов C_1, C_2 и C_3 из $\mathbb{F}_q^n$ выполняются следующие равенства:

$$(C_1 + C_2) \star C_3 = C_1 \star C_3 + C_2 \star C_3. \quad (8)$$

Из леммы 3 и представления (6) вытекает, что

$$(C \oplus D) \star E = (\tilde{C} + \tilde{D}) \star E = \tilde{C} \star E + \tilde{D} \star E = \tilde{C} \star \Pi_{\operatorname{supp}(\tilde{C})}(E) + \tilde{D} \star \Pi_{\operatorname{supp}(\tilde{D})}(E)$$

для любых кодов $C \subseteq \mathbb{F}_q^n$, $D \subseteq \mathbb{F}_q^m$ и $E \subseteq \mathbb{F}_q^{n+m}$. Тогда

$$(C \oplus D) \star E = (C \star E_1) \oplus (D \star E_2), \quad (9)$$

где код $E_1 \subseteq \mathbb{F}_q^n$ получается из кода E отбрасыванием последних m координат в кодовых словах из E, а код $E_2 \subseteq \mathbb{F}_q^m$ — отбрасыванием первых n координат. Из (9), в частности, вытекает, что

$$(C \oplus D)^2 = C^2 \oplus D^2.$$

В общем случае

$$(C_1 \oplus \ldots \oplus C_n)^s = C_1^s \oplus \ldots \oplus C_n^s.$$

Лемма 4. Для любых $G_{C_1} = (\mathbf{g}_i^1)_{i=1}^{k_1} \in \mathcal{G}(C_1)$ и $G_{C_2} = (\mathbf{g}_i^2)_{i=2}^{k_2} \in \mathcal{G}(C_2)$ выполняется равенство

$$C_1 \star C_2 = \mathcal{L}\left(G_{C_1} \star G_{C_2}\right).$$

Доказательство. По определению кода $C_1 \star C_2$ произвольный вектор $\mathbf{c} \in C_1 \star C_2$ представляет собой некоторую линейную комбинацию вида

$$\mathbf{c} = \sum_{i=1}^{l_\mathbf{c}} \gamma_i(\mathbf{a}_i \star \mathbf{b}_i),\ \gamma_i \neq 0,\ \mathbf{a}_i \in C_1,\ \mathbf{b}_i \in C_2,$$

где $l_\mathbf{c}$ для каждого $\mathbf{c}$ в общем случае своё. Так как $\mathbf{a}_i = \sum\limits_{l=1}^{k_A} \alpha_l \mathbf{g}_l^1$, $\mathbf{b}_i = \sum\limits_{r=1}^{k_B} \beta_r \mathbf{g}_r^2$, то из п. 3 леммы 1 получаем

$$\mathbf{c} = \sum_{i=1}^{l_\mathbf{c}} \gamma_i(\mathbf{a}_i \star \mathbf{b}_i) = \sum_{i=1}^{l_\mathbf{c}} \gamma_i \left(\sum_{l=1}^{k_A} \alpha_l \mathbf{g}_l^1 \star \sum_{r=1}^{k_B} \beta_r \mathbf{g}_r^2\right) = \sum_{i=1}^{l_\mathbf{c}} \gamma_i \left(\sum_{l=1}^{k_A} \sum_{r=1}^{k_B} \alpha_l \beta_r (\mathbf{g}_l^1 \star \mathbf{g}_r^2)\right).$$

Вектор $\sum\limits_{l=1}^{k_A}\sum\limits_{r=1}^{k_B}\alpha_l\beta_r(\mathbf{g}_l^1\star\mathbf{g}_r^2)$ представляет собой линейную комбинацию строк матрицы $G_{C_1}\star G_{C_2}$, поэтому вектор $\mathbf{c}$ также является линейной комбинацией строк этой матрицы. Следовательно, $C_1\star C_2\subseteq\mathcal{L}\left(G_{C_1}\star G_{C_2}\right)$. Обратное вложение очевидно. ■

Пусть C_i — $[n_i,k_i,d_i]_q$-код, G_{C_i} — его порождающая матрица, $i=1,2$. Тензорным произведением кодов C_1 и C_2 называется $[n_1n_2,k_1k_2,d_1d_2]_q$-код, обозначаемый $C_1\otimes C_2$, порождающая матрица которого имеет вид $G_{C_1\otimes C_2}=G_{C_1}\otimes G_{C_2}$. Дуальным к тензорному произведению кодов является код

$$(C_1\otimes C_2)^{\perp}=(\mathbb{F}_q^{n_1}\otimes C_2^{\perp})+(C_1^{\perp}\otimes\mathbb{F}_q^{n_2}). \tag{10}$$

По определению тензорного произведения получаем

$$C_1\otimes C_2\subseteq\mathbb{F}_q^{n_1}\otimes C_2=\underbrace{C_2\oplus\ldots\oplus C_2}_{n_1}. \tag{11}$$

Лемма 5 [15]. Пусть C — $[n,k]_q$-код, тогда

$$\dim(C^2)\leqslant\min\left\{n,k(k+1)/2\right\}. \tag{12}$$

В [15] для случайного линейного кода C получены теоретические оценки вероятности выполнения равенства в (12).

Исследуем свойства произведения Шура — Адамара для кода $C_1\otimes C_2$.

Лемма 6. Пусть C_i — $[n_i,k_i,d_i]_q$-код с порождающей матрицей G_{C_i}, $i=1,2$. Тогда

$$\dim((C_1\otimes C_2)^2)\leqslant\min\left\{n_2\dim(C_1^2),\ n_1\dim(C_2^2),\ k_1k_2(k_1k_2+1)/2\right\}. \tag{13}$$

Доказательство. Неравенство $\dim((C_1\otimes C_2)^2)\leqslant n_1\dim(C_2^2)\leqslant n_1n_2$ вытекает из (11) и того, что $\dim(C_2^2)\leqslant n_2$. В [16] показано, что для любых матриц A и B всегда найдутся две такие матрицы перестановок P_l и P_r подходящих размеров, что

$$A\otimes B=P_l(B\otimes A)P_r. \tag{14}$$

Поэтому код $C_1\otimes C_2$ перестановочно эквивалентен некоторому подкоду кода $\mathbb{F}_q^{n_2}\otimes C_1$ и $\dim((C_1\otimes C_2)^2)\leqslant n_2\dim(C_1^2)$. Тогда (13) следует из (12). ■

Важной для дальнейшего является

Теорема 1. Пусть $C_1,D_1\subseteq\mathbb{F}_q^{n_1}$, $C_2,D_2\subseteq\mathbb{F}_q^{n_2}$. Тогда

$$(C_1\otimes C_2)\star(D_1\otimes D_2)=(C_1\star D_1)\otimes(C_2\star D_2).$$

Доказательство. Как следует из леммы 4, для доказательства теоремы 1 достаточно показать, что для любых порождающих матриц G_{C_1}, G_{C_2}, G_{D_1}, G_{D_2} выполняется равенство

$$\mathcal{L}\left((G_{C_1}\otimes G_{C_2})\star(G_{D_1}\otimes G_{D_2})\right)=\mathcal{L}\left((G_{C_1}\star G_{D_1})\otimes(G_{C_2}\star G_{D_2})\right).$$

Пусть $\mathbf{c}_i^1$, $\mathbf{c}_l^2$, $\mathbf{d}_j^1$, $\mathbf{d}_m^2$ — произвольные строки матриц G_{C_1}, G_{C_2}, G_{D_1} и G_{D_2} соответственно. Тогда из п. 5 леммы 1 получаем

$$(\mathbf{c}_i^1\otimes\mathbf{c}_l^2)\star(\mathbf{d}_j^1\otimes\mathbf{d}_m^2)=(\mathbf{c}_i^1\star\mathbf{d}_j^1)\otimes(\mathbf{c}_l^2\star\mathbf{d}_m^2). \tag{15}$$

Заметим, что в левой части равенства (15) стоит представление некоторой строки из $(G_{C_1} \otimes G_{C_2}) \star (G_{D_1} \otimes G_{D_2})$, а в правой — некоторой строки из $(G_{C_1} \star G_{D_1}) \otimes (G_{C_2} \star G_{D_2})$. Таким образом, каждая строка матрицы $(G_{C_1} \otimes G_{C_2}) \star (G_{D_1} \otimes G_{D_2})$ является строкой матрицы $(G_{C_1} \star G_{D_1}) \otimes (G_{C_2} \star G_{D_2})$, и наоборот. ■

Из (3) и теоремы 1 вытекает, что если $C_1 = \mathbb{F}_q^{n_1}$ и код D_1 не имеет фиктивных координат (или $D_1 = \mathbb{F}_q^{n_1}$ и код C_1 не имеет фиктивных координат), то

$$(C_1 \otimes D_1) \star (C_2 \otimes D_2) = \mathbb{F}_q^{n_1} \otimes C_2 \star D_2.$$

Теорема 2. Пусть $\tau_i \subseteq \underline{n_i}$ — множество фиктивных координат $[n_i, k_i]_q$-кода $C_i^\perp$, $i = 1, 2$. Тогда

1) $(C_1 \otimes C_2)^2 = C_1^2 \otimes C_2^2$;
2) $((C_1 \otimes C_2)^\perp)^2 = \mathbb{F}_q^{n_1} \otimes (C_2^\perp)^2 + \mathbb{F}_q^{n_1}(\underline{n_1} \setminus \tau_1) \otimes \mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2) + (C_1^\perp)^2 \otimes \mathbb{F}_q^{n_2}$.

Доказательство. Утверждение 1 вытекает непосредственно из теоремы 1 при $D_1 = C_1$ и $D_2 = C_2$. Докажем утверждение 2. Из (10) и (8) получаем

$$\begin{aligned}((C_1 \otimes C_2)^\perp)^2 &= (\mathbb{F}_q^{n_1} \otimes C_2^\perp + C_1^\perp \otimes \mathbb{F}_q^{n_2})^2 = \\ &= (\mathbb{F}_q^{n_1} \otimes C_2^\perp)^2 + (\mathbb{F}_q^{n_1} \otimes C_2^\perp) \star (C_1^\perp \otimes \mathbb{F}_q^{n_2}) + (C_1^\perp \otimes \mathbb{F}_q^{n_2})^2.\end{aligned}$$

Из теоремы 1 следует, что $(\mathbb{F}_q^{n_1} \otimes C_2^\perp)^2 = \mathbb{F}_q^{n_1} \otimes (C_2^\perp)^2$, $(C_1^\perp \otimes \mathbb{F}_q^{n_2})^2 = (C_1^\perp)^2 \otimes \mathbb{F}_q^{n_2}$, а по лемме 2 имеем

$$(\mathbb{F}_q^{n_1} \star C_1^\perp) \otimes (C_2^\perp \star \mathbb{F}_q^{n_2}) = \mathbb{F}_q^{n_1}(\underline{n_1} \setminus \tau_1) \otimes \mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2).$$

Собрав вместе представления слагаемых, получаем утверждение 2 теоремы. ■

Из п. 1 теоремы 2 для натурального $s \geqslant 1$ получаем равенство

$$(C_1 \otimes C_2)^s = C_1^s \otimes C_2^s. \tag{16}$$

Коды C и D из $\mathbb{F}_q^n$ будем называть перестановочно эквивалентными и писать $C \sim D$, если найдётся такая перестановка $\sigma \in \mathcal{S}_n$, что $\sigma(C) = D$. Подгруппа $\mathcal{S}_n$ таких перестановок σ, что $\sigma(C) = C$, называется группой перестановочных автоморфизмов и обозначается здесь как $\mathrm{PAut}(C)$.

Следствие 1. Пусть $\tau_i \subseteq \underline{n_i}$ — множество фиктивных координат $[n_i, k_i]_q$-кода $C_i^\perp$, $i = 1, 2, 3$. Имеют место следующие свойства:

1) если $\tau_1 = \varnothing$, то $((C_1 \otimes C_2)^\perp)^2 \sim (\mathbb{F}_q^{n_2}(\tau_2) \otimes ((C_1^\perp)^2)^\perp)^\perp$;
2) если $\tau_2 = \varnothing$, то $((C_1 \otimes C_2)^\perp)^2 = (\mathbb{F}_q^{n_1}(\tau_1) \otimes ((C_2^\perp)^2)^\perp)^\perp$;
3) если $\tau_2 = \varnothing$, $n_1 = n_3$ и $\tau_1 = \tau_3$, то $((C_1 \otimes C_2)^\perp)^2 = ((C_3 \otimes C_2)^\perp)^2$;
4) если $\tau_1 = \tau_2 = \varnothing$, то $((C_1 \otimes C_2)^\perp)^2 = \mathbb{F}_q^{n_1 n_2}$.

Доказательство.

Докажем свойство 1. Из утверждения 2 теоремы 2 и условия $\tau_1 = \varnothing$ вытекает цепочка равенств

$$\begin{gathered}((C_1 \otimes C_2)^\perp)^2 = \mathbb{F}_q^{n_1} \otimes (C_2^\perp)^2 + \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2) + (C_1^\perp)^2 \otimes \mathbb{F}_q^{n_2} = \\ = \mathbb{F}_q^{n_1} \otimes ((C_2^\perp)^2 + \mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2)) + (C_1^\perp)^2 \otimes \mathbb{F}_q^{n_2} = \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2) + (C_1^\perp)^2 \otimes \mathbb{F}_q^{n_2}.\end{gathered}$$

Отсюда, последовательно применяя (10) и (14), получаем

$$((C_1 \otimes C_2)^\perp)^2 = (((C_1^\perp)^2)^\perp \otimes (\mathbb{F}_q^{n_2}(\underline{n_2} \setminus \tau_2))^\perp)^\perp \sim (\mathbb{F}_q^{n_2}(\tau_2) \otimes ((C_1^\perp)^2)^\perp)^\perp.$$

Свойство 2 доказывается по аналогии со свойством 1 с естественными упрощениями; свойство 3 вытекает из свойства 2.

Докажем свойство 4. Из п. 2 теоремы 2 и условия 4 получаем

$$((C_1 \otimes C_2)^{\perp})^2 = \mathbb{F}_q^{n_1} \otimes (C_2^{\perp})^2 + \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2} + (C_1^{\perp})^2 \otimes \mathbb{F}_q^{n_2} = \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2} = \mathbb{F}_q^{n_1 n_2}.$$

Следствие 1 доказано. ■

Рассмотрим некоторые примеры.

Пример 1. Пусть $\mathrm{GRS}_{k,n}$ — обобщённый $[n,k]_q$-код Рида — Соломона [17], $s \in \mathbb{N}$. Известно [4], что $\mathrm{GRS}_{k,n}^2 = \mathrm{GRS}_{\min\{2k-1,n\},n}$. Отсюда следует

$$\mathrm{GRS}_{k,n}^s = \mathrm{GRS}_{\min\{s(k-1)+1,n\},n}. \tag{17}$$

Из (16) следует, что s-я степень тензорного произведения обобщённых кодов Рида — Соломона есть тензорное произведение обобщённых кодов Рида — Соломона. Пусть $C_i = \mathrm{GRS}_{k_i,n_i}$, $i = 1,2$. Если существует такое s, что

$$\left\lceil \frac{n_1 - 1}{k_1 - 1} \right\rceil \leqslant s < \left\lfloor \frac{n_2 - 1}{k_2 - 1} \right\rfloor, \tag{18}$$

то из (16), (17) и $\mathrm{GRS}_{s(k_1-1)+1,n_1} = \mathrm{GRS}_{n_1,n_1} = \mathbb{F}_q^{n_1}$ получаем

$$(\mathrm{GRS}_{k_1,n_1} \otimes \mathrm{GRS}_{k_2,n_2})^s = (\mathrm{GRS}_{k_1,n_1})^s \otimes (\mathrm{GRS}_{k_2,n_2})^s = \mathbb{F}_q^{n_1} \otimes \mathrm{GRS}_{s(k_2-1)+1,n_2} \neq \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2}.$$

Другими словами, s-я степень тензорного произведения обобщённых кодов Рида — Соломона, при выполнении неравенств (18), равна прямой сумме нетривиальных обобщённых кодов Рида — Соломона. Так как обобщённый код Рида — Соломона не имеет фиктивных координат, из п. 4 следствия 1 получаем, что $((\mathrm{GRS}_{k_1,n_1} \otimes \mathrm{GRS}_{k_2,n_2})^{\perp})^s = \mathbb{F}_q^{n_1 n_2}$ для всех $s \geqslant 2$.

Пример 2. Пусть $\mathrm{RM}(r,m)$ — бинарный код Рида — Маллера порядка r и длины 2^m. Из результатов работы [5] следует, что $(\mathrm{RM}(r,m))^s = \mathrm{RM}(\min\{m, sr\}, m)$. Тогда из (16) получаем, что s-я степень тензорного произведения бинарных кодов Рида — Маллера есть тензорное произведение бинарных кодов Рида — Маллера, но большего порядка. Пусть $C_i = \mathrm{RM}(r_i, m_i)$, $i = 1,2$. Если существует такое $s \in \mathbb{N}$, что

$$\left\lceil \frac{2^{m_1}}{r_1} \right\rceil \leqslant s < \left\lfloor \frac{2^{m_2}}{r_2} \right\rfloor,$$

то из равенства $\mathrm{RM}(m_1, m_1) = \mathbb{F}_2^{2^{m_1}}$ вытекает, что s-я степень тензорного произведения бинарных кодов Рида — Маллера есть прямая сумма нетривиальных кодов Рида — Маллера большего порядка:

$$\begin{aligned}(\mathrm{RM}(r_1,m_1) \otimes \mathrm{RM}(r_2,m_2))^s &= (\mathrm{RM}(r_1,m_1))^s \otimes (\mathrm{RM}(r_2,m_2))^s = \\ &= \mathbb{F}_2^{2^{m_1}} \otimes \mathrm{RM}(sr_2, m_2) \neq \mathbb{F}_2^{2^{m_1}} \otimes \mathbb{F}_2^{2^{m_2}}.\end{aligned}$$

Учитывая, что бинарный код Рида — Маллера не имеет фиктивных координат, из п. 4 следствия 1 получаем, что $((\mathrm{RM}(r_1,m_1) \otimes \mathrm{RM}(r_2,m_2))^{\perp})^s = \mathbb{F}_2^{2^{m_1+m_2}}$ для всех $s \geqslant 2$.

2. Группа перестановочных автоморфизмов прямой суммы неразложимых кодов

2.1. Неразложимые коды

Говорят, что код C *разложимый*, если он перестановочно эквивалентен прямой сумме двух или более нетривиальных кодов [18, 19]. В противном случае код называется неразложимым. Под *полным* разложением кода понимается представление перестановочно эквивалентного ему кода в виде прямой суммы неразложимых кодов. Разложимый код в этом случае перестановочно эквивалентен коду с порождающей матрицей, представимой в блочно-диагональном виде с двумя или более блоками на главной диагонали. В [6] построен эффективный алгоритм, позволяющий определить, является ли произвольный линейный код C разложимым, и найти для перестановочно эквивалентного ему кода порождающую матрицу в блочно-диагональном виде. Из (9) вытекает

Лемма 7. Пусть C — n-мерный код. Тогда

1) если C — разложимый, то для любого натурального $s \geqslant 2$ код C^s разложимый;
2) если C — разложимый, то для любого $D \subseteq \mathbb{F}_q^n$ код $C \star D$ разложимый;
3) если C^s — неразложимый, то и C^i — неразложимый код для всех $i = 1, \ldots, s-1$.

С использованием леммы 7 доказывается

Теорема 3 [11, лемма 5]. Бинарный код Рида — Маллера $\mathrm{RM}(r, m)$ для $r = 0, \ldots, m-1$ является неразложимым.

2.2. Группа перестановочных автоморфизмов

Д. Слепианом в работе [18] доказана следующая

Теорема 4 [18, теорема 2]. Для каждого $[n, k]_q$-кода X существует m неразложимых кодов $C_1, \ldots, C_m$, таких, что код X перестановочно эквивалентен прямой сумме $C = C_1 \oplus \ldots \oplus C_m$. Это разложение единственно в следующем смысле: если $X \sim C' = C'_1 \oplus \ldots \oplus C'_{m'}$, где $C'_1, \ldots, C'_{m'}$ — неразложимые коды, то $m = m'$ и $C_1 \sim C'_{i_1}, \ldots, C_m \sim C'_{i_m}$, где $i_1, \ldots, i_m$ — натуральные числа от 1 до m в некотором порядке.

В [14] построен алгоритм разложения произвольного линейного кода в прямую сумму неразложимых подкодов. Однако, кроме разложения произвольного кода в прямую сумму кодов, интерес представляет описание группы перестановочных автоморфизмов прямой суммы неразложимых кодов.

Пусть $n \in \mathbb{N}$. Для $a, b \in \underline{n}$, $a < b$, обозначим $\mathcal{S}_n[a; b]$ подгруппу симметрической группы $\mathcal{S}_n$, такую, что всякая перестановка σ из $\mathcal{S}_n[a; b]$ переставляет элементы из множества $\{a, \ldots, b\} \subseteq \underline{n}$, а остальные элементы из $\underline{n}$ оставляет на месте: $\sigma(i) \in \{a, \ldots, b\}$, если $i \in \{a, \ldots, b\}$, и $\sigma(i) = i$, если $i \notin \{a, \ldots, b\}$.

Пусть $i \in \underline{u}$, C_i — $[n_i, k_i]_q$-код с группой перестановочных автоморфизмов $\mathrm{PAut}(C_i)$, $k = \sum\limits_{i=1}^{u} k_i$, $n = \sum\limits_{i=1}^{u} n_i$, $\mathbf{n}_i = \sum\limits_{j=1}^{i} n_j$, $\mathbf{n}_0 = 0$. Рассмотрим $[n, k]_q$-код $C = C_1 \oplus \ldots \oplus C_u$. Отметим, что для произвольного вектора

$$\mathbf{x} = (x_1, \ldots, x_{\mathbf{n}_1}, x_{\mathbf{n}_1+1}, \ldots, x_{\mathbf{n}_2}, \ldots, x_{\mathbf{n}_{u-1}+1}, \ldots, x_{\mathbf{n}_u}) \in C$$

выполняется условие $\mathbf{c}_i = (x_{\mathbf{n}_{i-1}+1}, \ldots, x_{\mathbf{n}_i}) \in C_i$ (см. (5)). Пусть

$$\tilde{C}_i = \Pi_{\{\mathbf{n}_{i-1}+1, \ldots, \mathbf{n}_i\}}(C_1 \oplus \ldots \oplus C_u)$$

(определение проекции $\Pi_{\{\mathbf{n}_{i-1}+1, \ldots, \mathbf{n}_i\}}(C_1 \oplus \ldots \oplus C_u)$ см. в (4)),

$$\mathrm{PAut}_{n, [\mathbf{n}_{i-1}+1; \mathbf{n}_i]}(\tilde{C}_i) = \mathrm{PAut}(\tilde{C}_i) \cap \mathcal{S}_n[\mathbf{n}_{i-1} + 1; \mathbf{n}_i].$$

Отсюда вытекает, что группы $\mathrm{PAut}(C_i)$ и $\mathrm{PAut}_{n,[\mathbf{n}_{i-1}+1;\mathbf{n}_i]}(\tilde{C}_i)$ естественно изоморфны; соответствующий изоморфизм обозначим так:

$$\xi_{n,C_i,\mathbf{n}_{i-1}+1,\mathbf{n}_i} : \mathrm{PAut}(C_i) \to \mathrm{PAut}_{n,[\mathbf{n}_{i-1}+1;\mathbf{n}_i]}(\tilde{C}_i).$$

Отметим, что $\mathrm{PAut}(C_i) = \mathcal{S}_{n_i}$ в случае $C_i = \mathbb{F}_q^{n_i}$, поэтому перестановки из группы $\xi_{n,\mathbb{F}_q^{n_i},\mathbf{n}_{i-1}+1,\mathbf{n}_i}(\mathcal{S}_{n_i})$ переставляют произвольным образом координаты с номерами из множества $\{\mathbf{n}_{i-1}+1,\ldots,\mathbf{n}_i\}$, а другие оставляют неподвижными. Нетрудно проверить, что произведение подгрупп

$$\mathrm{PAut}_{n,[\mathbf{n}_0+1;\mathbf{n}_1]}(\tilde{C}_1)\cdot\ldots\cdot\mathrm{PAut}_{n,[\mathbf{n}_{u-1}+1;\mathbf{n}_u]}(\tilde{C}_u)$$

не зависит от порядка следования и является подгруппой группы $\mathcal{S}_n$.

Лемма 8. Пусть C_i — неразложимый $[n_i,k_i]_q$-код без фиктивных координат, $i = 1,2$, $C_1 \not\sim C_2$. Тогда

$$\mathrm{PAut}(C_1\oplus C_2) = \mathrm{PAut}_{n_1+n_2,[\mathbf{n}_0+1;\mathbf{n}_1]}(\tilde{C}_1)\cdot\mathrm{PAut}_{n_1+n_2,[\mathbf{n}_1+1;\mathbf{n}_2]}(\tilde{C}_2).$$

Доказательство. Очевидно вложение

$$\mathrm{PAut}_{n_1+n_2,[\mathbf{n}_0+1;\mathbf{n}_1]}(\tilde{C}_1)\cdot\mathrm{PAut}_{n_1+n_2,[\mathbf{n}_1+1;\mathbf{n}_2]}(\tilde{C}_2) \subseteq \mathrm{PAut}(C_1\oplus C_2).$$

Докажем равенство. Предположим, что существует такая перестановка π в группе $\mathrm{PAut}(C_1\oplus C_2)$, что

$$\pi \notin \mathrm{PAut}_{n_1+n_2,[\mathbf{n}_0+1;\mathbf{n}_1]}(\tilde{C}_1)\cdot\mathrm{PAut}_{n_1+n_2,[\mathbf{n}_1+1;\mathbf{n}_2]}(\tilde{C}_2). \tag{19}$$

Пусть $\mathbf{0}_i$ — нулевой вектор длины n_i, $i = 1,2$. Без потери общности, предположим, что $n_1 \geqslant n_2$. Из определения $\mathrm{PAut}(C_1\oplus C_2)$ вытекает, что

$$\Pi_{\{1,\ldots,n_1\}}(\pi(C_1\oplus C_2)) = \Pi_{\{1,\ldots,n_1\}}(C_1\oplus C_2) = C_1\oplus\{\mathbf{0}_2\}. \tag{20}$$

Рассмотрим множество номеров координат $\tau \subseteq \underline{n_1}$ вида

$$\tau = \{j \in \underline{n_1} : \pi^{-1}(j) \in \underline{n_1}\}$$

и его дополнение $\overline{\tau} = \underline{n_1}\setminus\tau$ до множества $\underline{n_1}$. По предположению, выполняется (19), поэтому из условия $n_1 \geqslant n_2$ вытекает

$$0 < |\tau|, |\overline{\tau}| < n_1.$$

Так как $\pi \in \mathrm{PAut}(C_1\oplus C_2)$, из определения τ и $\overline{\tau}$ получаем

$$\pi(C_1\oplus\{\mathbf{0}_2\}) \subseteq C_1\oplus C_2,\ \pi(\{\mathbf{0}_1\}\oplus C_2) \subseteq C_1\oplus C_2,$$
$$\Pi_\tau(\pi(C_1\oplus\{\mathbf{0}_2\})) \subseteq C_1\oplus\{\mathbf{0}_2\},\ \Pi_{\overline{\tau}}(\pi(\{\mathbf{0}_1\}\oplus C_2)) \subseteq C_1\oplus\{\mathbf{0}_2\}.$$

Тогда

$$\Pi_\tau(C_1\oplus C_2) = \Pi_\tau(\pi(C_1\oplus C_2)) = \Pi_\tau(\pi(C_1\oplus\{\mathbf{0}_2\})) \subseteq C_1\oplus\{\mathbf{0}_2\}; \tag{21}$$
$$\Pi_{\overline{\tau}}(C_1\oplus C_2) = \Pi_{\overline{\tau}}(\pi(C_1\oplus C_2)) = \Pi_{\overline{\tau}}(\pi(\{\mathbf{0}_1\}\oplus C_2)) \subseteq C_1\oplus\{\mathbf{0}_2\}. \tag{22}$$

Из (21) и (22) следует

$$\Pi_\tau(\pi(C_1 \oplus C_2)) + \Pi_{\overline{\tau}}(\pi(C_1 \oplus C_2)) = \Pi_\tau(C_1 \oplus C_2) + \Pi_{\overline{\tau}}(C_1 \oplus C_2) \subseteq C_1 \oplus \{\mathbf{0}_2\}. \quad (23)$$

Так как для любого линейного кода D длины n и любого множества $\tau \subseteq \underline{n}$ выполняется неравенство

$$\dim(\Pi_\tau(D)) + \dim(\Pi_{\overline{\tau}}(D)) \geqslant \dim(D),$$

то $\dim(\Pi_\tau(C_1 \oplus C_2)) + \dim(\Pi_{\overline{\tau}}(C_1 \oplus C_2)) \geqslant \dim(C_1)$, откуда с учётом (23) имеем

$$\Pi_\tau(C_1 \oplus C_2) + \Pi_{\overline{\tau}}(C_1 \oplus C_2) = C_1 \oplus \{\mathbf{0}_2\}. \quad (24)$$

Так как коды C_1 и C_2 не содержат фиктивных координат, то $\dim(\Pi_\tau(C_1 \oplus C_2)) > 0$ и $\dim(\Pi_{\overline{\tau}}(C_1 \oplus C_2)) > 0$. Отсюда и из (20) получам, что $\dim(\Pi_\tau(C_1 \oplus C_2)) < k_1$ и $\dim(\Pi_{\overline{\tau}}(C_1 \oplus C_2)) < k_1$. Тогда (с учётом (24)) код C_1 изоморфен внешней прямой сумме двух нетривиальных кодов, так как носители кодов $\Pi_\tau(C_1 \oplus C_2)$ и $\Pi_{\overline{\tau}}(C_1 \oplus C_2)$ не пересекаются. Однако это противоречит неразложимости кода C_1. ■

Из леммы 8 вытекает

Лемма 9. Пусть $u \in \mathbb{N}$, C_i — неразложимый $[n_i, k_i]_q$-код C_1, $i = 1, \ldots, u$, $C_l \not\sim C_j$ для всех $l \neq j$. Тогда

$$\mathrm{PAut}(C_1 \oplus \ldots \oplus C_u) = \mathrm{PAut}_{n,[\mathbf{n}_0+1;\mathbf{n}_1]}(\tilde{C}_1) \cdot \ldots \cdot \mathrm{PAut}_{n,[\mathbf{n}_{u-1}+1;\mathbf{n}_u]}(\tilde{C}_u),$$

где $n = \sum\limits_{i=1}^{u} n_i$.

Рассмотрим группу $\mathcal{P}_n$ $(n \times n)$-матриц перестановок и естественный изоморфизм $\alpha_n : \mathcal{S}_n \to \mathcal{P}_n$. Для натуральных n и m в группе $\mathcal{P}_{nm}$ рассмотрим подгруппу

$$\mathcal{P}_{n,m} = \{B \otimes I_n : B \in \mathcal{P}_m\},$$

где I_n — единичная $(n \times n)$-матрица. Пусть $\mathcal{S}_{n,m} = \alpha_{nm}^{-1}(\mathcal{P}_{n,m})$. Отметим, что группа $\mathcal{S}_{n,m}$ изоморфна группе $\mathcal{S}_m$, причём изоморфизм $\beta_{n,m} : \mathcal{S}_m \to \mathcal{S}_{n,m}$ можно записать в виде

$$\beta_{n,m}(\gamma) = \alpha_{nm}^{-1}(\alpha_n(\gamma) \otimes I_n), \gamma \in \mathcal{S}_m.$$

Лемма 10. Пусть $C_i = \sigma_i(C)$ — $[n_i, k_i]_q$-код, где C — неразложимый $[n, k]_q$-код без фиктивных координат, $\sigma_i \in \mathcal{S}_n$, $i = 1, 2$. Тогда

$$\mathrm{PAut}(C_1 \oplus C_2) = \left\{ \begin{array}{c|c} (\hat{\sigma}_1 \circ \omega_1 \circ \dot{\sigma}_1) \circ & \hat{\sigma}_i = \xi_{2n,\mathbb{F}_q^n,\mathbf{n}_{i-1}+1,\mathbf{n}_i}(\sigma_i), \\ (\hat{\sigma}_2 \circ \omega_2 \circ \dot{\sigma}_2) \circ & \dot{\sigma}_i = \xi_{2n,\mathbb{F}_q^n,\mathbf{n}_{i-1}+1,\mathbf{n}_i}(\sigma_{\gamma^{-1}(i)}^{-1}), \\ \beta_{n,2}(\gamma) & \omega_i \in \mathrm{PAut}_{2n,[\mathbf{n}_{i-1}+1;\mathbf{n}_i]}(\tilde{C}), \\ & i = 1, 2,\ \gamma \in \mathcal{S}_2. \end{array} \right\} \quad (25)$$

Доказательство. Сначала заметим, что множество, определённое в правой части равенства (25), является подгруппой группы $\mathcal{S}_{2n}$. Непосредственная проверка показывает, что любая перестановка из правой части (25) не меняет код $C_1 \oplus C_2$, а композиция двух перестановок из этого множества представима в таком же виде. Отсюда следует, что это множество является подгруппой и содержится в $\mathrm{PAut}(C_1 \oplus C_2)$. Для доказательства совпадения этих групп достаточно повторить рассуждения из доказательства леммы 8, положив $n_1 = n_2 = n$ и заменив $\mathrm{PAut}_{n_1+n_2,[\mathbf{n}_0+1,\mathbf{n}_1]}(\tilde{C}_1) \times$ $\times \mathrm{PAut}_{n_1+n_2,[\mathbf{n}_1+1,\mathbf{n}_2]}(\tilde{C}_2)$ на правую часть из равенства (25). ■

Лемма 10 может быть обобщена на случай суммы u одинаковых кодов.

Лемма 11. Пусть $C_i = \sigma_i(C)$ — $[n_i, k_i]_q$-код, где C — неразложимый $[n, k]_q$-код без фиктивных координат, $\sigma_i \in \mathcal{S}_n$, $i \in \underline{u}, u \in \mathbb{N}$. Тогда

$$\mathrm{PAut}(C_1 \oplus \ldots \oplus C_u) = \left\{ \begin{array}{c} (\hat{\sigma}_1 \circ \omega_1 \circ \dot{\sigma}_1)\circ \\ \ldots \\ (\hat{\sigma}_u \circ \omega_u \circ \dot{\sigma}_u)\circ \\ \beta_{n,u}(\gamma) \end{array} : \begin{array}{c} \hat{\sigma}_i = \xi_{un,\mathbb{F}_q^n,\mathbf{n}_{i-1}+1,\mathbf{n}_i}(\sigma_i), \\ \dot{\sigma}_i = \xi_{un,\mathbb{F}_q^n,\mathbf{n}_{i-1}+1,\mathbf{n}_i}(\sigma^{-1}_{\gamma^{-1}(i)}), \\ \omega_i \in \mathrm{PAut}_{un,[\mathbf{n}_{i-1}+1;\mathbf{n}_i]}(\tilde{C}), \\ i \in \underline{u},\ \gamma \in \mathcal{S}_u. \end{array} \right\} \tag{26}$$

Следствие 2. Пусть $u \in \mathbb{N}$, $C_1 = \ldots = C_u = \mathrm{RM}(1, m)$, тогда

$$\mathrm{PAut}(\mathbb{F}_2^u \otimes \mathrm{RM}(1, m)) = \ldots = \mathrm{PAut}(\mathbb{F}_2^u \otimes \mathrm{RM}(m-2, m)) =$$
$$= \mathrm{PAut}_{u2^m,[1,2^m]}(\tilde{C}_1) \cdot \ldots \cdot \mathrm{PAut}_{u2^m,[\mathbf{n}_{u-1}+1;\mathbf{n}_u]}(\tilde{C}_u)\, \mathcal{S}_{2^m,u}.$$

Доказательство. Из (11) получаем, что для $j = 1, \ldots, m-2$

$$\mathbb{F}_2^u \otimes \mathrm{RM}(j, m) = \underbrace{\mathrm{RM}(j, m) \oplus \ldots \oplus \mathrm{RM}(j, m)}_{u}.$$

Как следует из теоремы 3, все бинарные коды Рида — Маллера неразложимые. Поэтому из леммы 11 (см. представление (26) группы перестановочных автоморфизмов перестановочно эквивалентных неразложимых кодов) вытекает, что

$$\mathrm{PAut}(\mathbb{F}_2^u \otimes \mathrm{RM}(1, m)) = \mathrm{PAut}_{u2^m,[1,2^m]}(\tilde{C}_1) \cdot \ldots \cdot \mathrm{PAut}_{u2^m,[\mathbf{n}_{u-1}+1;\mathbf{n}_u]}(\tilde{C}_u)\, \mathcal{S}_{2^m,u}.$$

Известно, что $\mathrm{PAut}(\mathrm{RM}(1, m)) = \ldots = \mathrm{PAut}(\mathrm{RM}(m-2, m))$ [20, с. 400, теорема 24]. Отсюда следует доказываемое утверждение. ■

Теорема 5. Пусть $u \in \mathbb{N}$, $l \in \underline{u}$, $r_l \in \mathbb{N}$, D_l — неразложимый $[N_l, K_l]_q$-код без фиктивных координат, при этом $D_i \not\sim D_j$ для всех $i \neq j$, $\mathbf{r}_l = \sum\limits_{j=1}^{l} r_j$, $\mathbf{r}_0 = 0$, $\mathbf{N}_l = \sum\limits_{j=1}^{l} r_j N_j$, $\mathbf{N}_0 = 0$, $n = \sum\limits_{j=1}^{u} r_j N_j$, $\mathbf{n}_{l,i} = \mathbf{N}_{l-1} + i \cdot N_l$. Рассмотрим набор из $\mathbf{r}_u$ линейных $[n_i, r_i]_q$-кодов C_i, $i \in \underline{\mathbf{r}_u}$, где $C_{\mathbf{r}_{l-1}+1} = \sigma_{l,1}(D_l)$, …, $C_{\mathbf{r}_l} = \sigma_{l,r_l}(D_l)$ для $l \in \underline{u}$, $\sigma_{l,m} \in \mathcal{S}_{n_l}$, $m \in \underline{r_l}$. Тогда код C вида

$$C = \underbrace{C_{\mathbf{r}_0+1} \oplus \ldots \oplus C_{\mathbf{r}_1}}_{r_1} \oplus \underbrace{C_{\mathbf{r}_1+1} \oplus \ldots \oplus C_{\mathbf{r}_2}}_{r_2} \oplus \ldots \oplus \underbrace{C_{\mathbf{r}_{u-1}+1} \oplus \ldots \oplus C_{\mathbf{r}_u}}_{r_u} \tag{27}$$

имеет группу перестановочных автоморфизмов $\mathrm{PAut}(C) = \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_u$, где для $l \in \underline{u}$

$$\mathcal{P}_l = \left\{ \begin{array}{c} (\hat{\sigma}_{l,1} \circ \omega_{l,1} \circ \dot{\sigma}_{l,1})\circ \\ \ldots \\ (\hat{\sigma}_{l,r_l} \circ \omega_{l,r_l} \circ \dot{\sigma}_{l,r_l})\circ \\ \xi_{n,\mathbb{F}_q^{N_l r_l},\mathbf{N}_{l-1}+1,\mathbf{N}_l}(\beta_{N_l,r_l}(\gamma)) \end{array} : \begin{array}{c} \hat{\sigma}_{l,i} = \xi_{n,\mathbb{F}_q^{N_l},\mathbf{n}_{l,i-1}+1,\mathbf{n}_{l,i}}(\sigma_{l,i}), \\ \dot{\sigma}_{l,i} = \xi_{n,\mathbb{F}_q^{N_l},\mathbf{n}_{l,i-1}+1,\mathbf{n}_{l,i}}(\sigma^{-1}_{l,\gamma^{-1}(i)}), \\ \omega_{l,i} \in \mathrm{PAut}_{n,[\mathbf{n}_{l,i-1}+1;\mathbf{n}_{l,i}]}(\tilde{D}_l), \\ i \in \underline{r_l},\ \gamma \in \mathcal{S}_{r_l}. \end{array} \right\}$$

Доказательство. Из (26) вытекает, что группа $\mathrm{PAut}(\oplus_{j=1}^{r_i} C_{\mathbf{r}_{i-1}+j}) \subseteq \mathcal{S}_{r_i N_i}$ изоморфна группе $\mathcal{P}_i \subseteq \mathcal{S}_n$ для $i = 1, \ldots, u$. Поэтому $\mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_u \subseteq \mathrm{PAut}(C)$. Предположим, что существует перестановка σ из $\mathrm{PAut}(C) \setminus \{\mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_u\}$. Тогда такая перестановка в представлении (27) для $i \neq j$ меняет координаты между двумя слагаемыми-суммами

$$\underbrace{C_{\mathbf{r}_{i-1}+1} \oplus \ldots \oplus C_{\mathbf{r}_i}}_{r_i},\ \underbrace{C_{\mathbf{r}_{j-1}+1} \oplus \ldots \oplus C_{\mathbf{r}_j}}_{r_j}.$$

Но в силу леммы 9 таких перестановок не существует. ■

Заключение

В работе [12] авторами предложена кодовая криптосистема типа Мак-Элиса $\mathrm{McE}(C_1 \otimes C_2)$ на основе тензорного произведения кодов C_1 и C_2. Проведённый в [12] анализ криптосистемы $\mathrm{McE}(C_1 \otimes C_2)$ позволил сделать вывод о её высокой стойкости к структурным атакам. При этом в [12] получено, что высокая стойкость достигается даже при использовании кодов C_1 и C_2, для которых известны структурные атаки для систем $\mathrm{McE}(C_1)$ и $\mathrm{McE}(C_2)$, например в случае использования двоичных кодов Рида — Маллера.

Результаты [4 – 11] показали, что произведение Шура — Адамара позволяет в ряде случаев построить эффективную структурную атаку для рассмотренных в этих работах криптосистем. В настоящей работе с целью уточнения стойкости к структурным атакам системы $\mathrm{McE}(C_1 \otimes C_2)$ из [12] исследуются свойства произведения Шура — Адамара для тензорного произведения $C_1 \otimes C_2$. Полученные результаты, в частности формула (16) из п. 1, позволяют с помощью произведения Шура — Адамара построить по публичной матрице системы $\mathrm{McE}(C_1 \otimes C_2)$ код, перестановочно эквивалентный прямой сумме кодов. Представляется, что это позволит, например, используя алгоритм из [14], найти такую матрицу перестановки P_π, с помощью которой публичная матрица системы $\mathrm{McE}(C_1 \otimes C_2)$ может быть преобразована к более простому для анализа виду. При этом если группа перестановочных автоморфизмов прямой суммы кодов имеет вид (26), то применение матрицы P_π, полученной по некоторой степени (в смысле произведения Шура — Адамара) публичной матрицы, к матрице публичного ключа будет корректным. Результаты по уточнению стойкости системы $\mathrm{McE}(C_1 \otimes C_2)$ планируется опубликовать отдельно.

Ю. В. Косолапов признателен рецензенту за внимательное прочтение статьи, в особенности за полезные советы по исправлению найденной ошибки в первоначальном варианте доказательства леммы 8 и обобщению полученных результатов.

ЛИТЕРАТУРА

1. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. P. 42–44.
2. *Sendrier N. and Tillich J. P.* Code-Based Cryptography: New Security Solutions against a Quantum Adversary. ERCIM News. ERCIM, 2016.
3. *Alagic G., Alperin-Sheriff J., Apon D., et al.* Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. US Department of Commerce, NIST, 2019.
4. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes // LNCS. 2010. V. 6061. P. 61–72.
5. *Бородин М. А., Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.
6. *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.
7. *Бородин М. А., Чижов И. В.* Классификация произведений Адамара подкодов коразмерности 1 кодов Рида — Маллера // Дискретная математика. 2020. Т. 32. № 1. С. 115–134.
8. *Высоцкая В. В.* Квадрат кода Рида — Маллера и классы эквивалентности секретных ключей криптосистемы Мак-Элиса — Сидельникова // Прикладная дискретная математика. Приложение. 2017. № 10. С. 66–68.

9. *Vysotskaya V. and Chizhov I.* Equivalence classes of McEliece — Sidelnikov-type cryptosystems // Sixteenth Intern. Workshop Algebraic Combinat. Coding Theory. Svetlogorsk (Kaliningrad region), Russia, 2018. P. 121–124.
10. *Давлетшина А.М.* Поиск эквивалентных ключей криптосистемы Мак-Элиса — Сидельникова, построенной на двоичных кодах Рида — Маллера // Прикладная дискретная математика. Приложение. 2019. № 12. С. 98–100.
11. *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.
12. *Deundyak V. M., Kosolapov Y. V., and Lelyuk E. A.* Decoding the tensor product of MLD codes and applications for code cryptosystems // Aut. Control Comp. Sci. 2019. V. 52. No. 7. P. 647–657.
13. *Randriambololona H.* On Products and Powers of Linear Codes under Componentwise Multiplication. arXiv:1312.0022. 2014.
14. *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.
15. *Cascudo I., Cramer R., Mirandola D., and Zemor G.* Squares of random linear codes // IEEE Trans. Inform. Theory. 2015. V. 61. No. 3. P. 1159–1173.
16. *Henderson H. V. and Searle S. R.* The vec-permutation matrix, the vec operator and Kronecker products: A review // Linear and Multilinear Algebra. 1981. V. 9. P. 271–288.
17. *Сидельников В. М.* Теория кодирования. М.: Физматлит, 2008. 324 с.
18. *Slepian D.* Some further theory of group codes // Bell Syst. Tech. J. 1960. V. 39. No. 5. P. 1219–1252.
19. *Assmus E. F.* The category of linear codes // IEEE Trans. Inform. Theory. 1998. V. 44. No. 2. P. 612–629.
20. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 746 с.

REFERENCES

1. *McEliece R. J.* A Public-Key Cryptosystem Based On Algebraic Coding Theory. DSN Progress Report, 1978, pp. 42–44.
2. *Sendrier N. and Tillich J. P.* Code-Based Cryptography: New Security Solutions against a Quantum Adversary. ERCIM News, ERCIM, 2016.
3. *Alagic G., Alperin-Sheriff J., Apon D., et al.* Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. US Department of Commerce, NIST, 2019.
4. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. LNCS, 2010, vol. 6061, pp. 61–72.
5. *Borodin M. A. and Chizhov I. V.* Effective attack on the McEliece cryptosystem based on Reed — Muller codes. Discrete Math. Appl., 2014, vol. 24, no. 5, pp. 273–280.
6. *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.
7. *Borodin M. A. and Chizhov I. V.* Klassifikacija proizvedenij Adamara podkodov korazmernosti 1 kodov Rida — Mallera [Classification of Hadamard products of codimension 1 subcodes of Reed — Muller codes]. Diskret. Matem., 2020, vol. 32, no. 1, pp. 115–134. (in Russian)
8. *Vysotskaya V. V* Kvadrat koda Rida — Mallera i klassy ekvivalentnosti sekretnykh klyuchey kriptosistemy Mak-Elisa — Sidel'nikova [The Reed — Muller code square and equivalence

classes of McEliece — Sidelnikov cryptosystem private keys]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, pp. 66–68. (in Russian)

9. *Vysotskaya V. and Chizhov I.* Equivalence classes of McEliece — Sidelnikov-type cryptosystems. Sixteenth Intern. Workshop Algebraic Combinat. Coding Theory, Svetlogorsk (Kaliningrad region), Russia, 2018, pp. 121–124.
10. *Davletshina A. M.* Poisk ekvivalentnykh klyuchey kriptosistemy Mak-Elisa — Sidel'nikova, postroennoy na dvoichnykh kodakh Rida — Mallera [Search for equivalent keys of the McEliece — Sidelnikov cryptosystem built on the Reed — Muller binary codes]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 98–100. (in Russian)
11. *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.
12. *Deundyak V. M., Kosolapov Y. V., and Lelyuk E. A.* Decoding the tensor product of MLD codes and applications for code cryptosystems. Aut. Control Comp. Sci, 2019, vol. 52, no. 7, pp. 647–657.
13. *Randriambololona H.* On Products and Powers of Linear Codes under Componentwise Multiplication. arXiv:1312.0022, 2014.
14. *Deundyak V. M. and Kosolapov Yu. V.* Analiz stoykosti nekotorykh kodovykh kriptosistem, osnovannyy na razlozhenii kodov v pryamuyu summu [The use of the direct sum decomposition algorithm for analyzing the strength of some McEliece type cryptosystems]. Vestn. JuUrGU. Ser. Matem. Modelirovanie i Programmirovanie, 2019, vol. 12, no. 3, pp. 89–101. (in Russian)
15. *Cascudo I., Cramer R., Mirandola D., and Zemor G.* Squares of random linear codes. IEEE Trans. Inform. Theory, 2015, vol. 61, no. 3, pp. 1159–1173.
16. *Henderson H. V. and Searle S. R.* The vec-permutation matrix, the vec operator and Kronecker products: A review. Linear and Multilinear Algebra, 1981, vol. 9, pp. 271–288.
17. *Sidel'nikov V. M.* Teorija kodirovanija [Coding Theory]. Moscow: Fizmatlit Publ., 2008. 324 p. (in Russian)
18. *Slepian D.* Some further theory of group codes. Bell Syst. Tech. J., 1960, vol. 39, no. 5, pp. 1219–1252.
19. *Assmus E. F.* The category of linear codes. IEEE Trans. Inform. Theory, 1998, vol. 44, no. 2, pp. 612–629.
20. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam; New York, North-Holland Pub. Co., 1977. 762 p.