The Hadamard square of concatenated linear codes

The 10th Workshop on Current Trends in Cryptology (CTCrypt'2021)

Ivan Chizhov[1], Alexandra Davletshina[2]

[1]Lomonosov Moscow State University, JSC «NPK Kryptonite», Federal Research Center «Informatics and Control» of Russian Academy of Science, Russia

[2]JSC «InfoTeCS», Russia

June 4, 2021

The Hadamard Product

The main theorem and its applications

Definitions

- Let V_q^n be the linear space of all vectors of length n over $GF(q)$.
- Block linear $[n, k]_q$-code C is a k-dimensional linear subspace 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 $C \subseteq V_q^n$ is not essential to us, it will be called the $[n]_q$-code C.
  Vectors $c \in C$ are called codewords of the code C.
- The $[n]_q$-code C is generated by the $(k \times n)$-matrix G with elements from $GF(q)$ if the linear span of the rows of the matrix G over $GF(q)$ coincides with C.
  This fact we write as $C = \langle G \rangle$.
  If matrix G has the minimum rank among all matrices generating code C, then it is called the generator matrix of the code C.

The Cartesian product

Definition

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

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

Definition

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

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

The Hadamard product

Definition

The 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

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

Applying the Hadamard product

- The Hadamard product was first introduced in the paper
  R.Pellikaan, On decoding by error location and dependent sets of error positions, Discrete Mathematics, 106107 (1992), 369-381.
  The Hadamard product was used for the constructing of error-correcting algebraic decoders for some linear codes.
- *C. Wieschebrink, Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, Lecture Notes in Computer Science, 6061 LNCS (2010), 6172.*
  proposes to use the Hadamard product to construct algebraic attacks on code-based public-key cryptosystems. The first algebraic attack on Niederreiter public-key cryptosystem based on some special subcodes of the Reed–Solomon is introduced.

Applying the Hadamard product

- *M. A. Borodin, I. V. Chizhov, Effective attack on the McEliece cryptosystem based on Reed–Muller codes, Diskr. Mat., 26:1 (2014), 1020; Discrete Math. Appl., 24:5 (2014), 273280.*
  proposes the first polynomial attack on McEliece cryptosystem based on Reed–Muller codes.
- *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, 173183.*
  proposes the first attack on the McEliece public-key cryptosystem based on modified Reed-Muller codes

Applying the Hadamard product

- *A. Couvreur, I. Marquez-Corbella and R. Pellikaan, "Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes,"in IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 5404-5418, Aug. 2017, doi: 10.1109/TIT.2017.2712636.* introduces the first square code attack on the McEliece public-key cryptosystem based on algebraic geometry codes.

The code's concatenation

Definition

The concatenation $cat(C_1, \ldots, C_u)$ of codes $C_1, \ldots, C_u$ is called the set of codes 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 C_i, $i = 1, 2, \ldots, u$. It is clear that
$C \in cat(C_1, \ldots, C_u)$ is $[n_1 + \ldots + n_u]_q$-code.
Also, for any code $C \in cat(C_1, \ldots, C_u)$, the following inclusion is true

$$C \subseteq C_1 \times \ldots \times C_u.$$

The Hadamard product and PKC based on concatenated codes

- *I. Chizhov, S. Koniukhov, A. Davletshina, Effective structural attack on McEliece-Sidelnikov public-key cryptosystem, International Journal of Open Information Technologies, 8:7 (2020), 110, In Russian.* The first effective algebraic attack on McEliece-Sidelnikov public-key cryptosystem is proposed. This attack uses the Hadamard square of linear concatenated codes.

The Hadamard product and PKC based on concatenated codes

- *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), 2433, In Russian.* The algebraic attack in some model of adversary on McEliece-Sidelnikov public-key cryptosystem based on concatenation of random linear codes is proposed.
- *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.*
  The conception of attack on McEliece-Sidelnikov public-key cryptosystem based on concatenation of linear codes from various classes is described.

The main result

Proposition

Let $C \in \mathsf{cat}(C_0, C_1, \ldots, C_u)$ *for some codes* $C_0, C_1, \ldots, C_u$. *Then the following inclusion is true*

$$C^2 \subseteq C_0^2 \times C_1^2 \times \ldots \times C_u^2. \tag{1}$$

All previous attacks require (1) to turn into equality.

We will try to answer this question: under what condition the inclusion (1) turns into equality?

The main theorem

Theorem

Let u be a positive integer, and for each $i = 0, 1, \ldots, u$ the code C_i be a $[n_i]_q$-code. Let also $[N, k]_q$-code $C \in \mathsf{cat}(C_0, C_1, \ldots, C_u)$. If $k \geqslant 4$, $N \leqslant \frac{k(k+1)}{2}$, $N \cdot \log_q(2 - q^{-1}) \leqslant \frac{k(k-3)}{2}$, for every pair of coordinate there is a code word of C for which these coordinates are different, and

$$N - \log_q \frac{3k+4}{4} \geqslant \dim C_0^2 + \dim C_1^2 + \ldots + \dim C_u^2,$$

then we have

$$C^2 = C_0^2 \times C_1^2 \times \ldots \times C_u^2. \tag{2}$$

McEliece–Sidel'nikov public-key cryptosystem

- *V. M. Sidelnikov, Open coding based on ReedMuller binary codes, Diskr. Mat., 6:2 (1994), 320; Discrete Math. Appl., 4:3 (1994), 191207* introduces McEliece public-key cryptosystem based on a code from the set $cat(C_0, C_1, \ldots, C_u)$, where C_i, $i = 0, 1, \ldots, u$, — Reed–Muller codes $RM(r, m)$.
- *I. Chizhov, S. Koniukhov, A. Davletshina, Effective structural attack on McEliece-Sidelnikov public-key cryptosystem, International Journal of Open Information Technologies, 8:7 (2020), 110, In Russian* describes effective structural attack on this public-key cryptosystem. In this case, it is necessary that the code C satisfies the equality (2).

Application of main theorem

The main theorem allows us to prove (2) for RM-codes. For example, in case of Sidel'nikov's original parameters, $u = 3,\ k = 176,\ n = 1024$, we get

$$\dim C_i^2 = \dim RM(6, 10) = 848,\ k = 176,\ N = 4 \cdot 1024 = 4096.$$

The main inequality of theorem holds:

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

This ensures that the attack succeeds.

Kabatiansky–Tavernier public-key cryptosystem

- *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*
  introduces McEliece public-key cryptosystem based on a code from the set $cat(RM(r, m), \Gamma)$, here Γ — binary Goppa codes. Moreover, the code Γ is chosen so that the dimension of it and the dimension or $RM(r, m)$ coincide.
- *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), 2433, In Russian*
  proposes the algebraic attack in some model of adversary on this cryptosystem.

The attack works for codes for which equality is achieved in (2).

Kabatiansky–Tavernier public-key cryptosystem

Let 2^m be length of code $RM(r, m)$, n_1 be length of code Γ, and k be dimension of these codes.
It holds the following trivial inequality for dimension of Hadamard square of Goppa codes:

$$\dim \Gamma^2 \leqslant n_1.$$

Then we get

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

So if

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

hence, the equality is achieved in (2), then the attack will work for any binary Goppa code.
For example, the inequality (3) holds for code $RM(3, 10)$, because

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

McEliece public-key cryptosystem based on modified Reed–Muller codes

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, 173183 proposes a square code attack on McEliece public-key cryptosystem based on linear code, obtained from Reed-Muller code $RM(r, m)$ by adding random coordinates to each codeword linearity code is preserved.
In the section 5.2, remark 1, authors write: "...we observed experimentally that (..) is always true, and the upper-bound given in (..) is always reached, that is to say":

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

here $\mathcal{B}$ is linear code obtained from Reed-Muller code $RM(r, m)$ by adding t random coordinates.

McEliece public-key cryptosystem based on modified Reed–Muller codes

We can consider $\mathcal{B}$ as a linear code from a family $cat(RM(r, m), C)$, where the code C is generated by submatrix consisting from random columns of $\mathcal{B}$'s generator matrix.
Therefore, C has length t, and $\dim C^2 \leqslant t$.
This means that if the inequality (3) holds, then the main theorem implies the following equality:

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

Based on Theorem 2.2 of the article *I. Cascudo, R. Cramer, D. Mirandola, G. Zemor, Squares of Random Linear Codes, IEEE Transactions on Information Theory, 61: 3 (2015), 1159-1173* for random codes $\dim C^2 = t$ with high probability.
In the case when the set of added columns has the maximum rank t, then $\dim C^2 = t$ with probability 1.

Thank You for your attention!

Please, your questions.

Outline of the proof of the main theorem

Theorem

Let X_i, $i = 0, \ldots, u$, be $(k \times n_i)$-matrices over $GF(q)$. Matrix X_i, $i = 0, \ldots, u$, generates linear code C_i. Denote by $N = n_0 + n_1 + \ldots + n_u$. Let C be $[N, k]_q$-code over $GF(q)$ generated by the matrix $X = (X_0 \| X_1 \| \ldots \| X_u)$. Let us require that the matrix X does not contain identical columns. If $k \geqslant 4$, $N \leqslant \frac{k(k+1)}{2}$, $N \cdot \log_q(2 - q^{-1}) \leqslant \frac{k(k-3)}{2}$ and

$$N - \log_q \frac{3k+4}{4} \geqslant \dim C_0^2 + C_1^2 + \ldots + \dim C_u^2,$$

then we have

$$C^2 = C_0^2 \times C_1^2 \times \ldots \times C_u^2.$$

Quadratic forms

Definition

A quadratic form over $GF(q)$ is called homogeneous quadratic polynomial over this field

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

here $a_{i,j} \in GF(q), 1 \leqslant i < j \leqslant k,\ b_i \in GF(q), 1 \leqslant i \leqslant k$.
Let denotes by $Q_k(q)$ the set of all quadratic forms over $GF(q)$ in k variables.

Quadratic forms

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 $\ell_G : Q_k(q) \to V_q^n$ 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 C generated by the matrix G is the image of the linear operator ℓ_G:

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

Quadratic forms

Proposition

Let $C \in \mathsf{cat}(C_0, C_1, \ldots, C_u)$ for some codes $C_0, C_1, \ldots, C_u$. Then we have

$$\dim \ker \ell_{(G_0 \| G_1 \| \ldots \| G_u)} \geqslant \frac{k(k+1)}{2} - \sum_{i=0}^{u} \dim C_i^2, \tag{4}$$

where $(G_0 \| G_1 \| \ldots \| G_u)$ is generator matrix of code C.
Moreover, equality in (4) is achieved if and only if

$$C^2 = C_0^2 \times C_1^2 \times \ldots \times C_u^2.$$

Reduction to evaluating mat. expectation of one random variable

estimate the mathematical expectation of a random variable Let be given a uniform distribution on the set of $(k \times N)$-matrices $X = (X_0 \| \ldots \| X_u)$, 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. If we prove that

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

here $\mathcal{M}$ is the mathematical expectation of a random variable, then the random variable $\dim \ker \ell_X$ with nonzero probability can take only the value

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

Therefore, the truth of the theorem will follow from this.

Evaluating mat. expectation of one random variable

Next, we estimate $\mathcal{M}|\ker \ell_X|$.
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

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

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

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

Notice that

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

Therefore

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

Evaluating mat. expectation of one random variable

Let for all $f \in Q_k(q)$ holds the inequality

$$\Pr\{I_f = 1\} \leqslant q^{-\sum_{i=0}^{u} \dim C_i^2}, \tag{5}$$

then

$$M|\ker \ell_X| \leqslant |Q_k(q)| \cdot q^{-\sum_{i=0}^{u} \dim C_i^2}.$$

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

$$M \dim \ker \ell_X \leqslant \dim Q_k(q) - \sum_{i=0}^{u} \dim C_i^2.$$

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

$$M \dim \ker \ell_X \leqslant \frac{k(k+1)}{2} - \sum_{i=0}^{u} \dim C_i^2.$$

So, to prove the theorem, it is necessary to establish that the inequality (5) holds for any quadratic form f.

Evaluating of probability

Let Q_w be number of quadratic forms of weight w. Then by the formula of total probability

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

Fix some $k^{-1} \leqslant \varepsilon \leqslant \frac{1}{4}$. The following proposition can be proved using the known weight spectrum of quadratic forms over $GF(q)$:

$$P \leqslant q^{-k(k+1)/2} + \frac{k}{2} q^{-N} + \frac{k}{4} q^{-N(1-\log_q \alpha_q)} q^{2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k - k(k+1)/2}.$$

Let us choose a so that the conditions

$$-N \geqslant -N(1 - \log_q(2 - q^{-1})) + 2\varepsilon(1-\varepsilon)k^2 + 2\varepsilon k - \frac{k(k+1)}{2}.$$

Evaluating of probability

First, there is such ε if $N \log_q(2 - q^{-1}) \leqslant \frac{k(k-3)}{2}$.
Second, for such ε, we obtain the following estimate for the probability

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

Now, if $N \leqslant k(k+1)/2$, then $q^{-N} \geqslant q^{-k(k+1)/2}$, so we finally get

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

Then, to satisfy the desired inequality, it should be required that

$$-N + \log_q \frac{3k+4}{4} \leqslant -\sum_{i=0}^{u} \dim C_i^2 \Leftrightarrow N - \log_q \frac{3k+4}{4} \geqslant \sum_{i=0}^{u} \dim C_i^2. \square$$