ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.725 DOI 10.17223/20710410/68/4

НЕАСИМПТОТИЧЕСКАЯ ОЦЕНКА ВЕРОЯТНОСТИ ТОГО, ЧТО КВАДРАТ ШУРА — АДАМАРА СЛУЧАЙНОГО ДЛИННОГО ЛИНЕЙНОГО КОДА ИМЕЕТ МАКСИМАЛЬНУЮ РАЗМЕРНОСТЬ

И. В. Чижов

МГУ имени М. В. Ломоносова,
Федеральный исследовательский центр «Информатика и управление» РАН,
АО «НПК „Криптонит“», г. Москва, Россия

E-mail: ichizhov@cs.msu.ru

Установлена оценка вероятности того, что квадрат Адамара (Шура — Адамара) случайного линейного кода размерности k и длины $n > k(k+1)/2$ имеет максимально возможную размерность. Оценка носит неасимптотический характер и поэтому может быть использована для обоснования сложности методов криптографического анализа постквантовых криптосистем, построенных на основе теории помехоустойчивого кодирования.

Ключевые слова: *произведение Шура линейных кодов, произведение Адамара линейных кодов, случайный код, квадрат Шура, квадрат Адамара, криптосистема Мак-Элиса.*

A NON-ASYMPTOTIC ESTIMATE OF THE PROBABILITY THAT A SHUR — HADAMARD SQUARE OF LONG RANDOM LINEAR CODE HAS A MAXIMUM DIMENSION

I. V. Chizhov

Lomonosov Moscow State University,
Federal Research Center “Computer Science and Control” of the RAS,
Joint Stock “Research and production company Kryptonite”, Moscow, Russia

Let $\mathbb{F}_q$ be a finite field of q elements. Let $\mathcal{V}_n(q)$ denote the vector space of length n over $\mathbb{F}_q$. Define a linear $[n,k]_q$-code $\mathcal{C}$ as any linear subspace of dimension k of the space $\mathcal{V}_n(q)$. This paper focuses on a special operation defined on the set of linear codes of the same length: the Schur — Hadamard product, also known as the Schur product or Hadamard product. The Schur — Hadamard product of two vectors $x = (x_1, \ldots, x_n) \in \mathcal{V}_n(q)$ and $y = (y_1, \ldots, y_n) \in \mathcal{V}_n(q)$ is defined as the vector $x \circ y = (x_1 \cdot y_1, \ldots, x_n \cdot y_n) \in \mathcal{V}_n(q)$, where $\cdot$ is the field $\mathbb{F}_q$ multiplication. Define the Schur — Hadamard square $\mathcal{C}^{\circ 2}$ of $[n]_q$-code $\mathcal{C}$ as the linear span of the set of vectors $\{c \circ b : c, b \in \mathcal{C}\}$. It is known that for any $[n,k]_q$-code $\mathcal{C}$ the inequality $\dim \mathcal{C}^{\circ 2} \leqslant \min\left(k(k+1)/2, n\right)$ holds. For a random linear code, the probability that its Schur — Hadamard square has the maximum possible dimension tends to 1 as $n, k \to \infty$. This fact is used in the analysis of code-based cryptosystems. However, in

practice researchers deal with fixed values of k and n. Therefore, the non-asymptotic estimation of the probability that the Schur — Hadamard square of a random $[n,k]_q$-code has the maximum possible dimension is of interest. In the case $n < k(k+1)/2$ such an estimate was obtained earlier. We provide a non-asymptotic estimate for the case $n > k(k+1)/2$. Two theorems are proven: the first gives an estimate for very long codes, while the second applies to relatively short codes. Let $k, n \in \mathbb{N}$ be such that $k \geqslant 5$ and $n > k(k+1)/2$. Then the following inequality holds:

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - q^{k(k+1)/2+\log_q 2-(2-\log_q(2q-1))n}.$$

If $k \geqslant 6$ and $n < (k^2-4k)/2(\log_q(2q-1)-1)$, then

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - q^{k(k+1)/2+\log_q 2-\left(1-\log_q\left(1+(q-1)q^{-\delta_q(n,k)k}\right)\right)n},$$

where $\delta_q(n,k) = \dfrac{1}{2} + \dfrac{1}{2k} - \dfrac{1}{2k}\sqrt{2k+1+2(\log_q(2q-1)-1)n}$. Finally, examples of estimates are given for different values of n, k and q.

Keywords: *Shur product of linear codes, Hadamard product of linear codes, random codes, Shur square of linear code, Hadamard square of linear code, McEliece public key cryptosystem.*

Введение

Значительный прогресс в области анализа кодовых постквантовых криптографических систем с открытым ключом не в последнюю очередь обязан применению такой операции над линейными кодами, как их покоординатное произведение, или произведение Шура — Адамара.

В алгебраической теории помехоустойчивого кодирования произведение Шура — Адамара появилось в 1992 г. В работе [1] операция покоординатного произведения линейных кодов использовалась для построения так называемых пар локаторов ошибок.

В области анализа кодовых криптосистем операция произведения Шура — Адамара использована впервые в [2], где построена первая полиномиальная атака на криптосистему Бергера — Луадро [3].

В 2013 г. в работе [4] был построен первый эффективный алгоритм, который позволяет отличать коды Гоппы с высокой скоростью передачи от случайных кодов. Выяснилось, что иногда произведение Шура — Адамара кодов, дуальных к кодам Гоппы, не заполняет собой всё пространство; при этом случайные коды длины n при возведении в квадрат Адамара должны совпадать со всем пространством векторов длины n.

В дальнейшем тот факт, что код, на основе которого построена кодовая криптосистема, ведёт себя относительно произведения Адамара не как случайный, был использован для построения атак на различные модификации криптосистемы Мак-Элиса [5–10].

В 2015 г. в работе [11] установлена асимптотическая оценка того, что квадрат Адамара случайного линейного кода имеет максимально возможную размерность. Таким образом, было показано, что при росте параметров кода найти случайно код, квадрат Адамара которого имеет не максимальную размерность, практически невозможно.

Однако в криптографических приложениях криптоаналитики имеют дело с фиксированными значениями параметров линейных кодов. И возникает вопрос, насколько эффективен тот или иной отличитель кода от случайного при этих параметрах, а не в бесконечности. В 2023 г. в работе [12] была применена техника, связанная с обобщённым расстоянием Хемминга кодов Рида — Маллера второго порядка, для получения

неасимптотической оценки вероятности того, что квадрат Адамара линейного кода заполняет собой всё пространство. Однако эта оценка становится тривиальной, если рассматриваются длинные линейные коды, т. е. такие коды, у которых длина больше половины квадрата размерности.

В настоящей работе изучается случай длинных кодов. Доказана неасимптотическая оценка вероятности того, что случайный линейный длинный код имеет максимально возможную размерность. Заметим, что в этом случае квадрат Адамара такого кода не будет заполнять всё пространство, так как в силу большой длины кода в квадрате Адамара не хватит кодовых слов.

Для получения неасимптотической оценки применена более простая техника, чем в работе [11], но новая оценка вполне может быть использована для изучения конкретных вариантов кодовых криптосистем с заранее фиксированным набором значений их параметров.

1. Основные термины и определения

Рассмотрим конечное поле $\mathbb{F}_q$, состоящее из q элементов. Обозначим через $\mathcal{V}_n(q)$ пространство векторов длины n над $\mathbb{F}_q$. Будем считать, что элементами $\mathcal{V}_n(q)$ являются векторы-строки с координатами из поля $\mathbb{F}_q$.

Следуя классической монографии [13], дадим основные определения из теории кодов, исправляющих ошибки.

Линейным блоковым кодом, исправляющим ошибки, или *линейным кодом*, или просто *кодом* над полем $\mathbb{F}_q$ будем называть произвольное подпространство $\mathcal{C}$ пространства $\mathcal{V}_n(q)$. Число n в этом случае называется *длиной* кода. Векторы c, принадлежащие $\mathcal{C}$, называются *кодовыми словами* (или просто *словами*) кода $\mathcal{C}$. Линейный код $\mathcal{C}$ длины n над полем $\mathbb{F}_q$ называется $[n]_q$-кодом.

Любой $[n]_q$-код $\mathcal{C}$ как линейное пространство имеет размерность k. Тогда k называется *размерностью* $\mathcal{C}$ и обозначается $\dim\mathcal{C}$. Кроме того, $[n]_q$-код $\mathcal{C}$ размерности k называется $[n,k]_q$-кодом.

Так как $[n,k]_q$-код $\mathcal{C}$ является линейным пространством, он может быть задан своим базисом. Матрица, строками которой являются базисные векторы кода $\mathcal{C}$, называется *порождающей матрицей*. Порождающая матрица $[n,k]_q$-кода $\mathcal{C}$ является $(k\times n)$-матрицей и имеет полный ранг, равный k. Получается, что произвольный $[n,k]_q$-код $\mathcal{C}$ с порождающей матрицей G может быть задан как множество всех линейных комбинаций строк матрицы G, т. е. $\mathcal{C}=\{a\cdot G:\ a\in\mathcal{V}_k(q)\}$.

Иногда удобно задавать $[n,k]_q$-код $\mathcal{C}$ некоторой $(\ell\times n)$-матрицей D, которая обладает таким же свойством, как и порождающая матрица: линейная комбинация строк D совпадает с кодом $\mathcal{C}$, т. е. $\mathcal{C}=\{a\cdot D:\ a\in\mathcal{V}_\ell(q)\}$. Матрица D называется *охватывающей матрицей* кода $\mathcal{C}$ [14]. Порождающая матрица G кода $\mathcal{C}$ является и охватывающей. Фактически порождающая матрица является частным случаем охватывающей, а именно: это охватывающая матрица, имеющая полный ранг. В общем случае ни порождающая, ни охватывающая матрицы не заданы однозначно. Однако каждая порождающая и каждая охватывающая матрица задаёт ровно один линейный код.

Для каждого вектора $v\in\mathcal{V}_n(q)$ обозначим через $\mathrm{wt}(v)$ его вес Хемминга, т. е. число ненулевых координат этого вектора. С $[n,k]_q$-кодом $\mathcal{C}$ свяжем характеристику $d_{\mathcal{C}}$, которая равна минимальному весу Хемминга ненулевых кодовых слов $\mathcal{C}$: $d_{\mathcal{C}}=\min\limits_{c\in\mathcal{C},\ c\neq 0}\mathrm{wt}(c)$. Число $d_{\mathcal{C}}$ называется *минимальным расстоянием* кода $\mathcal{C}$. В дальнейшем $[n,k]_q$-код $\mathcal{C}$ с минимальным расстоянием d будем называть $[n,k,d]_q$-кодом.

Объектом исследований настоящей работы является специальная операция, заданная на множестве линейных кодов одной длины: произведение Шура — Адамара (произведение Шура или произведение Адамара).

Произведением Адамара векторов $x = (x_1, x_2, \ldots, x_n) \in \mathcal{V}_n(q)$ и $y = (y_1, y_2, \ldots, y_n) \in \in \mathcal{V}_n(q)$ называется вектор $x \circ y \in \mathcal{V}_n(q)$, равный покомпонентному произведению этих векторов:

$$x \circ y = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n).$$

Здесь «$\cdot$» — произведение элементов поля $\mathbb{F}_q$.

Операцию произведения Адамара двух $[n]_q$-кодов $\mathcal{C}$ и $\mathcal{B}$ можно задать двумя эквивалентными способами [15].

П е р в ы й с п о с о б. *Произведением Адамара* двух $[n]_q$-кодов $\mathcal{C}$ и $\mathcal{B}$ называется $[n]_q$-код $\mathcal{C} \circ \mathcal{B}$, равный линейной оболочке множества векторов $\{c \circ b : c \in \mathcal{C}, b \in \mathcal{B}\}$.

В т о р о й с п о с о б — через базисы кодов $\mathcal{C}$ и $\mathcal{B}$. Пусть $c_1, c_2, \ldots, c_{k_\mathcal{C}}$ — базис $[n, k_\mathcal{C}]_q$-кода $\mathcal{C}$, а $\{b_1, b_2, \ldots, b_{k_\mathcal{B}}\}$ — базис $[n, k_\mathcal{B}]_q$-кода $\mathcal{B}$. Тогда произведением Адамара называется $[n, k]_q$-код $\mathcal{C} \circ \mathcal{B}$, который охватывается матрицей D, составленной из $k_\mathcal{C} \cdot k_\mathcal{B}$ строк $c_i \circ b_j$, $i = 1, \ldots, k_\mathcal{C}$ и $j = 1, \ldots, k_\mathcal{B}$.

Квадратом Шура — Адамара (или *квадратом Адамара*) $[n]_q$-кода $\mathcal{C}$ будем называть $[n]_q$-код $\mathcal{C}^{\circ 2}$, равный произведению Адамара кода $\mathcal{C}$ на себя: $\mathcal{C}^{\circ 2} = \mathcal{C} \circ \mathcal{C}$.

Утверждение 1 [11]. Для любого $[n, k]_q$-кода $\mathcal{C}$ выполняется неравенство

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

В работе [11] установлено, что для случайного $[n, k]_q$-кода неравенство (1) обращается в равенство с вероятностью, которая стремится к 1 при $n, k \to \infty$. Однако в практических приложениях, особенно в задачах криптографического анализа, исследователи имеют дело с фиксированными значениями k и n, поэтому интерес представляет получение неасимптотической оценки вероятности того, что для случайного $[n, k]_q$-кода неравенство (1) становится равенством. В случае, когда $n < k(k+1)/2$, такая оценка вероятности получена ранее в [12]. Далее доказана неасимптотическая оценка в случае, когда $n > k(k+1)/2$.

2. Произведение Шура — Адамара линейного кода и квадратичные формы над конечным полем

Впервые связь между произведением Адамара линейных кодов и пространством квадратичных форм была установлена в работе [16]. Эта связь была использована авторами работы [11] для описания асимптотического поведения вероятности того, что квадрат Адамара случайного линейного кода достигает максимальной размерности. Этот же аппарат применён далее для получения неасимптотических оценок вероятности этого события.

Начнём с некоторых определений.

Квадратичной формой $Q(x_1, \ldots, x_k)$ над полем $\mathbb{F}_q$ называется однородный многочлен степени 2 от переменных $x_1, x_2, \ldots, x_k$ над тем же полем, т.е.

$$Q(x_1, \ldots, x_k) = \sum_{1 \leqslant i < j \leqslant k} a_{i,j} x_i x_j + \sum_{i=1}^{k} b_i x_i^2,$$

где $a_{i,j} \in \mathbb{F}_q$, $1 \leqslant i < j \leqslant k$; $b_i \in \mathbb{F}_q$, $1 \leqslant i \leqslant k$.

Множество всех квадратичных форм над полем $\mathbb{F}_q$ от k переменных будем обозначать как $\mathcal{Q}_k(q)$. Очевидно, что $\mathcal{Q}_k(q)$ является линейным пространством над полем $\mathbb{F}_q$. Базис этого пространства состоит из элементов

$$x_1^2,\ x_2^2,\ \ldots,\ x_k^2,\ x_1x_2,\ \ldots, x_{k-1}x_k.$$

Таким образом, $\mathcal{Q}_k(q)$ имеет размерность $k + \binom{k}{2} = \dfrac{k(k+1)}{2}$.

Зададим на множестве $\mathcal{V}_k(q)$ лексикографический порядок, упорядочив элементы поля $\mathbb{F}_q$ любым удобным способом. Этот порядок будем обозначать через $(\mathcal{V}_k(q), \leqslant) = \{x^{(0)} < x^{(1)} < \cdots < x^{(q^k-1)}\}$.

Для квадратичной формы $Q(x_1, \ldots, x_k) \in \mathcal{Q}_k(q)$ рассмотрим её вектор значений

$$\operatorname{eval}(Q) = \Big(Q(x^{(0)}), Q(x^{(1)}), \ldots, Q(x^{(q^k-1)})\Big) \in \mathcal{V}_{q^k}(q).$$

Матрица R, составленная из строк

$$\operatorname{eval}(x_1^2),\ \operatorname{eval}(x_2^2),\ \ldots,\ \operatorname{eval}(x_k^2),\ \operatorname{eval}(x_1x_2),\ \ldots,\ \operatorname{eval}(x_{k-1}x_k),$$

порождает некоторый $[q^k, k(k+1)/2, (q-1)^2q^{k-2}]_q$-код, который называется *однородным кодом Рида — Маллера* [17] и обозначается как $\mathcal{HRM}_q(2,k)$.

Каждый столбец матрицы R, как и каждая координата слова кода $\mathcal{HRM}_q(2,k)$, однозначно соответствует вектору $x^{(i)} \in (\mathcal{V}_q(n), \leqslant)$, поэтому столбцы этой матрицы и координаты кодовых слов можно занумеровать элементами частичного порядка $(\mathcal{V}_q(k), \leqslant)$; через $R_{x^{(i)}}$ будем обозначать столбец матрицы R с номером $x^{(i)}$.

Теперь, если $G = (g_1^\top g_2^\top \ldots g_n^\top)$ — $(k \times n)$-матрица над полем $\mathbb{F}_q$, составленная из столбцов $g_1^\top, g_2^\top, \ldots, g_n^\top$, то каждому g_i соответствует столбец R_{g_i} матрицы R, а всей матрице — подматрица R_G, составленная из столбцов R_{g_i}, $i = 1, 2, \ldots, n$.

Из [12, следствие 1] несложно вывести следующее

Утверждение 2. Для произвольных $k, n \in \mathbb{N}$, $k > 1$ и $n > k(k+1)/2$, рассмотрим некоторый $[n,k]_q$-код $\mathcal{C}$. Пусть G — его порождающая матрица. Тогда равенство $\dim \mathcal{C}^{\circ 2} = k(k+1)/2$ выполняется, если и только если $\operatorname{rank} R_G = k(k+1)/2$.

Утверждение 3. Пусть $G = (g_1^\top g_2^\top \ldots g_n^\top)$ — произвольная $(k \times n)$-матрица над полем $\mathbb{F}_q$ и $n > k(k+1)/2$. Тогда ранг матрицы R_G равен $k(k+1)/2$, если и только если для любой квадратичной формы $Q(x_1, \ldots, x_k) \in \mathcal{Q}_q(k)$, $Q \neq 0$, хотя бы для одного $i \in \{1, \ldots, k\}$ выполняется неравенство $Q(g_i) \neq 0$.

Из утверждений 2 и 3 прямо следует

Утверждение 4. Для произвольных $k, n \in \mathbb{N}$, $k > 1$ и $n > k(k+1)/2$, рассмотрим некоторый $[n,k]_q$-код $\mathcal{C}$. Пусть G — его порождающая матрица. Тогда равенство $\dim \mathcal{C}^{\circ 2} = k(k+1)/2$ выполняется, если и только если для любой квадратичной формы $Q(x_1, \ldots, x_k) \in \mathcal{Q}_k(q)$, $Q \neq 0$, хотя бы для одного $i \in \{1, \ldots, k\}$ верно неравенство $Q(g_i) \neq 0$.

В дальнейшем нам потребуется утверждение, которое задаёт значение спектра весов кода $\mathcal{HRM}_q(2,m)$ [17].

Утверждение 5. Пусть A_w — количество кодовых слов веса w в коде $\mathcal{HRM}_q(2,m)$. Тогда справедливы следующие равенства:

1) $A_0 = 1$;
2) $A_{q^m - q^{m-1}} = q^m - 1 + \sum\limits_{j=1}^{\lfloor (m-1)/2 \rfloor} q^{j^2+j} \prod\limits_{i=m-2j}^{m} (q^i - 1) \Big/ \prod\limits_{i=1}^{j} (q^{2i} - 1)$;
3) $A_{q^m - q^{m-1} - \tau q^{m-j-1}(q-1)} = \dfrac{q^{j^2+j} + \tau q^{j^2}}{2} \prod\limits_{i=m-2j+1}^{m} (q^i - 1) \Big/ \prod\limits_{i=1}^{j} (q^{2i} - 1)$, где $\tau \in \{-1, 1\}$ и $1 \leqslant j \leqslant \lfloor m/2 \rfloor$;
4) $A_w = 0$ для остальных w.

3. Оценка вероятности того, что случайный линейный код имеет максимальную размерность

Определим вероятностную схему $A_{n,k}(q)$ выбора случайного линейного $[n, k]_q$-кода. Будем последовательно случайно, равновероятно и независимо друг от друга выбирать векторы $g_1, g_2, \ldots, g_n$ из $\mathcal{V}_k(q)$. Сформируем из выбранных векторов матрицу $G = (g_1^\top, g_2^\top, \ldots, g_n^\top)$. Эта матрица охватывает некоторый $[n]_q$-код $\mathcal{C}$, который имеет размерность не более k. Тот факт, что код $\mathcal{C}$ построен описанным способом, будем обозначать следующим образом: $\mathcal{C} \xleftarrow{\$} A_{n,k}(q)$.

Другие вероятностные схемы обсуждаются в заключении.

Далее, используя утверждение 5, установим вероятность того, что случайно выбранный набор элементов из $\mathcal{V}_k(q)$ состоит из корней хотя бы одной квадратичной формы $Q \in \mathcal{Q}_k(q)$. На основании утверждения 3 эта вероятность определяет вероятность того, что случайный линейный код $\mathcal{C}$, выбранный по схеме $A_{n,k}(q)$, имеет максимально возможную размерность.

Утверждение 6. Пусть $k, n \in \mathbb{N}$ и $k > 1$. Зафиксируем произвольное $\delta \in \mathbb{R}$ таким образом, чтобы выполнялось неравенство $1 < \delta \cdot k \leqslant k/2$. Выберем $\mathcal{C} \xleftarrow{\$} A_{n,k}(q)$. Тогда справедливо неравенство

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - q^{2\delta(1-\delta)k^2 + 2\delta k + \log_q(\delta k) - a_q n} - q^{k(k+1)/2 - n(1 - \log_q(1 + (q-1)q^{-\delta k}))},$$

где $a_q = 2 - \log_q(2q-1)$.

Доказательство. Будем оценивать сверху вероятность противоположного события

$$\Gamma = \left[\dim \mathcal{C}^{\circ 2} \neq k(k+1)/2\right].$$

Если $G = (g_1^\top, g_2^\top, \ldots, g_n^\top)$ — порождающая матрица кода $\mathcal{C}$, то на основании утверждения 4 событие Γ возникает, если и только если существует квадратичная форма $Q \in \mathcal{Q}_k(q)$, $Q \neq 0$, которая обращается в нуль на всех столбцах матрицы G:

$$Q(g_1) = Q(g_2) = \ldots = Q(g_n) = 0.$$

Поэтому справедливо неравенство

$$\Pr[\Gamma] \leqslant \sum_{Q \in \mathcal{Q}_k(q), Q \neq 0} \Pr\left[Q(g_1) = Q(g_2) = \ldots = Q(g_n) = 0\right].$$

Теперь, так как в соответствии с распределением $A_{n,k}(q)$ каждый вектор g_i, $i = 1, \ldots, n$, выбирается случайно и равновероятно из $\mathcal{V}_k(q)$ независимо от других векторов, то

$$\Pr\left[Q(g_1) = Q(g_2) = \ldots = Q(g_n) = 0\right] = \prod_{i=1}^{n} \Pr\left[Q(g_i) = 0\right].$$

Но так как $\Pr\left[Q(g_i)=0\right]=1-\Pr\left[Q(g_i)\neq 0\right]$, $i=1,\ldots,n$, то выполнено равенство

$$\Pr\left[Q(g_1)=Q(g_2)=\ldots=Q(g_n)=0\right]=\prod_{i=1}^{n}\left(1-\Pr\left[Q(g_i)\neq 0\right]\right).$$

В силу выбора g_i равновероятно из всех векторов длины k над полем $\mathbb{F}_q$ верно равенство

$$\Pr\left[Q(g_i)\neq 0\right]=\mathrm{wt}(\mathrm{eval}(Q))/q^k,\quad i=1,\ldots,n.$$

Значит,

$$\Pr\left[Q(g_1)=Q(g_2)=\ldots=Q(g_n)=0\right]=\left(1-\mathrm{wt}(\mathrm{eval}(Q))/q^k\right)^n.$$

Отсюда получаем оценку

$$\Pr\left[\Gamma\right]\leqslant\sum_{Q\in\mathcal{Q}_k(q),Q\neq 0}\left(1-\frac{\mathrm{wt}(\mathrm{eval}(Q))}{q^k}\right)^n.$$

Зафиксируем некоторое $\delta\in\mathbb{R}$, $1/k<\delta\leqslant 1/2$. Множество всех квадратичных форм разобьём на два непересекающихся подмножества $\mathcal{Q}^0$ и $\mathcal{Q}^1$. Подмножество $\mathcal{Q}^0$ состоит из всех квадратичных форм $Q\in\mathcal{Q}_k(q)$, для которых вес вектора $\mathrm{eval}(Q)$ не больше $q^k-q^{k-1}-(q-1)q^{k-1-\delta k}$:

$$\mathcal{Q}^0=\{Q\in\mathcal{Q}_k(q):\mathrm{wt}(\mathrm{eval}(Q))\leqslant q^k-q^{k-1}-(q-1)q^{k-1-\delta k}\}.$$

В подмножество $\mathcal{Q}^1$ поместим оставшиеся $Q\in\mathcal{Q}_k(q)$:

$$\mathcal{Q}^1=\{Q\in\mathcal{Q}_k(q):\mathrm{wt}(\mathrm{eval}(Q))>q^k-q^{k-1}-(q-1)q^{k-1-\delta k}\}.$$

Заметив, что $0\in\mathcal{Q}^0$, можно записать

$$\sum_{Q\in\mathcal{Q},Q\neq 0}\left(1-\frac{\mathrm{wt}(\mathrm{eval}(Q)}{q^k}\right)^n=\sum_{Q\in\mathcal{Q}^0,Q\neq 0}\left(1-\frac{\mathrm{wt}(\mathrm{eval}(Q)}{q^k}\right)^n+\sum_{Q\in\mathcal{Q}^1}\left(1-\frac{\mathrm{wt}(\mathrm{eval}(Q))}{q^k}\right)^n.$$

Минимальное расстояние кода $\mathcal{HRM}_q(2,k)$ равно $d_{\mathcal{HRM}_q(2,k)}=(q-1)^2q^{k-2}$. Поэтому по определению числа $d_{\mathcal{HRM}_q(2,k)}$, если $Q\in\mathcal{Q}^0$ и $Q\neq 0$, то $\mathrm{wt}(\mathrm{eval}(Q))\geqslant d_{\mathcal{HRM}_q(2,k)}=$ $=(q-1)^2q^{k-2}$, а значит,

$$1-\frac{\mathrm{wt}(\mathrm{eval}(Q))}{q^k}\leqslant 1-\frac{(q-1)^2}{q^2}=\frac{2q-1}{q^2}.$$

Для $Q\in\mathcal{Q}^1$ по определению верно неравенство

$$\mathrm{wt}(\mathrm{eval}(Q))>(q-1)q^{k-1}-(q-1)q^{k-1-\delta k},$$

поэтому в этом случае

$$1-\frac{\mathrm{wt}(\mathrm{eval}(Q))}{q^k}<1-\frac{q-1}{q}(1-q^{-\delta k})=\frac{1}{q}(1+(q-1)q^{-\delta k}).$$

Следовательно, справедливо неравенство

$$\Pr\left[\Gamma\right]<\left(\frac{2q-1}{q^2}\right)^n|\mathcal{Q}^0\setminus\{0\}|+\frac{(1+(q-1)q^{-\delta k})^n}{q^n}|\mathcal{Q}^1|.$$

По построению $\mathcal{Q}^1 \subseteq \mathcal{Q}_k(q)$, поэтому верна тривиальная оценка $|\mathcal{Q}^1| \leqslant |\mathcal{Q}_k(q)| = q^{(k+1)k/2}$. Получаем неравенство

$$\Pr\left[\Gamma\right] < \left(\frac{2q-1}{q^2}\right)^n |\mathcal{Q}^0 \setminus \{0\}| + (1+(q-1)q^{-\delta k})^n\, q^{k(k+1)/2-n}.$$

Введя константу $a_q = 2 - \log_q(2q-1)$, будем иметь

$$\Pr\left[\Gamma\right] < q^{-a_q n}|\mathcal{Q}^0 \setminus \{0\}| + q^{k(k+1)/2-n(1-\log_q(1+(q-1)q^{-\delta k}))}. \tag{2}$$

Оценим сверху величину $|\mathcal{Q}^0\setminus\{0\}|$. В множестве $\mathcal{Q}^0$ лежат квадратичные формы Q, у которых вес вектора $\mathrm{eval}(Q)$ не больше, чем $q^k - q^{k-1} - (q-1)q^{k-1-\delta k}$. Так как $q > 1$, для любого δ справедливо неравенство $q^k - q^{k-1} - (q-1)q^{k-1-\delta k} < q^k - q^{k-1}$ и, кроме того, для любого j верно, что $q^k - q^{k-1} < q^k - q^{k-1} + (q-1)q^{k-1-j}$. Значит, согласно утверждению 5, если $Q \in \mathcal{Q}^0$, то либо $\mathrm{wt}(\mathrm{eval}(Q)) = 0$, либо $\mathrm{wt}(\mathrm{eval}(Q)) = q^k - q^{k-1} - (q-1)q^{k-1-j}$ для некоторого j, $1 \leqslant j \leqslant \lfloor k/2 \rfloor$. Из неравенства

$$q^k - q^{k-1} - (q-1)q^{k-1-j} \leqslant q^k - q^{k-1} - (q-1)q^{k-1-\delta k}$$

следует, что если $Q \in \mathcal{Q}^0$ и $\mathrm{wt}(\mathrm{eval}(Q)) \neq 0$, то $\mathrm{wt}(\mathrm{eval}(Q)) = q^k - q^{k-1} - (q-1)q^{k-1-j}$ для $j \in \mathbb{Z}$, $1 \leqslant j \leqslant \delta k$. Следовательно,

$$|\mathcal{Q}^0 \setminus \{0\}| = \sum_{j=1}^{\lfloor \delta k \rfloor} A_{q^k - q^{k-1} - (q-1)q^{k-1-j}}.$$

С учётом утверждения 5 получим следующее выражение:

$$|\mathcal{Q}^0 \setminus \{0\}| = \sum_{j=1}^{\lfloor \delta k \rfloor} \frac{q^{j^2+j} + q^{j^2}}{2} \prod_{i=k-2j+1}^{k} (q^i - 1) \Big/ \prod_{i=1}^{j} (q^{2i} - 1). \tag{3}$$

Так как по условию $\delta k > 1$, то $\lfloor \delta k \rfloor \geqslant 1$, поэтому сумма (3) содержит хотя бы одно ненулевое слагаемое.

Оценим сверху каждое слагаемое суммы (3) для $j = 1, \ldots, \lfloor \delta k \rfloor$.

При $q \geqslant 2$ и $i \geqslant 1$ верно неравенство $(q-1)q^{i-1} \geqslant 1$, поэтому $q^i - 1 \geqslant q^{i-1}$ для всех $i \geqslant 1$ и $q \geqslant 2$, а значит,

$$\prod_{i=1}^{j} (q^{2i} - 1) \geqslant \prod_{i=1}^{j} q^{2i-1} = q^{2\sum\limits_{i=1}^{j} i - j} = q^{j(j+1)-j} = q^{j^2}.$$

Тогда

$$q^{j^2}(q^j + 1) \Big/ \prod_{i=1}^{j} (q^{2i} - 1) \leqslant \frac{q^{j^2}(q^j+1)}{q^{j^2}} = q^j + 1.$$

Далее,

$$\prod_{i=k-2j+1}^{k} (q^i - 1) < \prod_{i=k-2j+1}^{k} q^i = q^{\sum\limits_{i=k-2j+1}^{k} i} = q^{j(2k-2j+1)}.$$

Таким образом, для $j \geqslant 1$ верно неравенство

$$\frac{q^{j^2+j} + q^{j^2}}{2} \frac{\prod\limits_{i=k-2j+1}^{k} (q^i - 1)}{\prod\limits_{i=1}^{j} (q^{2i} - 1)} = \frac{1}{2} \frac{q^{j^2}(q^j+1)}{\prod\limits_{i=1}^{j} (q^{2i} - 1)} \prod_{i=k-2j+1}^{k} (q^i - 1) < \frac{1}{2}(q^j + 1)q^{j(2k-2j+1)}.$$

Так как $q^j > 1$ при $q > 1$ и $j \geqslant 1$, то в этом случае $q^j > (q^j + 1)/2$. Получим оценку мощности $\mathcal{Q}^0 \setminus \{0\}$:

$$|\mathcal{Q}^0 \setminus \{0\}| < \sum_{j=1}^{\lfloor \delta k \rfloor} q^{2j(k-j+1)}.$$

Функция $f(x) = x(k - x + 1)$ на отрезке $0 \leqslant x \leqslant (k + 1)/2$ не убывает; δ выбрано таким образом, чтобы $\delta k \leqslant k/2 < (k + 1)/2$, поэтому для любого $1 \leqslant j \leqslant \lfloor \delta k \rfloor \leqslant \delta k$ выполняется неравенство $2j(k - j + 1) \leqslant 2\delta k(k - \delta k + 1)$. Значит,

$$|\mathcal{Q}^0 \setminus \{0\}| < \delta k q^{2\delta(1-\delta)k^2+2\delta k} = q^{2\delta(1-\delta)k^2+2\delta k+\log_q \delta k}.$$

Из неравенства (2) окончательно получим оценку вероятности события Γ:

$$\Pr\left[\Gamma\right] < q^{2\delta(1-\delta)k^2+2\delta k+\log_q(\delta k)-a_q n} + q^{k(k+1)/2-n(1-\log_q(1+(q-1)q^{-\delta k}))}.$$

С учётом $\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] = 1 - \Pr\left[\Gamma\right]$ получим требуемое неравенство. ■

Проанализируем оценку из утверждения 6.

Теорема 1. Зафиксируем числа $k, n \in \mathbb{N}$ таким образом, что $k \geqslant 5$ и $n > k(k+1)/2$. Выберем $\mathcal{C} \xleftarrow{\$} A_{n,k}(q)$. Тогда справедливо неравенство

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - q^{k(k+1)/2+\log_q 2-(2-\log_q(2q-1))n}.$$

Доказательство. Докажем, что существует δ, $1 < \delta k \leqslant k/2$, для которого выполняется неравенство

$$2\delta(1-\delta)k^2 + 2\delta k \leqslant k(k+1)/2. \tag{4}$$

Действительно, $2\delta(1-\delta)$ достигает максимального значения при $\delta = 1/2$, поэтому для любого $\delta \leqslant 1/2$ имеет место

$$2\delta(1-\delta)k^2 \leqslant k^2/2.$$

Если $k \geqslant 5$, то $1/k \leqslant 1/5 < \delta = 1/4 < 1/2$, поэтому, например, при $\delta = 1/4$ верно (4).

Далее докажем, что для любых k, $k > 0$, δ, $1/k < \delta \leqslant 1/2$, и любого q, $q > 1$, выполняется неравенство

$$1 - \log_q(1 + (q-1)q^{-\delta k}) > a_q = 2 - \log_q(2q-1).$$

Это неравенство эквивалентно следующему:

$$\log_q \frac{2q-1}{1+(q-1)q^{-\delta k}} > 1,$$

которое, в свою очередь, эквивалентно неравенству

$$\frac{2q-1}{1+(q-1)q^{-\delta k}} > q \quad \Leftrightarrow \quad 2q - 1 > q + (q-1)q^{1-\delta k}.$$

Упрощая и учитывая условие $q > 1$, придём к равносильному неравенству $1 > q^{1-\delta k}$, которое выполняется, если и только если $\delta k > 1$.

Итак, для выбранных k, δ и q выполняется условие

$$k(k+1)/2 - (1 - \log_q(1 + (q-1)q^{-\delta k}))n < k(k+1)/2 - a_q n.$$

Следовательно, при $k \geqslant 5$ существует такое δ, $1/k < \delta \leqslant 1/2$, что

$$q^{2\delta(1-\delta)k^2+2\delta k-a_q n} + q^{k(k+1)/2-(1-\log_q(1+(q-1)q^{-\delta k}))n} \leqslant 2q^{k(k+1)/2-a_q n}.$$

Из этого неравенства и утверждения 6 получим требуемую оценку вероятности. ■

В силу того, что при маленьких q константа $2-\log_q(2q-1)$ мала, оценка теоремы 1 имеет смысл только либо в случае достаточно больших q, либо для очень длинных кодов, у которых длина больше, чем $k(k+1)$. Для относительно коротких кодов оценку можно улучшить.

Теорема 2. Зафиксируем числа $k, n \in \mathbb{N}$ таким образом, что $k \geqslant 6$ и $n < \dfrac{k^2-4k}{2(\log_q(2q-1)-1)}$. Выберем $\mathcal{C} \xleftarrow{\$} A_{n,k}(q)$. Тогда справедливо неравенство

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - q^{k(k+1)/2+\log_q 2-(1-\log_q(1+(q-1)q^{-\delta_q(n,k)k}))n},$$

где

$$\delta_q(n,k) = \frac{1}{2} + \frac{1}{2k} - \frac{1}{2k}\sqrt{2k+1+2(\log_q(2q-1)-1)n}.$$

Доказательство. Найдём условия на n, k и q, при которых существует такое δ из полуинтервала $(k^{-1}, 2^{-1}]$, что выполнено неравенство

$$2\delta(1-\delta)k^2 + 2\delta k + \log_q(\delta k) - a_q n \leqslant k(k+1)/2 - n(1-\log_q(1+(q-1)q^{-\delta k})). \qquad (5)$$

Сначала заметим, что при $\delta \leqslant 1/2$, $k > 1$ и $q > 1$ верно $\log_q \delta k \leqslant k/2$, поэтому добьёмся выполнения условия

$$2\delta(1-\delta)k^2 + 2\delta k + k/2 - a_q n \leqslant k(k+1)/2 - n(1-\log_q(1+(q-1)q^{-\delta k})),$$

которое равносильно неравенству

$$2\delta(1-\delta)k^2 + 2\delta k - a_q n \leqslant k^2/2 - n(1-\log_q(1+(q-1)q^{-\delta k})).$$

При $q > 1$ имеет место $\log_q(1+(q-1)q^{-\delta k}) > 0$, поэтому

$$k^2/2 - n < k^2/2 - n(1-\log_q(1+(q-1)q^{-\delta k})).$$

Значит, достаточно найти условия, при которых существует $\delta \in (k^{-1}, 2^{-1}]$, гарантирующее выполнение равенства

$$2\delta(1-\delta)k^2 + 2\delta k - a_q n = k^2/2 - n.$$

Раскрывая скобки и приводя подобные слагаемые, получим квадратное уравнение относительно переменной δ:

$$2k^2\delta^2 - 2\delta(k^2+k) + k^2/2 - (1-a_q)n = 0.$$

Разделив уравнение на $2k^2 \neq 0$, получим

$$\delta^2 - \delta\left(1+\frac{1}{k}\right) + \frac{1}{4} - (1-a_q)\frac{n}{2k^2} = 0.$$

Решениями этого уравнения являются действительные числа δ_1 и δ_2:

$$\begin{aligned}\delta_1 &= \frac{1}{2} + \frac{1}{2k} - \frac{1}{2k}\sqrt{2k+1+2(1-a_q)n},\\ \delta_2 &= \frac{1}{2} + \frac{1}{2k} + \frac{1}{2k}\sqrt{2k+1+2(1-a_q)n}.\end{aligned} \tag{6}$$

Нетрудно понять, что $\delta_2 > 1/2$, так как $k > 0$. Значит, нужно искать такое δ_1, что $k^{-1} < \delta_1 \leqslant 2^{-1}$.

Условие $\delta_1 \leqslant 2^{-1}$ эквивалентно следующему: $1 \leqslant 2k + 1 + 2(1-a_q)n$. Так как при $q > 1$ выполняется неравенство $\log_q(2q-1) > 1$, то $1 - a_q = \log_q(2q-1) - 1 > 0$; значит, $2k + 2(1-a_q)n > 0$ и условие $\delta_1 \leqslant 2^{-1}$ верно при любых $n, k, q, q > 1$.

Осталось рассмотреть неравенство $k^{-1} < \delta_1$. Оно эквивалентно следующему:

$$\frac{1}{2k}\sqrt{2k+1+2(1-a_q)n} < \frac{1}{2} - \frac{1}{2k}.$$

Упрощая его, получим

$$2k + 1 + 2(1-a_q)n < (k-1)^2 = k^2 - 2k + 1 \Leftrightarrow 2(1-a_q)n < k^2 - 4k.$$

Таким образом, если $n < \dfrac{k^2-4k}{2(\log_q(2q-1)-1)}$, то найдётся такое $\delta_1 \in (k^{-1}, 2^{-1}]$, при котором выполнено (5).

Из неравенства (5) и утверждения 6 при $\delta_q(n,k) = \delta_1$ следует оценка вероятности

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - 2q^{k(k+1)/2 - (1-\log_q(1+(q-1)q^{-\delta_q(n,k)k}))n},$$

где через $\delta_q(n,k)$ обозначено δ_1 из (6). ■

4. Примеры

Рассмотрим несколько примеров.

Начнём с двоичных кодов. Пусть $n = 1600$ и $k = 50$. Из теоремы 1 следует оценка вероятности

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = k(k+1)/2\right] > 1 - 2^{50\cdot 51/2 + 1 - (2-\log_2 3)1600} \approx 1 - 2^{611},$$

т. е. в этом случае она тривиальная. Однако при выбранных параметрах верно неравенство

$$\frac{50^2 - 4\cdot 50}{2(\log_2(3)-1)} > 1983,$$

поэтому можно применить теорему 2. Вычислим $\delta_2(1600, 50)$:

$$\delta_2(1600,50) = \frac{1}{2} + \frac{1}{2\cdot 50} - \frac{1}{2\cdot 50}\sqrt{2\cdot 50 + 1 + 2\left(\log_2(3)-1\right)1600} > 0{,}0658.$$

Далее

$$1 - \log_2(1 + 2^{-0{,}0658\cdot 50}) < 0{,}85956.$$

Следовательно, из теоремы 2 следует, что для любого случайного $[1600, 50]$-кода $\mathcal{C}$ выполняется неравенство

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = 1275\right] > 1 - 2^{1275+1-0{,}85965\cdot 1600} > 1 - 2^{-99{,}44}.$$

Рассмотрим линейные коды размерности $k = 50$ и длины $n = 1600$, но уже над полем $\mathbb{F}_3$. Верно неравенство

$$\frac{50^2 - 4 \cdot 50}{2(\log_3(5) - 1)} > 2473.$$

Можно применить теорему 2. В этом случае

$$\delta_3(1600, 50) = \frac{1}{2} + \frac{1}{2 \cdot 50} - \frac{1}{2 \cdot 50}\sqrt{2 \cdot 50 + 1 + 2\,(\log_3(5) - 1)\,1600} > 0{,}111.$$

Далее

$$1 - \log_3(1 + 2 \cdot 3^{-0{,}111 \cdot 50}) < 0{,}996.$$

Значит, из теоремы 2 получим, что для любого случайного $[1600, 50]_3$-кода $\mathcal{C}$ выполняется неравенство

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = 1275\right] > 1 - 3^{1275 + \log_3(2) - 0{,}996 \cdot 1600} > 1 - 3^{-317{,}9} > 1 - 2^{-500}.$$

Нетрудно установить, для каких значений k и n оценка теоремы 2 является нетривиальной (строго больше нуля). Для этого нужно рассмотреть неравенство

$$k(k+1)/2 + \log_q 2 < (1 - \log_q(1 + (q-1)q^{-\delta_q(n,k)k}))n.$$

Оно эквивалентно неравенству

$$\delta_q(n,k)\,k > \log_q\left(\frac{q-1}{q^{1-k(k+1)/(2n)-(\log_q 2)/n} - 1}\right).$$

Подставляя значение $\delta_q(n,k)$, получим условие

$$\frac{k}{2} + \frac{1}{2} - \frac{1}{2}\sqrt{2k + 1 + 2(\log_q(2q-1) - 1)n} > \log_q\left(\frac{q-1}{q^{1-k(k+1)/(2n)-(\log_q 2)/n} - 1}\right),$$

которое должно выполняться, чтобы оценка имела смысл. С учётом неравенства $k \leqslant n$ получим

$$\frac{k}{2} + \frac{1}{2} - \frac{1}{\sqrt{2}}\sqrt{\log_q(2q-1) + 1} > \log_q\left(\frac{q-1}{q^{1-k(k+1)/(2n)-(\log_q 2)/n} - 1}\right).$$

Из этого неравенства видно, что при относительно больших k и n при условии, что отношение $k(k+1)/(2n)$ достаточно мало, правая часть неравенства стремится к нулю, а левая при этом идёт к бесконечности. Таким образом, при достаточно больших k оценка теоремы 2 имеет смысл для почти всех допустимых n, т. е. при $k(k+1)/2 < n < \dfrac{k^2 - 4k}{2(\log_q(2q-1) - 1)n}$.

В завершении рассмотрим пример применения оценки теоремы 1.

Выберем $k = 50$ и $n = 3200$. Тогда квадрат Адамара случайного двоичного $[3200, 50]$-кода $\mathcal{C}$ имеет максимально возможную размерность 1275 с вероятностью

$$\Pr\left[\dim \mathcal{C}^{\circ 2} = 1275\right] > 1 - 2^{1276 - (2 - \log_2 3) \cdot 3200} > 1 - 2^{-52{,}11}.$$

Если рассматриваются троичные коды, то квадрат Адамара случайного $[3200, 50]_3$-кода $\mathcal{C}$ будет иметь размерность 1275 с вероятностью

$$\Pr\left[\mathcal{C}^{\circ 2} = 1275\right] > 1 - 3^{1275 + \log_3(2) - (2 - \log_3 5) \cdot 3200} > 1 - 3^{-436{,}45} > 1 - 2^{-691{,}76}.$$

Таким образом, найти случайно код, у которого квадрат Адамара не имеет максимальную размерность, оказывается трудной задачей.

Заключение

В работе с использованием известных результатов о спектре весов однородных кодов Рида — Маллера второго порядка установлена оценка вероятности того, что случайный линейный код длины n и размерности не более k над полем из q элементов имеет максимальную размерность. При этом полученная оценка не является асимптотической и может быть использована в обосновании результатов криптографического анализа постквантовых криптографических систем, построенных на основе кодов, исправляющих ошибки.

Сделаем несколько замечаний.

Первое касается вероятностной модели. Все результаты получены в модели, в которой фактически случайный линейный код отождествляется со случайной $(k \times n)$-матрицей, которая охватывает его. Однако эта модель не учитывает, что на практике используются коды с фиксированной размерностью, а не просто ограниченной сверху некоторым числом.

Рассмотрим другую модель. Для построения случайного $[n, k]_q$-кода $\mathcal{C}$ выбирается случайно и равновероятно $(k \times n)$-матрица G максимального ранга из множества всех $(k \times n)$-матриц ранга k и в качестве $\mathcal{C}$ выбирается код, порождаемый матрицей G. Этот факт будем записывать как $\mathcal{C} \xleftarrow{\$} U_{n,k}(q)$.

Известно [11], что если для некоторого $a \in \mathbb{R}$ выполняется

$$\Pr_{\mathcal{C} \xleftarrow{\$} A_{n,k}(q)} [\dim \mathcal{C} = k(k+1)/2] > 1 - q^{-a(n,k,q)},$$

то верно неравенство

$$\Pr_{\mathcal{C} \xleftarrow{\$} U_{n,k}(q)} [\dim \mathcal{C} = k(k+1)/2] > 1 - q^{-a(n,k,q)} - q^{-(n-k)}.$$

Используя этот факт, можно скорректировать оценки теорем 1 и 2. Отметим, что в конечном итоге добавленное в оценку слагаемое является несоизмеримо малой величиной по сравнению с основным слагаемым.

Второе замечание касается случая таких параметров n, k и q, что оценки обеих теорем 1 и 2 являются тривиальными. Такое возможно при относительно малых k и n. Так, например, если $k = 40$ и $n = 1024$, то для двоичных кодов оценка теоремы 1 становится равной примерно $1 - 2^{396} < 0$, а оценка теоремы 2 — примерно $1 - 2^{19{,}89} < 0$. Таким образом, остаётся открытым вопрос установления более точной оценки вероятности для кодов, параметры которых достаточно малы.

ЛИТЕРАТУРА

1. *Pellikaan R.* On decoding by error location and dependent sets of error positions // Discrete Math. 1992. V. 106–107. P. 369–381.
2. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes // LNCS. 2010. V. 6061. P. 61–72.
3. *Berger T. and Loidreau P.* How to mask the structure of codes for a cryptographic use // Des. Codes Cryptogr. 2005. V. 35. P. 63–79.
4. *Faugère J., Gauthier-Umanã V., Otmani A., et al.* A distinguisher for high-rate McEliece cryptosystems // IEEE Trans. Inform. Theory. 2013. V. 59. No. 10. P. 6830–6844.
5. *Couvreur A., Gaborit P., Gauthier-Umanã V., et al.* Distinguisher-based attacks on public-key cryptosystems using Reed — Solomon codes // Des. Codes Cryptogr. 2014. V. 73. No. 2. P. 641–666.

6. *Otmani A. and Kalachi H.* Square code attack on a modified Sidelnikov cryptosystem // LNCS. 2015. V. 9084. P. 173–183.
7. *Couvreur A., Otmani A., Tillich J.-P., and Gauthier-Umanã V.* A polynomial-time attack on the BBCRS scheme // LNCS. 2015. V. 9020. P. 175–193.
8. *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.
9. *Чижов И. В., Попова Е. А.* Структурная атака на криптосистемы типа Мак-Элиса — Сидельникова, построенные на основе комбинирования случайных кодов с кодами Рида — Маллера // Intern. J. Open Inform. Technol. 2020. V. 8. No. 6. P. 24–33.
10. *Бородин М. А., Чижов И. В.* Классификация произведений Адамара подкодов коразмерности 1 кодов Рида — Маллера // Дискретная математика. 2020. Т. 32. № 1. С. 115–134.
11. *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.
12. *Чижов И. В.* Квадрат Адамара и обобщённое минимальное расстояние кода Рида — Маллера порядка 2 // Дискретная математика. 2023. Т. 35. № 1. С. 128–152.
13. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
14. *Hall J. I.* Notes on Coding Theory. `https://users.math.msu.edu/users/halljo/classes/CODENOTES/CODING-NOTES.HTML`. 2010.
15. *Чижов И. В.* Полная классификация произведений Адамара подкодов коразмерности 1 кодов Рида — Маллера // Вестник Московского университета. Сер. 15: Вычислительная математика и кибернетика. 2024. № 1. С. 67–80.
16. *Randriambololona H.* On products and powers of linear codes under componentwise multiplication // Algorithmic Arithmetic, Geometry, and Coding Theory. 2015. V. 637. P. 3–78.
17. *Shuxing L.* On the weight distribution of second order Reed — Muller codes and their relatives // Des. Codes Cryptogr. 2019. V. 87. No. 10. P. 2447–2460.

REFERENCES

1. *Pellikaan R.* On decoding by error location and dependent sets of error positions. Discrete Math., 1992, vol. 106–107, pp. 369–381.
2. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. LNCS, 2010, vol. 6061, pp. 61–72.
3. *Berger T. and Loidreau P.* How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 2005, vol. 35, pp. 63–79.
4. *Faugère J., Gauthier-Umanã V., Otmani A., et al.* A distinguisher for high-rate McEliece cryptosystems. IEEE Trans. Inform. Theory, 2013, vol. 59, no. 10, pp. 6830–6844.
5. *Couvreur A., Gaborit P., Gauthier-Umanã V., et al.* Distinguisher-based attacks on public-key cryptosystems using Reed — Solomon codes. Des. Codes Cryptogr., 2014, vol. 73, no. 2, pp. 641–666.
6. *Otmani A. and Kalachi H.* Square code attack on a modified Sidelnikov cryptosystem. LNCS, 2015, vol. 9084, pp. 173–183.
7. *Couvreur A., Otmani A., Tillich J.-P., and Gauthier-Umanã V.* A polynomial-time attack on the BBCRS scheme. LNCS, 2015, vol. 9020, pp. 175–193.
8. *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.

9. *Chizhov I. V. and Popova E. A.* Strukturnaya ataka na kriptosistemy tipa Mak-Elisa — Sidel'nikova, postroennye na osnove kombinirovaniya sluchaynykh kodov s kodami Rida — Mallera [Structural attack on McEliece-Sidelnikov cryptosystems built on the combining of random codes with Reed-Muller codes]. Intern. J. Open Inform. Technol., 2020, vol. 8, no. 6, pp. 24–33. (in Russian)
10. *Borodin M. A. and Chizhov I. V.* Classification of Hadamard products of one-codimensional subcodes of Reed — Muller codes. Discrete Math. Appl., 2022, vol. 32, no. 5, pp. 297–311.
11. *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.
12. *Chizhov I. V.* Hadamard square of linear codes and the generalized minimal distance of Reed — Muller code of order 2. Discrete Math. Appl., 2025, vol. 35, no. 1, pp. 15–34. 1
13. *McWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Parts I and II. Amsterdam, North-Holland Publ., 1977. 762 p.
14. *Hall J. I.* Notes on Coding Theory. `https://users.math.msu.edu/users/halljo/classes/CODENOTES/CODING-NOTES.HTML`, 2010.
15. *Chizhov I. V.* Polnaya klassifikatsiya proizvedeniy Adamara podkodov korazmernosti 1 kodov Rida—Mallera [Complete classification of Hadamard products of codimension 1 subcodes of Reed-Muller codes]. Bulletin of Moscow University. Ser. 15: Comput. Math. and Cybernetics, 2024, no. 1, pp. 67–80. (in Russian)
16. *Randriambololona H.* On products and powers of linear codes under componentwise multiplication. Algorithmic Arithmetic, Geometry, and Coding Theory, 2015, vol. 637, pp. 3–78.
17. *Shuxing L.* On the weight distribution of second order Reed — Muller codes and their relatives. Des. Codes Cryptogr., 2019, vol. 87, no. 10, pp. 2447–2460.