The Hadamard square of concatenated linear codes

Ivan Chizhov[1] and Alexandra Davletshina[2]

[1]Lomonosov Moscow State University, Federal Research Center «Informatics and Control» of Russian Academy of Science, JSC «NPK Kryptonite», Russia
[2] JSC «InfoTeCS», Russia
ichizhov@cs.msu.ru, sdav94@rambler.ru

Abstract

The paper is devoted to the Hadamard square of concatenated linear codes. Such codes consist of codewords that are obtained by concatenation part of the codewords from other codes. It is proved that if the sum of Hadamard squares' dimensions of the codes used in the concatenation is slightly less than the dimension of the entire space, then the Hadamard square of the concatenated code is equal to the Cartesian product of the Hadamard square of code-components.

It means that the cryptanalysis for many code-based post-quantum cryptographic mechanisms built on concatenated codes is equivalent to the cryptanalysis of these mechanisms built on code-components. So using the concatenation of codes from different classes instead of one class of codes, generally speaking, does not increase the cryptographic strength of the mechanisms.

Keywords: concatenated linear codes, Hadamard square, Hadamard product, Schur product, component-wise product, McEliece public-key cryptosystem, post-quantum cryptography

1 Introduction

The Hadamard (Schur) product or the coordinate-wise product of linear codes has been studied for a long time. In the beginning, it was used to construct algebraic decoders correcting errors for some linear codes [18]. Recently, it is increasingly used in cryptography. Many constructions of secret sharing schemes and cryptographic protocols for secure multi-party computation [4] use the Hadamard product of linear codes. Attacks on post-quantum code-based cryptographic mechanisms are one of the main applications of this operation over linear codes. So, worth noting the attack [2] on the McEliece cryptosystem based on Reed-Muller binary codes, or the attack [22] on the same cryptosystem, but based on Reed-Solomon subcodes. Numerous examples of the Hadamard product application for constructing attacks on code-based cryptosystem given in works [7, 8, 9, 10, 17]. For the first time, the efficient algorithm was constructed in [13] that distinguishes Goppa codes from random binary codes using this operation.

For practical applications be essential to describe the Hadamard square of the linear code and establish its properties as a linear code. For example, in [3] it was proved that the Hadamard square of the linear code fills the entire space with a probability close to one. This property is often used to construct attacks on post-quantum public-key cryptosystems; for example, see works [1, 7, 10, 17]. Some cryptographic mechanisms are based on linear codes, the Hadamard square of which is not equal to the entire space. Then the algebraic or combinatorial structure of the Hadamard square of the linear code becomes important.

Recently, several attacks [5, 6, 11, 17] have been constructed on post-quantum cryptographic mechanisms based on the concatenation of linear codes from different classes. Such linear codes consist of codewords which are obtained by combining part of the codewords from other codes. Moreover, for these attacks to work correctly, it is required that the Hadamard square of the combined code is equal to the Cartesian product of Hadamard squares of the codes used in the combination. The researchers noted that this property is fulfilled almost always in the experiments, but there is no theoretical for this fact proved was provided.

In this paper, the theoretical gap is eliminated. And it is proved that if the sum of the Hadamard squares' dimensions of the codes used in the concatenation is slightly less than the dimension of the entire space, then the Hadamard square of the concatenated code is equal to the Cartesian product of Hadamard squares of code-components.

2 The main result

Let V_q^n be the linear space of all vectors of length n over $GF(q)$. *Block linear* $[n,k]_q$*-code* over $GF(q)$ or just *code* is a k-dimensional linear subspace $\mathcal{C}$ of V_q^n. In this case, n is called the *length* of the code, and k is called the *dimension* of code. When the dimension of the code $\mathcal{C} \subseteq V_q^n$ is not essential to us, it will be called the $[n]_q$-code $\mathcal{C}$. Vectors $c \in \mathcal{C}$ are called *codewords* of the code $\mathcal{C}$.

We say that the $[n]_q$-code $\mathcal{C}$ is generated by the $(k \times n)$-matrix G with elements from $GF(q)$ if the linear combination of the rows of the matrix G over $GF(q)$ coincides with $\mathcal{C}$. This fact we write as $\mathcal{C} = \langle G \rangle$. Moreover, if matrix G has the minimum rank among all matrices generating code $\mathcal{C}$, then it is called the *generator* matrix of the code $\mathcal{C}$.

The vector $h = (h_1, \ldots, h_n) \in V_q^n$ is called *parity check* of the code $\mathcal{C}$, if for any vector $c = (c_1, \ldots, c_n) \in \mathcal{C}$ holds equality

$$h_1 \cdot c_1 + \ldots + h_n \cdot c_n = 0,$$

here all operations are performed in the field $GF(q)$. It is clear that the set of all parity checks of code $\mathcal{C}$ is a linear subspace of V_q^n, i.e. the linear code. This code is called the *dual* code to code $\mathcal{C}$. We denote the code dual to $\mathcal{C}$ as $\mathcal{C}^\perp$.

The generator matrix H of code $\mathcal{C}^\perp$ is called the *parity-check matrix* of code $\mathcal{C}$. Note that from the definition of the parity-check matrix H of code $\mathcal{C}$, it follows that for any $c \in \mathcal{C}$ holds the equalities

$$Hc^T = 0, \quad cH^T = 0.$$

The minimum distance(see [16]) of the linear code $\mathcal{C}$ is called the number

$$d_{\mathcal{C}} = \min_{c \in \mathcal{C},\ c \neq 0} \mathrm{wt}(c),$$

here $\mathrm{wt}(c)$ is the Hamming weight (the number of nonzero coordinates) of the vector c. The minimum distance of code $\mathcal{C}^\perp$, which is dual to code $\mathcal{C}$, is denoted as $d_{\mathcal{C}}^\perp$.

The Cartesian product of vectors $c = (c_1, \ldots, c_n) \in V_q^n$ and $b = (b_1, \ldots, b_m) \in V_q^m$ is called vector

$$c \times b = (c_1, \ldots, c_n, b_1, \ldots, b_m) \in V_q^{m+n}.$$

Accordingly, the *Cartesian product* $[n]_q$-code $\mathcal{C}$ and $[m]_q$-code $\mathcal{B}$ is called $[n+m]_q$-code $\mathcal{C} \times \mathcal{B}$ consisting of vectors

$$\mathcal{C} \times \mathcal{B} = \{c \times b | c \in \mathcal{C},\ b \in \mathcal{B}\}.$$

The concatenation $cat(\mathcal{C}_1, \ldots, \mathcal{C}_u)$ of codes $\mathcal{C}_1, \ldots, \mathcal{C}_u$ is called the set of codes $\mathcal{C}$, which are generated by a matrix of the form

$$(G_1 \| \ldots \| G_u),$$

here $\|$ is the concatenation of matrix columns, and the $(k \times n_i)$-matrix G_i generates the code $\mathcal{C}_i$, $i = 1, 2, \ldots, u$. It is clear that $\mathcal{C} \in cat(\mathcal{C}_1, \ldots, \mathcal{C}_u)$ is $[n_1 + \ldots + n_u]_q$-code.

Also, for any code $\mathcal{C} \in cat(\mathcal{C}_1, \ldots, \mathcal{C}_u)$, the following inclusion is true

$$\mathcal{C} \subseteq \mathcal{C}_1 \times \ldots \times \mathcal{C}_u.$$

Hadamard product of two vectors $c, b \in V_q^n$ is called the vector $c \circ b$ obtained as a result of the component-wise product of coordinates of these vectors:

$$c \circ b = (c_1, \ldots, c_n) \circ (b_1, \ldots, b_n) = (c_1 b_1, \ldots, c_n b_n).$$

Definition 1. *Let $\mathcal{C}$ and $\mathcal{B}$ are $[n]_q$-codes. Then* Hadamard product (Schur product, component-wise product) *$\mathcal{C} \circ \mathcal{B}$ of codes $\mathcal{C}$ and $\mathcal{B}$ will be called the $[n]_q$-code, consisting of the linear span of the following vectors $\{c \circ b | c \in \mathcal{C},\ b \in \mathcal{B}\}$. If $\mathcal{C} = \mathcal{B}$, then code $\mathcal{C} \circ \mathcal{C} = \mathcal{C}^2$ is called* Hadamard square *of code $\mathcal{C}$.*

For the Hadamard square of codes that are the concatenation of other codes, the following proposition is true.

Proposition 1. *Let $\mathcal{C} \in cat(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u)$ for some codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u$. Then the following inclusion is true*

$$\mathcal{C}^2 \subseteq \mathcal{C}_0^2 \times \mathcal{C}_1^2 \times \ldots \times \mathcal{C}_u^2. \tag{1}$$

We will be interested in the following problem. Under what condition the inclusion (1) turns into equality. The paper's main result is the following 1.

Theorem 1. *Let u be a positive integer, and for each $i = 0, 1, \ldots, u$ the code $\mathcal{C}_i$ be a $[n_i]_q$-code. Let also $[N, k]_q$-code $\mathcal{C} \in cat(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u)$.*

If $d_{\mathcal{C}}^{\perp} \neq 2$, $k \geq 4$, $N \leq \frac{k(k+1)}{2}$, $N \cdot \log_q(2 - q^{-1}) \leq \frac{k(k-3)}{2}$ and

$$N - \log_q \frac{3k+4}{4} \geq \dim \mathcal{C}_0^2 + \dim \mathcal{C}_1^2 + \ldots + \dim \mathcal{C}_u^2,$$

then we have

$$\mathcal{C}^2 = \mathcal{C}_0^2 \times \mathcal{C}_1^2 \times \ldots \times \mathcal{C}_u^2. \tag{2}$$

3 Hadamard square and quadratic forms

It turns out to be a convenient interpretation of the Hadamard square of the linear code with a point of view of quadratic forms over $GF(q)$. Such an approach allowed the authors of [3] to establish the behavior of the dimension of Hadamard square of a random linear code.

Definition 2. *A quadratic form over $GF(q)$ is called homogeneous quadratic polynomial over this field*

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

here $a_{i,j} \in GF(q), 1 \leq i < j \leq k$, и $b_i \in GF(q), 1 \leq i \leq k$.

Let denotes by $\mathcal{Q}_k(q)$ the set of all quadratic forms over $GF(q)$ in k variables. Consider a $(k \times n)$-matrix G, let $g_i \in V_q^k$ be the column of the matrix G with index i. Define a mapping $\ell_G : \mathcal{Q}_k(q) \to V_q^n$ in the following way:

$$\ell_G(f) = \big(f(g_1), \ldots, f(g_n)\big).$$

In this case, the Hadamard square of the linear $[n,k]_q$-code $\mathcal{C}$ generated by the matrix G is the image of the linear operator ℓ_G (see, for example, [3, 19]):

$$\mathcal{C}^2 = \operatorname{Im} \ell_G. \tag{3}$$

The following proposition attends directly from proposition 1.

Proposition 2. *Let $\mathcal{C} \in cat(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u)$ for some codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u$. Then we have*

$$\dim \mathcal{C}^2 = \dim \operatorname{Im} \ell_{(G_0\|G_1\|\ldots\|G_u)} \leq \sum_{i=0}^{u} \dim \operatorname{Im} \ell_{G_i}, \tag{4}$$

where $(G_0\|G_1\|\ldots\|G_u)$ is generator matrix of code $\mathcal{C}$.

Moreover, equality in (4) is achieved if and only if

$$\mathcal{C}^2 = \mathcal{C}_0^2 \times \mathcal{C}_1^2 \times \ldots \times \mathcal{C}_u^2.$$

Let $\ker \ell_G$ be a kernel of linear operator ℓ_G. Since $\dim \mathcal{Q}_k(q) = \frac{k(k+1)}{2}$, then the equality

$$\dim \operatorname{Im} \ell_G = \frac{k(k+1)}{2} - \dim \ker \ell_G$$

holds.

So the following proposition is true.

Proposition 3. *Let $\mathcal{C} \in cat(\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u)$ for some codes $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_u$. Then we have*

$$\dim \ker \ell_{(G_0\|G_1\|\ldots\|G_u)} \geq \frac{k(k+1)}{2} - \sum_{i=0}^{u} \dim \mathcal{C}_i^2, \tag{5}$$

where $(G_0\|G_1\|\ldots\|G_u)$ is generator matrix of code $\mathcal{C}$.

Moreover, equality in (5) is achieved if and only if

$$\mathcal{C}^2 = \mathcal{C}_0^2 \times \mathcal{C}_1^2 \times \ldots \times \mathcal{C}_u^2.$$

Proof. The proof follows from the equality

$$\dim \ker \ell_{(G_0\|G_1\|\ldots\|G_u)} = \frac{k(k+1)}{2} - \dim \operatorname{Im} \ell_{(G_0\|G_1\|\ldots\|G_u)},$$

and from proposition 2 given (3). □

4 The proof of main theorem

This section is devoted to the proof of the main results of the paper. Let us first establish the truth of the most general theorem.

Theorem 2. *Let X_i, $i = 0, \dots, u$, be $(k \times n_i)$-matrices over $GF(q)$. Matrix X_i, $i = 0, \dots, u$, generates linear code $\mathcal{C}_i$. Denote by $N = n_0 + n_1 + \dots + n_u$. Let $\mathcal{C}$ be $[N, k]_q$-code over $GF(q)$ generated by the matrix $X = (X_0 \| X_1 \| \dots \| X_u)$. Let us require that the matrix X does not contain identical columns.*

If $k \geq 4$, $N \leq \frac{k(k+1)}{2}$, $N \cdot \log_q(2 - q^{-1}) \leq \frac{k(k-3)}{2}$ and

$$N - \log_q \frac{3k+4}{4} \geq \dim \mathcal{C}_0^2 + \mathcal{C}_1^2 + \dots + \dim \mathcal{C}_u^2,$$

then we have

$$\mathcal{C}^2 = \mathcal{C}_0^2 \times \mathcal{C}_1^2 \times \dots \times \mathcal{C}_u^2.$$

Proof. At first, we prove the useful technical lemma.

Lemma 1. *Consider a discrete random variable ξ with a finite number of values $\{a_1, \dots, a_s\}$. Let p_i be the probability of occurrence of the value a_i. We will assume that a_1 is the minimum possible value of ξ. Let us denote by $\mathcal{M}\xi$ the mathematical expectation of the random variable ξ. If $\mathcal{M}\xi \leq a_1$, then for any i we have either $p_i = 0$, or $a_i = a_1$.*

Proof. Indeed, by definition

$$a_1 \geq \mathcal{M}\xi = \sum_{i=1}^{s} a_i p_i \Leftrightarrow a_1 \sum_{i=1}^{s} p_i \geq \sum_{i=1}^{s} a_i p_i \Leftrightarrow 0 \geq \sum_{i=1}^{s} (a_i - a_1) p_i.$$

Now $p_i \geq 0$ and $a_i - a_1 \geq 0$ for $i = 2, \dots, s$, since a_1 is minimum value of random variable ξ. Therefore $\sum_{i=1}^{s} (a_i - a_1) p_i = 0$. But it is only possible if for each $i = 2, \dots, s$, either $p_i = 0$ or $a_i = a_1$. □

Consider $\ker \ell_X$.

Let be given a uniform distribution on the set of $(k \times N)$-matrices $X = (X_0 \| \dots \| X_u)$, such that the matrix X has no zero columns and repeated columns. Then $\ker \ell_X$ will be a random variable defined on the set of random matrices X. According to proposition 3 holds the following inequality

$$\dim \ker \ell_X \geq \frac{k(k+1)}{2} - \sum_{i=0}^{u} \dim \mathcal{C}_i^2.$$

This means that if we prove that

$$\mathcal{M}\dim\ker\ell_X \leq \frac{k(k+1)}{2} - \sum_{i=0}^{u}\dim\mathcal{C}_i^2,$$

then from Lemma 1, it will follow that the random variable $\dim\ker\ell_X$ with nonzero probability can take only the value

$$\dim\ker\ell_X = \frac{k(k+1)}{2} - \sum_{i=0}^{u}\dim\mathcal{C}_i^2.$$

Therefore, according to proposition 3, the truth of the theorem will follow from this.

Thus, it is necessary to estimate the mathematical expectation of a random variable $\dim\ker\ell_X$. Now $|\ker\ell_X| = q^{\dim\ker\ell_X}$, therefore, we will estimate the mathematical expectation of the cardinality of $\ker\ell_X$. By definition $f\in\ker\ell_X$, if and only if $f(X_0) = f(X_1) = \ldots = f(X_u) = 0$.

Let I_f be a random variable that takes the value one if $f(X_0) = f(X_1) = \ldots = f(X_u) = 0$, and 0 in other cases. Then

$$|\ker\ell_X| = \sum_{f\in\mathcal{Q}_k(q)} I_f.$$

Since the mathematical expectation is linear, the following equality is true

$$\mathcal{M}|\ker\ell_X| = \sum_{f\in\mathcal{Q}_k(q)} \mathcal{M}I_f.$$

Notice that

$$\mathcal{M}I_f = 0\cdot\Pr\{I_f = 0\} + 1\cdot\Pr\{I_f = 1\}.$$

Therefore

$$\mathcal{M}|\ker\ell_X| = \sum_{f\in\mathcal{Q}_k(q)} \Pr\{I_f = 1\}.$$

Let for all $f\in\mathcal{Q}_k(q)$ holds the inequality

$$\Pr\{I_f = 1\} \leq q^{-\sum_{i=0}^{u}\dim\mathcal{C}_i^2}, \tag{6}$$

then

$$\mathcal{M}|\ker\ell_X| \leq |\mathcal{Q}_k(q)|\cdot q^{-\sum_{i=0}^{u}\dim\mathcal{C}_i^2}.$$

However, then, taking into account $|\ker\ell_X| = q^{\dim\ker\ell_X}$, for $\dim\ker\ell_X$, we get

$$\mathcal{M}\dim\ker\ell_X \leq \dim\mathcal{Q}_k(q) - \sum_{i=0}^{u}\dim\mathcal{C}_i^2.$$

Since $\dim \mathcal{Q}_k(q) = \frac{k(k+1)}{2}$, we get

$$\mathcal{M} \dim \ker \ell_X \leq \frac{k(k+1)}{2} - \sum_{i=0}^{u} \dim \mathcal{C}_i^2.$$

So, to prove the theorem, it is necessary to establish that the inequality (6) holds for any quadratic form f.

Consider the quadratic form f which takes the value 0 on the set of values X, $|X| = N$. Let its weight be w. Then there are $\binom{q^k-w}{N}$ options for choosing from set of arguments of subset $Y = X_0 \cup X_1 \cup \ldots \cup X_u$ of cardinality $N = n_0 + n_1 + \ldots + n_u$, on which form f takes 0. Then the fraction of such subsets Y among all possible subsets of cardinality N will be equal to $\binom{q^k-w}{N} / \binom{q^k}{N}$. This means that

$$\Pr\{I_f = 1 | wt(f) = w\} = \frac{\binom{q^k-w}{N}}{\binom{q^k}{N}}.$$

Then by the law of total probability

$$P = \Pr\{I_f = 1\} = \sum_{w=0}^{q^k} \Pr\{wt(f) = w\} \Pr\{I_f = 1 | wt(f) = w\}.$$

Suppose that f is chosen randomly and with equal probability from $\mathcal{Q}_k(q)$, then the probability $\Pr\{wt(f) = w\}$ can be calculated by the formula

$$\Pr\{wt(f) = w\} = \frac{Q_w}{q^{\dim \mathcal{Q}_k(q)}} = \frac{Q_w}{q^{k(k+1)/2}},$$

where Q_w is number of quadratic forms of weight w.

Then we get

$$P = \sum_{w=0}^{q^k} \frac{Q_w}{q^{k(k+1)/2}} \frac{\binom{q^k-w}{N}}{\binom{q^k}{N}} = \frac{1}{q^{k(k+1)/2}} \cdot \sum_{w=0}^{q^k} Q_w \frac{\binom{q^k-w}{N}}{\binom{q^k}{N}}. \tag{7}$$

Let

$$Q = \sum_{w=0}^{q^k} Q_w \frac{\binom{q^k-w}{N}}{\binom{q^k}{N}}.$$

Further, $Q_w \neq 0$ only for $w = 0, q^k - q^{k-1}, q^k - q^{k-1} - \tau q^{k-1-h}(q-1)$ where $h = 1, \ldots, \lfloor k/2 \rfloor$ and $\tau = 1, -1$ (see [14, 15, 21]).

So, the following fractions need to be estimated

$$\frac{\binom{q^{k-1}}{N}}{\binom{q^k}{N}}, \quad \frac{\binom{q^{k-1}+q^{k-1-h}(q-1)}{N}}{\binom{q^k}{N}}, \quad \frac{\binom{q^{k-1}-q^{k-1-h}(q-1)}{N}}{\binom{q^k}{N}}.$$

Lemma 2. *If* $0 < a < q$*,* $n > 0$ *and* $N > 0$*, then we have*

$$\frac{\binom{a\cdot q^{k-1}}{N}}{\binom{q^k}{N}} \le a^N q^{-N}.$$

Proof. Consider equalities

$$\frac{\binom{a\cdot q^{k-1}}{N}}{\binom{q^k}{N}} = \frac{(a\cdot q^{k-1})!(q^k-N)!}{(a\cdot q^{k-1}-N)!q^k!} = \prod_{i=1}^{N} \frac{a\cdot q^{k-1}-N+i}{q^k-N+i}.$$

Further,

$$\frac{a\cdot q^{k-1}-N+i}{q^k-N+i} = \frac{a\cdot q^{k-1}-q^k+q^k-N+i}{q^k-N+i} = 1-\frac{q^{k-1}(q-a)}{q^k-N+i}. \qquad (8)$$

Since $a < q$, the fraction $q^{k-1}(q-a)/(q^k-N+i)$ is not negative, so the smaller it is, the (8) is more. Thus, the maximum of expression (8) is reached at $i = N$.

For $1 \le i \le N$ we have

$$1-\frac{q^{k-1}(q-a)}{q^k-N-n+i} \le 1-\frac{q^{k-1}(q-a)}{q^k} = \frac{a}{q}.$$

Therefore

$$\frac{\binom{a\cdot q^{k-1}}{N}}{\binom{q^k}{N}} \le a^N q^{-N}.$$

□

Let a takes one of the values $1, 1 \pm q^{-h}(q-1)$, where $1 \le h \le \lfloor k/2 \rfloor$. Since $q \ge 1$, then $1+q^{-h}(q-1) > 0$. Further, for $h \ge 1$, the inequality $1-q^{-h}(q-1) \ge 1-q^{-1}(q-1) = q^{-1} > 0$ holds.

Hence, according to Lemma 2, we have

$$\frac{\binom{q^{k-1}}{N}}{\binom{q^k}{N}} \le q^{-N}, \quad \frac{\binom{q^{k-1}\pm q^{k-1-h}(q-1)}{N}}{\binom{q^k}{N}} \le q^{-N}(1\pm q^{-h}(q-1))^N.$$

Thus,

$$Q \le 1+q^{-N}Q^0+q^{-N}\sum_{h=1}^{\lfloor k/2 \rfloor}\left[Q_h^-(1+q^{-h}(q-1))^N+Q_h^+(1-q^{-h}(q-1))^N\right],$$

where $Q^0 = Q_{q^k-q^{k-1}}$, $Q_h^- = Q_{q^k-q^{k-1}-q^{k-1-h}(q-1)}$ and $Q_h^+ = Q_{q^k-q^{k-1}+q^{k-1-h}(q-1)}$. Since $1+q^{-h}(q-1) \ge 1-q^{-h}(q-1)$ for $h \ge 1$, then

$$Q \le 1+q^{-N}Q^0+q^{-N}\sum_{h=1}^{\lfloor k/2 \rfloor}\left[Q_h^-+Q_h^+\right](1+q^{-h}(q-1))^N. \qquad (9)$$

Let us estimate Q^0 and $Q_h^- + Q_h^+$ for $1 \le h \le \lfloor k/2 \rfloor$.

According to works [14, 15, 21], holds

$$Q_h^\pm = \frac{1}{2} q^{h^2} (q^h \mp 1) \frac{\prod_{i=k-2h+1}^{k} (q^i - 1)}{\prod_{i=1}^{h} (q^{2i} - 1)}.$$

First, note that $Q_h^+ \le Q_h^-$, so we only estimate Q_h^-.

Choose any ε, $k^{-1} \le \varepsilon \le \frac{1}{4}$. Then $1 \le \varepsilon k \le k/4$. Let $h \le \varepsilon \cdot k$. In this case $2h < k - 2h + 1$. Then we get

$$Q_h^- \le \frac{1}{2} q^{h^2} \frac{\prod_{i=k-2h+1}^{k} q^i}{(q^h - 1) \prod_{i=1}^{h-1} (q^{2i} - 1)} = \frac{1}{2} \frac{q^{h^2 + 2hk - h(2h-1)}}{(q^h - 1) \prod_{i=1}^{h-1} (q^{2i} - 1)}.$$

Now we use the inequality $q^x - 1 \ge q^{x-1}$, which is valid for any $x \ge 1$ and $q \ge 2$.

$$(q^h - 1) \cdot \prod_{i=1}^{h-1} (q^{2i} - 1) \ge q^{h-1} \cdot \prod_{i=1}^{h-1} q^{2i-1} = q^{h-1+2\sum_{i=1}^{h-1} i - \sum_{i=1}^{h-1} 1} = q^{h(h-1)}.$$

Then for $2 \le h \le \varepsilon \cdot k$ we get

$$Q_h^- \le \frac{1}{2} \cdot q^{h^2 + 2hk - h(2h-1) - h(h-1)} = \frac{1}{2} \cdot q^{2h(k+1-h)}.$$

Let us find the extremum of $\phi(h) = 2h(k+1-h)$. For $k + 1 \ge 2h$ derivative $\phi'(h) = 2(k+1-h) - 2h = 2(k+1-2h)$ is not negative, therefore $\phi(h)$ does not decrease on the interval $[1, (k+1)/2]$.

Hence, for $2 \le h \le \varepsilon \cdot k \le k/4 < (k+1)/2$ we get $2h(k+1-h) \le 2\varepsilon k(k+1-\varepsilon k) = 2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k$.

If $h = 1$, then

$$Q_1^- = \frac{1}{2} q(q+1) \frac{\prod_{i=k-1}^{k} (q^i - 1)}{\prod_{i=1}^{1} (q^{2i} - 1)} = \frac{1}{2} q(q+1) \frac{(q^k - 1)(q^{k-1} - 1)}{q^2 - 1} \le \frac{1}{2} \cdot q^{2k}.$$

Since $1 \le \varepsilon k$ and $\varepsilon < 1$, then $2k \le 2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k$.

Then for $k^{-1} \le \varepsilon \le \frac{1}{4}$ and $1 \le h \le \varepsilon k$ we get

$$Q_h^\pm \le \frac{1}{2} \cdot q^{2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k}.$$

Thus for $1 \le h \le \varepsilon k$ we get

$$Q_h^- + Q_h^+ \le q^{2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k}.$$

And for the remaining Q_h^-, $h > \varepsilon k$, and Q^0, we have the trivial inequalities

$$Q_h^- + Q_h^+ \leq q^{k(k+1)/2}, \quad Q^0 \leq q^{k(k+1)/2}.$$

Then from (9) for every $k^{-1} \leq \varepsilon \leq 4^{-1}$ implies

$$Q \leq 1+(1+(1/2-\varepsilon)k)q^{-N}q^{k(k+1)/2}+q^{-N}q^{2\varepsilon(1-\varepsilon)k^2+2\varepsilon k}\sum_{h\leq\varepsilon k}(1+q^{-h}(q-1))^N.$$

Notice that $1 + q^{-h}(q-1) \leq 2 - q^{-1} = \alpha_q$. Then

$$Q \leq 1 + (1 + (1/2 - \varepsilon)k)q^{-N}q^{k(k+1)/2} + \varepsilon \cdot k \cdot q^{-N}q^{2\varepsilon(1-\varepsilon)k^2+2\varepsilon k}\alpha_q^N.$$

Further, if $k \geq 4$, then

$$1 + \left(\frac{1}{2} - \varepsilon\right) k = 1 - \varepsilon k + \frac{k}{2} \leq \frac{k}{2}.$$

. Thus,

$$Q \leq 1 + \frac{k}{2}q^{-N}q^{k(k+1)/2} + \frac{k}{4}q^{-N(1-\log_q \alpha_q)}q^{2\varepsilon(1-\varepsilon)k^2+2\varepsilon k}. \tag{10}$$

Let us choose ε so that

$$\frac{k(k+1)}{2} - N \geq -N(1 - \log_q \alpha_q) + 2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k. \tag{11}$$

This is equivalent to the following inequality

$$N \log_q \alpha_q + (2\varepsilon(1-\varepsilon) - 1/2)\, k^2 + (2\varepsilon - 1/2)k \leq 0. \tag{12}$$

The left side of the inequality is the square polynomial of ε. Not so hard to prove that (12) holds on the union of intervals

$$\left(-\infty, \frac{1}{2} - \frac{\sqrt{k+1+2b-1}}{2k}\right] \bigcup \left[\frac{1}{2} + \frac{\sqrt{k+1+2b+1}}{2k}, +\infty\right),$$

where $b = N\log_q \alpha_q$. The second half-interval cannot contain points of the segment $[k^{-1}, 4^{-1}]$ since $4^{-1} < 2^{-1}$. Therefore, let us require that the second contains it. For this, it is enough that

$$k^{-1} \leq \frac{1}{2} - \frac{\sqrt{k+1+2N\log_q \alpha_q} - 1}{2k}.$$

The last is equivalent to

$$N \log_q \alpha_q \leq \frac{k(k-3)}{2}. \tag{13}$$

Thus, if (13) holds, then we have (11). From (11) and (10), the inequality follows

$$Q \leq 1 + \frac{3k}{2} q^{-N} q^{k(k+1)/2}.$$

But then from (7) we get an estimate for the probability

$$P \leq \frac{3k}{4} q^{-N} + q^{-k(k+1)/2}.$$

If $N \leq k(k+1)/2$ then $q^{-N} \geq q^{-k(k+1)/2}$, therefore we finally get

$$P \leq \frac{3k+4}{4} q^{-N}.$$

Then, to satisfy (6), it is necessary to require that

$$-N + \log_q \frac{3k+4}{4} \leq -\sum_{i=0}^{u} \dim \mathcal{C}_i^2 \Leftrightarrow N - \log_q \frac{3k+4}{4} \geq \sum_{i=0}^{u} \dim \mathcal{C}_i^2.$$

The theorem is completely proved. □

Now, to prove the main theorem 1, let us apply the statement of Theorem 2 to the generator matrix $G = (G_0 \| G_1 \| \dots \| G_u)$ of the code $\mathcal{C} \in cat(\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_u)$. The inequality $d_{\mathcal{C}}^{\perp} > 2$ guarantees that G does not contain identical columns. It is also by definition of set $cat(\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_u)$, for $i = 0, 1, \dots, u$ matrix G_i generates code $\mathcal{C}_i$.

5 Application to cryptanalysis of some post-quantum cryptographic mechanisms

Concatenated codes are sometimes used to construct post-quantum cryptographic mechanisms based on error-correcting codes.

So in work [20], it is proposed to construct the McEliece cryptosystem, use codes from the set $cat(\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_u)$, where C_i, $i = 0, 1, \dots, u$, is Reed–Muller code $RM(r, m)$.

An effective attack on this variant of the McEliece cryptosystem is proposed in [5]. In this case, for the attack to succeed, equality (2) must hold for code $\mathcal{C}$. The authors of the attack could only verify the equality (2) experimentally. Theorem 1 strictly allows proving this fact. So, for example, for the original parameters proposed in [20], $\dim \mathcal{C}_i^2 = \dim RM(6, 10) = 848,\ k = 176,\ N = 4 \cdot 1024 = 4096$, we get

$$4096 - \log_2 \frac{3 \cdot 176 + 4}{4} > 4096 - 8 = 4088 > 4 \cdot 848 = 3392,$$

which guarantees the success of the attack [5].

In [12], authors propose to build the cryptosystem based on codes from the family $cat(RM(r,m),\Gamma)$, where Γ is a binary Goppa code. Moreover, the codes $RM(r,m)$ and Γ are chosen so that their dimensions coincide. In [6], an attack on this cryptosystem is constructed in some adversary models. Among other things, the attack uses the fact of equality (2). Let 2^m is the length of $RM(r,m)$, n_1 is the length of Γ, and k is the dimension of these codes. Since it is not enough what is known about the Hadamard square of Γ, then we restrict its dimension to n_1. We get

$$2^m + n_1 - \log_2 \frac{3k+4}{4} \geq n_1 + \dim RM(2r,m).$$

So, if

$$\dim RM(2r,m) \leq 2^m - \log_2 \frac{3k+4}{4}, \tag{14}$$

then, in this case, it is possible to prove the efficiency of the attack from [6] rigorously. For example, for the code $RM(6,10)$, the inequality (14) holds since

$$848 \leq 1024 - \log_2 133 \approx 1016.$$

Note also the attack from [11], where the McEliece cryptosystem is constructed on the class of codes $cat(\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_u)$ for a more general case of choosing codes $\mathcal{C}_i$. The center point of attack is equality (2). The authors note that they have experimentally verified its implementation, including for non-binary codes. It turned out that it is almost always fulfilled. Theorem 1 substantiates the experimental data from work [11].

Finally, consider the attack from [17]. It is devoted to the McEliece cryptosystem built on the Reed–Muller code $RM(r,m)$, in which random coordinates are added to each codeword so that the code's linearity is preserved. In Section 5.2 in Remark 1, the authors note that they experimentally established the following fact. If we add t random coordinates to the code $RM(r,m)$, then the Hadamard square of the new code $\mathcal{B}$ will have the dimension

$$\dim \mathcal{B}^2 = \dim RM(2r,m) + t.$$

Theorem 1 allows us to prove this fact. So code $\mathcal{B}$ can be considered a code from the family $cat(RM(r,m),\mathcal{C})$, where $\mathcal{C}$ is generated by a submatrix containing only added random columns of generator matrix of $\mathcal{B}$. However then the length of $\mathcal{C}$ is equal to t, therefore $\dim \mathcal{C}^2 \leq t$. It means that if the inequality (14) holds, then Theorem 1 implies the equality

$$\dim \mathcal{B}^2 = \dim RM(2r,m) + \dim \mathcal{C}^2.$$

It remains only to note that based on Theorem 2.2 of the article [3] for random linear codes with high probability $\dim \mathcal{C}^2 = t$. Moreover, for instance, when the set of added columns has the maximum rank t, then $\dim \mathcal{C}^2 = t$ with probability 1.

6 Conclusion remarks

The main theorem allows us to conclude that for some types of cryptographic mechanisms, the use of concatenation of codes from different classes instead of one class of codes, generally speaking, does not increase the cryptographic strength of the mechanism.

The authors hope that using the proven fact that the Hadamard square of the concatenated code is equal to the Cartesian product of Hadamard squares of the code-components, it will be possible to clarify several known attacks and build new attacks on post-quantum code-based cryptographic mechanisms.

This work was partially supported by the Russian Foundation for Basic Research under grant no. 18-29-03124.

References

[1] M. Bardet, M. Bertin, A. Couvreur, A. Otmani, "Practical Algebraic Attack on DAGS", *Code-Based Cryptography*, Lecture Notes in Computer Science, Springer International Publishing, Cham, 2019, 86-101.

[2] M. A. Borodin, I. V. Chizhov, "Effective attack on the McEliece cryptosystem based on Reed–Muller codes", *Diskr. Mat.*, **26**:1 (2014), 10–20; *Discrete Math. Appl.*, **24**:5 (2014), 273–280.

[3] I. Cascudo, R. Cramer, D. Mirandola, G. Zémor, "Squares of Random Linear Codes", *IEEE Transactions on Information Theory*, **61**:3 (2015), 1159-1173.

[4] H. Chen, R. Cramer, C. Dwork, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields", *Advances in cryptology - CRYPTO 2006*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, 521–536.

[5] I. Chizhov, S. Koniukhov, A. Davletshina, "Effective structural attack on McEliece-Sidelnikov public-key cryptosystem", *International Journal of Open Information Technologies*, **8**:7 (2020), 1–10, In Russian.

[6] I. Chizhov, E. Popova, "Structural attack on McEliece-Sidelnikov type public-key cryptosystem based on a combination of random codes with Reed-Muller codes", *International Journal of Open Information Technologies*, **8**:6 (2020), 24–33, In Russian.

[7] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, J.-P. Tillich, "Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes", *Des. Codes Cryptogr*, **73** (2014), 641–666.

[8] A. Couvreur, I. Márquez-Corbella, R. Pellikaan, "Cryptanalysis of Public-Key Cryptosystems That Use Subcodes of Algebraic Geometry Codes", *Coding Theory and Applications*, CIM Series in Mathematical Sciences, Springer International Publishing, Cham, 2015, 133-140.

[9] A. Couvreur, A. Otmani, J.-P. Tillich, "Polynomial Time Attack on Wild McEliece Over Quadratic Extensions", *IEEE Transactions on Information Theory*, **63**:1 (2017), 404-427.

[10] A. Couvreur, A. Otmani, J.-P. Tillich, V. Gauthier–Umaña, “A Polynomial-Time Attack on the BBCRS Scheme”, *Public-Key Cryptography – PKC 2015*, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2015, 175-193.

[11] V. M. Deundyak, Y. V. Kosolapov, “On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes”, *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)* (2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)), 2019, 143-148.

[12] E. Egorova, G. Kabatiansky, E. Krouk, C. Tavernier, “A new code-based public-key cryptosystem resistant to quantum computer attacks”, *J. Phys.: Conf. Ser.*, **1163** (2019), 012061.

[13] J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret, J.-P. Tillich, “A Distinguisher for High-Rate McEliece Cryptosystems”, *IEEE Transactions on Information Theory*, **59**:10 (2013), 6830-6844.

[14] S. Li, “On the weight distribution of second order Reed–Muller codes and their relatives”, *Designs, Codes and Cryptography*, **87**:10 (2019), 2447-2460.

[15] R. J. McEliece, “Quadratic forms over finite fields and second-order Reed-Muller codes”, *JPL Space Programs Summary*, **3** (1969), 37–58.

[16] F. J. McWilliams, N. J. A. Sloane, *The theory of error-correcting codes. I and II.*, North-Holland mathematical library; v. 16, North-Holland Pub. Co., North Holland, New York, 1977.

[17] A. Otmani, H. Kalachi, “Square Code Attack on a Modified Sidelnikov Cryptosystem”, *Codes, Cryptology, and Information Security*, Lecture Notes in Computer Science, Springer International Publishing, 2015, 173–183.

[18] R. Pellikaan, “On decoding by error location and dependent sets of error positions”, *Discrete Mathematics*, **106–107** (1992), 369-381.

[19] H. Randriambololona, “An Upper Bound of Singleton Type for Componentwise Products of Linear Codes”, *IEEE Transactions on Information Theory*, **59**:12 (2013), 7936-7939.

[20] V. M. Sidel’nikov, “Open coding based on Reed–Muller binary codes”, *Diskr. Mat.*, **6**:2 (1994), 3–20; *Discrete Math. Appl.*, **4**:3 (1994), 191–207.

[21] N. Sloane, E. Berlekamp, “Weight enumerator for second-order Reed-Muller codes”, *IEEE Transactions on Information Theory*, **16**:6 (1970), 745–751.

[22] C. Wieschebrink, “Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes”, *Lecture Notes in Computer Science*, **6061 LNCS** (2010), 61–72.