7. *Ведунова М. В., Геут К. Л., Игнатова А. О.* Преломляющие биекции в тройках Штейнера // Прикладная дискретная математика. Приложение. 2020. № 13. С. 6–8.
8. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
9. *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.
10. *Гайнанов Д. Н., Новокшенов Л. И., Тягунов Л. И.* О графах, порождаемых несовместными системами линейных неравенств // Матем. заметки. 1983. № 33:2. С. 146–150.
11. *Мазуров В. Д., Хачай М. Ю.* Бустинг и полиномиальная аппроксимируемость задачи о минимальном аффинном разделяющем комитете // Тр. ИММ УрО РАН. 2013. Т. 19. № 2. С. 231–236.

УДК 621.391.7 DOI 10.17223/2226308X/14/35

О РАЗЛОЖИМОСТИ ПРОИЗВЕДЕНИЯ ШУРА — АДАМАРА СУММЫ ТЕНЗОРНЫХ ПРОИЗВЕДЕНИЙ КОДОВ РИДА — МАЛЛЕРА

Ю. В. Косолапов, Е. А. Лелюк

В рамках оценки стойкости кодовых криптосистем типа Мак-Элиса рассматривается задача исследования разложимости квадрата кода K, являющегося суммой специального вида двух тензорных произведений кодов Рида — Маллера. В ряде случаев удалось найти условия на параметры кодов-множителей, при которых квадрат кода K раскладывается в прямую сумму кодов Рида — Маллера; найдены также условия, при которых такое разложение невозможно.

Ключевые слова: *криптосистема типа Мак-Элиса, сумма тензорных произведений, произведение Шура — Адамара, разложимость.*

Кодовые криптосистемы типа Мак-Элиса рассматриваются в качестве альтернативы современным асимметричным криптосистемам, так как при выборе подходящего кода являются стойкими к атакам с помощью компьютера на основе квантовой модели вычисления [1]. Оригинальная система Мак-Элиса на кодах Гоппы в настоящее время считается стойкой, но высокая стойкость достигается за счёт ключа большого размера [2]. С целью уменьшения размера ключа предложены криптосистемы типа Мак-Элиса на других кодах. Но для некоторых широко известных кодов, таких, как обобщённые коды Рида — Соломона, двоичные коды Рида — Маллера, системы типа Мак-Элиса оказываются нестойкими и для компьютеров на основе классической модели Тьюринга [3 – 5]. Для усиления стойкости криптосистем в [6] предлагается использовать тензорное произведение кодов Рида — Маллера. В [7] исследуется класс кодов, обобщающий конструкцию тензорного произведения. Коды из этого класса представляют собой сумму нескольких тензорных произведений специального вида. Эти коды эффективно декодируются, поэтому на их основе можно построить криптосистему типа Мак-Элиса. Но для применения криптосистемы необходимо проанализировать её стойкость. При анализе стойкости кодовых криптосистем к атакам на ключ часто исследуются свойства произведения Шура — Адамара кодов, которые лежат в основе этих криптосистем [8].

В настоящей работе ставится задача исследования разложимости квадрата суммы специального вида двух тензорных произведений кодов Рида — Маллера.

Напомним, что линейным $[n,k]_q$-кодом C называется подпространство размерности k пространства $\mathbb{F}_q^n$ над полем Галуа $\mathbb{F}_q$. Для кода C ортогональный к нему код будем обозначать $\overline{C} = \{\mathbf{x} \in \mathbb{F}_q^n : \forall \mathbf{c} \in C\big(\langle \mathbf{x}, \mathbf{c}\rangle = 0\big)\}$, где $\langle \mathbf{x}, \mathbf{c}\rangle$ — скалярное произведение векторов. Для двух кодов $C_1, C_2 \subseteq \mathbb{F}_q^n$ произведение Шура — Адамара $C_1 \star C_2$ определяется как линейная оболочка, натянутая на множество векторов $\{\mathbf{x} \star \mathbf{y} : \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$, где $\mathbf{x} \star \mathbf{y} = (x_1y_1, \ldots, x_ny_n)$. При этом под квадратом кода C понимается код $C^2 = C \star C$ [8]. Под внутренней суммой кодов C_1 и C_2 будем понимать код $C_1 + C_2 = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$, а под внешней (прямой) суммой кодов $C \subseteq \mathbb{F}_q^{n_1}$ и $D \subseteq \mathbb{F}_q^{n_2}$ — код $C \oplus D = \{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C, \mathbf{y} \in D\}$, где $(\mathbf{x}, \mathbf{y})$ — конкатенация векторов $\mathbf{x}$ и $\mathbf{y}$. Тензорное произведение кодов C и D обозначим $C \otimes D$ [9]. В случае $C = \mathbb{F}_q^{n_1}$ получаем следующее равенство:

$$\mathbb{F}_q^{n_1} \otimes D = \underbrace{D \oplus \ldots \oplus D}_{n_1},$$

а в случае $D = \mathbb{F}_q^{n_2}$ код $C \otimes \mathbb{F}_q^{n_2}$ перестановочно эквивалентен коду

$$\mathbb{F}_q^{n_2} \otimes C = \underbrace{C \oplus \ldots \oplus C}_{n_2}.$$

Код называется разложимым, если он перестановочно эквивалентен прямой сумме двух или более кодов ненулевой размерности [10].

Пусть $\mathrm{RM}(r,m)$ — двоичный код Рида — Маллера порядка r и длины 2^m. Рассмотрим коды $C_1 = \mathrm{RM}(r_1^1, m_1)$, $C_2 = \mathrm{RM}(r_2^1, m_1)$, $D_1 = \mathrm{RM}(r_1^2, m_2)$, $D_2 = \mathrm{RM}(r_2^2, m_2)$, такие, что $C_2 \subset C_1$, $D_1 \subset D_2$. Код

$$K = \overline{C}_1 \otimes \overline{D}_1 + \overline{C}_2 \otimes \overline{D}_2 \tag{1}$$

является мажоритарно-декодируемым кодом [7]. Отметим, что $\overline{C}_1 \subset \overline{C}_2$, $\overline{D}_2 \subset \overline{D}_1$. В [11] доказано, что для произвольных кодов $V_1, V_2 \subseteq \mathbb{F}_q^{n_1}$, $W_1, W_2 \subseteq \mathbb{F}_q^{n_2}$ выполняется равенство

$$(V_1 \otimes W_1) \star (V_2 \otimes W_2) = (V_1 \star V_2) \otimes (W_1 \star W_2).$$

Отсюда получаем, что квадрат кода K имеет следующий вид:

$$K^2 = \overline{C}_1^2 \otimes \overline{D}_1^2 + (\overline{C}_1 \star \overline{C}_2) \otimes (\overline{D}_1 \star \overline{D}_2) + \overline{C}_2^2 \otimes \overline{D}_2^2. \tag{2}$$

Теорема 1. Пусть K — код вида (1).
1) Если $m_1 - r_1^1 - 1 \geqslant m_1/2$ и $m_2 - r_1^2 - 1 < m_2/2$, то

$$K^2 = \mathbb{F}_2^{2^{m_1}} \otimes \mathrm{RM}(2(m_2 - r_1^2 - 1), m_2).$$

2) Если $m_1 - r_2^1 - 1 < m_1/2$ и $m_2 - r_2^2 - 1 \geqslant m_2/2$, то

$$K^2 = \mathrm{RM}(2(m_1 - r_2^1 - 1), m_1) \otimes \mathbb{F}_2^{2^{m_2}}.$$

Теорема 2. Пусть K — код вида (1). Если выполняется хотя бы одно из условий:
1) $m_1 - r_1^1 - 1 \geqslant m_1/2$ и $m_2 - r_1^2 - 1 \geqslant m_2/2$,
2) $2m_1 - (r_1^1 + r_2^1) - 2 \geqslant m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 \geqslant m_2$,
3) $m_1 - r_2^1 - 1 \geqslant m_1/2$ и $m_2 - r_2^2 - 1 \geqslant m_2/2$,

то

$$K^2 = \mathbb{F}_2^{2^{m_1+m_2}}.$$

Теорема 3. Пусть K — код вида (1), $m_1 - r_2^1 - 1 \geqslant m_1/2$, $m_2 - r_1^2 - 1 \geqslant m_2/2$, $m_1 - r_1^1 - 1 < m_1/2$, $m_2 - r_2^2 - 1 < m_2/2$.

1) Если $2m_1 - (r_1^1 + r_2^1) - 2 \geqslant m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 < m_2$, то

$$K^2 = \overline{\mathrm{RM}(2r_1^1 - m_1 + 1, m_1) \otimes \mathrm{RM}(r_1^2 + r_2^2 - m_2 + 1, m_2)}.$$

2) Если $2m_1 - (r_1^1 + r_2^1) - 2 < m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 \geqslant m_2$, то

$$K^2 = \overline{\mathrm{RM}(r_1^1 + r_2^1 - m_1 + 1, m_1) \otimes \mathrm{RM}(2r_2^2 - m_2 + 1, m_2)}.$$

В случаях, не рассмотренных в теоремах 1–3, то есть при

$$m_1 - r_1^1 - 1 < \frac{m_1}{2}, m_2 - r_2^2 - 1 < \frac{m_2}{2}, 2m_1 - (r_1^1 + r_2^1) - 2 < m_1, 2m_2 - (r_1^2 + r_2^2) - 2 < m_2, \quad (3)$$

представление (2) не удаётся упростить и сделать выводы о разложимости квадрата кода вида (1) в прямую сумму кодов Рида — Маллера. Но в этом случае можно оценить размерность кода (2) и проверить, возможно ли разложение этого кода в прямую сумму каких-либо кодов Рида — Маллера длины 2^{m_1} или 2^{m_2}. А именно, если размерность кода (2) не делится на 2^{m_1} или 2^{m_2}, то этот код не разлагается в прямую сумму и не является перестановочно эквивалентным такому коду. Согласно результатам вычислений, для $m_1 = 2, \ldots, 10$ и $m_2 = 2, \ldots, 10$ общее количество кодов вида (1), удовлетворяющих условиям (3), равно 9025. При этом количество кодов, размерность которых делится на 2^{m_1} или 2^{m_2}, равно 204. Это значит, что для случайно выбранного кода вида (1), удовлетворяющего условиям (3), с вероятностью более 0,97 его квадрат не разлагается в прямую сумму кодов Рида — Маллера длины 2^{m_1} или 2^{m_2}.

ЛИТЕРАТУРА

1. *Sendrier N. and Tillich J.-P.* Code-Based Cryptography: New Security Solutions Against a Quantum Adversary. ERCIM News, ERCIM, 2016.
2. `https://classic.mceliece.org/nist/mceliece-20201010.pdf` — Supporting Documentation describing the round-3 submission. 2020.
3. *Сидельников В. М., Шестаков С. О.* О системе шифрования, основанной на обобщенных кодах Рида — Соломона // Дискретная математика. 1992. Т. 3. № 3. С. 57–63.
4. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
5. *Чижов И. И., Бородин М. А.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.
6. *Деундяк В. М., Косолапов Ю. В., Лелюк Е. А.* Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам // Модел. и анализ информ. систем. 2017. Т. 24. № 2. С. 137–152.
7. *Деундяк В. М., Лелюк Е. А.* Теоретико-графовый метод декодирования некоторых групповых MLD-кодов // Дискретн. анализ и исслед. опер. 2020. Т. 27. № 2. С. 17–42.
8. *Randriambololona H.* On products and powers of linear codes under componentwise multiplication. arXiv:1312.0022. 2014.
9. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
10. *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.

11. *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.

УДК 519.17 DOI 10.17223/2226308X/14/36

РЕГУЛЯРНОЕ ВЕРШИННОЕ 1-РАСШИРЕНИЕ ДВУХМЕРНЫХ РЕШЁТОК[1]

А. А. Лобов, М. Б. Абросимов

Предлагается схема построения вершинного 1-расширения для двухмерной решётки $n \times m$ при $n \geqslant 2$ и $m \geqslant 2$, которое является регулярным графом степени 4. Показано, что с помощью данной схемы для некоторых решёток можно построить минимальное вершинное 1-расширение. Приведён пример графа, для которого построенное по схеме расширение не является минимальным.

Ключевые слова: *граф, решётка, отказоустойчивость, вершинное расширение.*

Безопасность вычислительных систем имеет большое значение. Отказ элементов может привести к её полной неработоспособности. Для обеспечения отказоустойчивости таких систем может применяться графовая модель. Каждому вычислительному узлу системы сопоставляется вершина графа, а связь между двумя узлами представляется ребром между соответствующими вершинами. Далее граф дополняется вершинами и рёбрами до вершинного k-расширения, которое является представлением устойчивой к отказу k узлов вычислительной системы. Будем рассматривать случай с $k = 1$.

Граф G^* является вершинным 1-расширением (В-1-Р) графа G, если G вкладывается в каждый граф, полученный из G^* удалением одной вершины. Если количество вершин в G^* на 1 больше, чем в G, и среди всех В-1-Р графа G с таким числом вершин количество рёбер в G^* минимально, то G^* называется минимальным вершинным 1-расширением (МВ-1-Р) графа G [1].

Задача построения расширений графа связана с построением отказоустойчивой вычислительной системы [2, 3]. В этих работах для некоторых классов графов, таких, как цепи и циклы, предложены способы построения МВ-1-Р, однако в целом задача нахождения МВ-1-Р заданного графа является вычислительно сложной [4].

Дадим определение рассматриваемым в работе графам.

Определение 1. *Двухмерной решёткой*, или просто *решёткой* $n \times m$, называется граф, множество вершин которого состоит из пар (i, j), $i, j \in \{0, \ldots, n-1\}$, и множество рёбер состоит из всех возможных пар вершин (u_1, v_1) и (u_2, v_2), для которых $|u_1 - u_2| = 1$ и $v_1 = v_2$ или $|v_1 - v_2| = 1$ и $u_1 = u_2$.

Пример такого графа представлен на рис. 1.

Двухмерная решётка является интересной топологией с практической точки зрения.

Теорема 1. При $n, m \geqslant 2$ для каждой решётки $n \times m$ существует регулярный граф степени 4, который является её вершинным 1-расширением. Количество дополнительных рёбер в данном расширении равно $n + m + 2$.

[1]Работа выполнена при поддержке Минобрнауки России в рамках выполнения госзадания (проект № FSRR-2020-0006).