COMPUTATIONAL MATHEMATICS

MSC 39A60 **DOI: 10.14529/jcem180202**

ON THE BERGER – LOIDREAU CRYPTOSYSTEM ON THE TENSOR PRODUCT OF CODES

V. M. Deundyak[1,2]***,*** vl.deundyak@gmail.com***,***
Yu. V. Kosolapov[1]***,*** itaim@mail.ru***.***
[1] Southern Federal University, Rostov-on-Don, Russian Federation***.***
[2] FGNU NII "Specvuzavtomatika", Rostov-on-Don, Russian Federation***.***

In the post-quantum era, asymmetric cryptosystems based on linear codes (code cryptosystems) are considered as an alternative to modern asymmetric cryptosystems. However, the research of the strength of code McEliece-type cryptosystems shows that algebraically structured codes do not provide sufficient strength of these cryptosystems. On the other hand, the use of random codes in such cryptosystems is impossible because of the high complexity of its decoding. Strengthening of code cryptosystems is currently conducted, usually, either by using codes for which no attacks are known, or by modifying the cryptographic protocol. In this paper both of these approaches are used. On the one hand, it is proposed to use the tensor product $C^1 \otimes C^2$ of the known codes C^1 and C^2, since for $C^1 \otimes C^2$ in some cases it is possible to construct an effective decoding algorithm. On the other hand, instead of a McEliece-type cryptosystem, it is proposed to use its modification, a Berger – Loidreau cryptosystem. The paper proves a high strength of the constructed code cryptosystem to attacks on the key even in the case when code cryptosystems on codes C^1 and C^2 are cracked.

Keywords: the Berger – Loidreau cryptosystem; the tensor product of codes; the attack on the key.

Introduction

In the basis of many cryptographic protocols which provide the confidentiality and/or integrity of data in the process of protocol execution lays the use of numerical asymmetric cryptosystems. For instance GOST P 34.10-2012, RSA, El-Gamal cryptosistem and more. The security of these cryptosystems is based on the one way trapdoor functions. In particular, the security of cryptosystems GOST R 34.10-2012 and El-Gamal is based on the complexity of discrete logarithm in a finite group, and the security of RSA is related to the complexity of factorization of large integers. According to [1], due to the constant growth of computing capabilities, to provide acceptable resilience, the size of the keys used in these cryptosystems should increase every year. However, increasing the size of the key leads to an increase in the complexity of encryption and decryption. Moreover, as follows from [2], for cryptoalgorithms based on complexity of factorization of integers and on the complexity of discrete logarithm, there are theoretically effective attacks based on quantum computing. In connection with the development of quantum computing, an alternative to such numerical asymmetric cryptosystems can be asymmetric code cryptosystems [3], for instance, McEliece-type ones [4]. This assumption can be justified. In fact, Grover's quantum algorithm is effective for numerical cryptosystems

and reinforces the attack on the ciphertext of the McEliece cryptosystem, nevertheless its complexity depends exponentially on the n is a length of code underlying the McEliece cryptosystem [5]. It should be noted that cryptosystems based on the McEliece are not widely used in practice in the connection with the large size of their keys in comparison with numerical cryptosystems, the strength of which is now considered sufficient. In addition to high strength to breaking on quantum computers, encryption and decryption operations of code cryptosystems are faster than similar operations of numerical cryptosystems. In particular, a comparison of the hardware implementation of the McEliece cryptosystem on Goppa codes with the hardware implementation of RSA-1024 in [6] showed that the encryption and decryption operations of the code cryptosystem are faster by 20 and 2.5 times, respectively. Moreover, the encryption and decryption of the code cryptosystem processes 50 and 30 respectively times more clear text bits than RSA-1024 [6].

Historically, the first code cryptosystem is the McEliece cryptosystem, which he proposed in 1978 (see [4]). By now, many McEliece-type cryptosystems have been extensively explored. Also, some weak classes of linear codes are known. It means that McEliece-type cryptosystems based on such codes are vulnerable to attacks on the key – structural attacks. In particular, in [8] - [10] effective algorithms of structural attacks are constructed in the case when cryptosystem is based on Reed – Solomon codes. In [11], [12] such algorithms are found in the case when cryptosystem is based on Reed – Muller codes. In a number of works, in order to increase the strength to attacks on the key, it is proposed to modify the cryptographic protocol (see [13], [14]). In particular, in [13] T. Berger and P. Loidreau proposed a method of enhancing the strength of McEliece-type cryptosystem. The main idea of the method is to use randomly selected subcode instead of error correcting code. The weakness of the Berger – Loidreau system is shown in the case of Reed – Solomon codes in [10], and in the particular case of Reed – Muller codes in [15].

The results of [8] - [15] show that not any code may be used in McEliece-type or Berger – Loidreau-type cryptosystems. Instead of searching for new codes for a McEliece-type cryptosystem, it is possible to use codes based on known codes. For example, in [16] it is suggested to use the induced codes in McEliece-type cryptosystems and in [17] it is suggested to use tensor product of codes, which is a generalization of induced codes. In these works, the high strength to key attacks on such McEliece-type cryptosystems is shown. Using of such code constructions is also justified by the fact that there are effective decoders for them [18], [17]. The present article is a continuation of the [16], [17] and is devoted to the investigation of the possibility of using the tensor product of codes in code cryptosystems of the Berger – Loidreau-type.

The definition of the tensor product of codes and the corresponding cryptosystem of Berger – Loidreau-type are described in the first section.The second section is devoted to the analysis of the strength of this cryptosystem. A third section is devoted to some examples.

1. The Berger – Loidreau System Based on the Tensor Product

In this section the McEliece-type and the Berger – Loidreau-type code cryptosystems are defined, known structural attacks on these cryptosystems are described and new Berger – Loidreau-type cryptosystem based on the tensor product of codes is constructed.

We shall use the basic of coding theory (see [7]). Let C be $[n, k, d]$-code of length n, of dimension k with code distance d over the Galois field $\mathbb{F}_q$ and let G be the generator matrix of this code. The linear span generated by the rows of the matrix M will be denoted by $\mathcal{L}(M)$; in particular, $\mathcal{L}(G) = C$. We also need the $\text{Gauss}_{m',m}$ algorithm, which uses $(m' \times m)$ matrix Γ of rank $s(\leq m')$ and finds the $(s \times m')$ matrix Z such that $\mathcal{L}(Z\Gamma) = \mathcal{L}(\Gamma)$. The Hamming's weight of vector $\mathbf{e}$ will be denoted as $\text{wt}(\mathbf{e})$.

1.1. McEliece-type Cryptosystem

Under the McEliece-type cryptosystem based on $[n, k, d]$-code C we mean an analogue of an asymmetric cryptosystem described in [4]. In this cryptosystem the public key $\mathbf{k}_{\text{pub}}$ is a pair $(\widetilde{G}, t = \lfloor (d-1)/2 \rfloor)$, and the secret key $\mathbf{k}_{\text{sec}}$ is a pair of matrices (S, P): S is a random matrix from the set of nonsingular $(k \times k)$ matrices $\text{GL}(k, \mathbb{F})$, P is a random matrix from the set of permutational $(n \times n)$ matrices MP_n, and $\widetilde{G} = SGP$. The encryption rule for an arbitrary message $\mathbf{s}(\in \mathbb{F}_q^k)$ has the form:

$$\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}, \tag{1}$$

where $\text{wt}(\mathbf{e}) \leq t$. For decryption $\mathbf{z}$ the secret key $\mathbf{k}_{\text{sec}}$ is used:

$$\mathbf{s} = \text{Dec}_C(\mathbf{z}P^{-1})S^{-1}, \tag{2}$$

where $\text{Dec}_C : \mathbb{F}_q^n \to \mathbb{F}_q^k$ – decoder of the code C. Further such cryptosystem will be denoted by $\text{McE}(C)$.

1.2. Berger – Loidreau-type Cryptosystem

Let $\text{GL}(k' \times k; \mathbb{F}_q)$ be the set of $(k' \times k)$-matrices of rank k' over $\mathbb{F}_q$. The public key $\mathbf{k}_{\text{pub}}$ in Berger – Loidreau-type cryptosystem based on $[n, k, d]$-code C is the pair $(\widetilde{G}, t = \lfloor (d-1)/2 \rfloor)$, and a secret key $\mathbf{k}_{\text{sec}}$ is the pair (H, P), where H is randomly chosen matrix from $\text{GL}(k' \times k; \mathbb{F}_q)$, P is randomly chosen matrix from MP_n, $\widetilde{G} = HGP$. The rule for encryption of an arbitrary message $\mathbf{s}(\in \mathbb{F}_q^{k'})$ has the form (1), and for decryption $\mathbf{z}$ the next rule is used:

$$\mathbf{s} = \text{Dec}_C(\mathbf{z}P^{-1})H^{\text{inv}}, \tag{3}$$

where H^{inv} is right inverse matrix, i.e. $(k \times k')$-matrix such that $H \cdot H^{\text{inv}} = I_{k'}$ is the identity matrix of rank k'. Further Berger – Loidreau-type system will be denoted by $\text{BL}_{k'}(C)$.

1.3. On the Structural Attacks on Cryptosystems $\text{McE}(C)$ and $\text{BL}_{k'}(C)$

Strength of cryptosystems $\text{McE}(C)$ and $\text{BL}_{k'}(C)$ depends on the underlying code C. For example, if the C is a Reed – Solomon code, then effective structural attacks on the corresponding cryptosystems are constructed in [8] and [10]. In the case of using the Reed – Muller code such attacks are constructed in [12], [15]. Note that in structural attacks cryptanalyst usually finds not the original secret key, but *suitable* one as in the case of McEliece-type cryptosystems. Recall that the automorphism group of the $[n, k, d]$-code C with the generator matrix G is the set PAut of permutation $(n \times n)$-matrices $\hat{P}$ for each of which there is a nonsingular $(k \times k)$-matrix R' such that [7]

$$R'G = G\hat{P}. \tag{4}$$

Note that if the automorphism group of the $[n, k]$ – code C is nontrivial and $\widetilde{G} = HGP$ is public key of the Berger – Loidreau-type cryptosystem, then there is more then one pair of matrices $(H', P') \in \mathrm{GL}(k', k, \mathbb{F}) \times \mathrm{MP}_n$, such that

$$\widetilde{G} = H'GP'. \tag{5}$$

Let

$$\mathcal{K}(C, \widetilde{G}) = \{(H', P') \in \mathrm{GL}(k', k, \mathbb{F}) \times \mathrm{MP}_n : \widetilde{G} = H'GP'\}. \tag{6}$$

Suitable key (H', P') for decryption is applied in accordance with the rule (3), where instead of P the matrix P' is used, and instead of H matrix H' is.

Remark 1. It is known (see [8]) if $\mathrm{rank}(H) = \mathrm{rank}(G)$, (H, P) is secret key, and (H', P') is suitable secret key, then

$$PP'^{-1} \in \mathrm{PAut}(C). \tag{7}$$

It was noted above that the cryptosystem $\mathrm{BL}_{k'}(C)$ for some codes was broken [10], [15]. Further we will assume that there is an algorithm of structural attack $\mathrm{Attack}_{k'}^{C}$ with complexity $Q^C(k')$, which can found a suitable secret key (H', P') for cryptosystem $\mathrm{BL}_{k'}(C)$. Since $1 \le k' \le k$, then for the family of cryptosystems $\{\mathrm{BL}_{k'}(C)\}_{1 \le k' \le k}$ it is conveniently to consider a family of structural attack algorithms

$$\mathcal{A}(C) = \{\mathrm{Attack}_{k'}^{C}\}_{1 \le k' \le k}. \tag{8}$$

In Section 1.5, a new code Berger – Loidreau-type cryptosystem will be constructed on the basis of the tensor product of two codes C^1 and C^2, and in Section 2 we investigate the strength of this cryptosystem in the strong assumption that there are effective attacks of (8) type on the Berger – Loidreau-type cryptosystems constructed on the codes C^1, C^2.

1.4. Tensor Product of Codes

Further $(l \times m)$-matrix $A = (a_{i,j})_{i=0,\ldots,l-1;\ j=0,\ldots,m-1}$ will be written in row form: $A = (\mathbf{a}_i)_{i=0}^{l-1}$. Under the tensor product $A \otimes B$ for $(k_1 \times n_1)$-matrix $A = (a_{i,j}) = (\mathbf{a}_i)_{i=0}^{k_1-1}$ and $(k_2 \times n_2)$-matrix $B = (\mathbf{b}_i)_{i=0}^{k_2-1}$ we mean as usual a matrix of the form:

$$A \otimes B = \begin{pmatrix} a_{0,0}B & \ldots & a_{0,n-1}B \\ a_{1,0}B & \ldots & a_{1,n-1}B \\ \ldots & \ldots & \ldots \\ a_{k-1,0}B & \ldots & a_{k-1,n-1}B \end{pmatrix} = \begin{pmatrix} \mathbf{a}_0 \otimes B \\ \mathbf{a}_1 \otimes B \\ \ldots \\ \mathbf{a}_{k_1-1} \otimes B \end{pmatrix}. \tag{9}$$

It is known (see [19]) that one can uniquely define such permutation matrices $P_l \in \mathrm{MP}_{k_1k_2}$ and $P_r \in \mathrm{MP}_{n_1n_2}$, depending only on dimensions of the matrices A and B, which

$$A \otimes B = P_l(B \otimes A)P_r. \tag{10}$$

Let C^i be $[n_i, k_i, d_i]$-code, $G^i = (\mathbf{g}_j^i)_{j=0}^{k_i-1}$ is generator matrix of the code C^i, $i \in \{1, 2\}$. Consider the tensor product of the codes C^1 and C^2 i.e. the $[n_1n_2, k_1k_2, d_1d_2]$-code $C^1 \otimes C^2$ with generator matrix $G^1 \otimes G^2$ [20]:

$$G^1 \otimes G^2 = \begin{pmatrix} g_{0,0}^1 G^2 & \ldots & g_{0,n_1-1}^1 G^2 \\ g_{1,0}^1 G^2 & \ldots & g_{1,n_1-1}^1 G^2 \\ \ldots & \ldots & \ldots \\ g_{k_1-1,0}^1 G^2 & \ldots & g_{k_1-1,n-1}^1 G^2 \end{pmatrix}. \tag{11}$$

Codes C^1 and C^2 will be referred to as multiplier codes. Note that the constructing of an effective decoding algorithm (with polynomial complexity) for the code $C^1 \otimes C^2$ is a special independent problem. For example, in the case when C^1 and C^2 are MLD -codes, the problem of constructing such algorithms is considered in [17],[18]. It is further assumed that for the code $C^1 \otimes C^2$ there is an effective decoding algorithm

$$\mathrm{Dec}_{C^1 \otimes C^2} : \mathbb{F}^{n_1+n_2} \to \mathbb{F}^{k_1+k_2}.$$

Note that if $A_0, ..., A_{n_1-1} \in \mathrm{PAut}(C^2)$ are different, then in the general case

$$\mathrm{diag}(A_0, ..., A_{n_1-1}) \notin \mathrm{PAut}(C^1 \otimes C^2). \tag{12}$$

1.5. Cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$

Let us define the Berger – Loidreau-type cryptosystem based on the code $C^1 \otimes C^2$. The secret key $\mathbf{k}_{\mathrm{sec}}$ is a pair of matrices (H, P), where H is randomly chosen from $\mathrm{GL}(k', k_1k_2, \mathbb{F})$, $k' < k_1k_2$, P is randomly chosen from $\mathrm{MP}_{n_1n_2}$, and the public key is a pair $(\widetilde{G}, t = \lfloor (d_1d_2 - 1)/2 \rfloor)$, where

$$\widetilde{G} = H \cdot (G^1 \otimes G^2) \cdot P. \tag{13}$$

The encryption rule for an arbitrary message $\mathbf{s}(\in \mathbb{F}^{k'})$ has the form:

$$\mathbf{z} = \mathbf{s}\widetilde{G} + \mathbf{e}, \mathrm{wt}(\mathbf{e}) \leq t. \tag{14}$$

The decryption rule is following: $\mathbf{s} = \mathrm{Dec}_{C^1 \otimes C^2}(\mathbf{z}P^{-1})H^{\mathrm{inv}}$.

2. The Strength of $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ to Structural Attacks

Consider the cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ with the secret key (H, P) and the public key (13) where the generator matrix $G^1 \otimes G^2$ of the code $C^1 \otimes C^2$ has the form (11). In this section the strength of this cryptosystem to structural attacks is analyzed. It is naturally to assume that the cryptanalysts knows families $\mathcal{A}(C^1)$ and $\mathcal{A}(C^2)$ of effective attack algorithms (8). Such strong adversary model is also used in [16] and [17]. Note that in the case when C^i is a Reed – Solomon code, the family $\mathcal{A}(C^i)$ of effective attack algorithms can be constructed in accordance with [10]. For the case when C^i is a Reed – Muller code, such a family can be constructed, for example, using the results of the paper [15].

2.1. Analysis of the Public Key Structure

We represent the $(k' \times k_1k_2)$-matrix H in the form:

$$H = \left(\widehat{H}_0 \,\middle|\, ... \,\middle|\, \widehat{H}_{k_1-1} \right), \tag{15}$$

where $\widehat{H}_i$ is $(k' \times k_2)$-matrix, consisting of columns of the matrix H with numbers from ik_2 to $(i+1)k_2 - 1$. Then from (11) we get:

$$H \cdot (G^1 \otimes G^2) = \left(\mathbf{\Gamma}_0 \,\middle|\, ... \,\middle|\, \mathbf{\Gamma}_{n_1-1}, \right), \mathbf{\Gamma}_i = \widetilde{\mathbf{H}}_i G^2, \;\; \widetilde{\mathbf{H}}_i = \sum_{j=0}^{k_1-1} \widehat{H}_j g^1_{j,i}. \tag{16}$$

It is easy to verify that the following set of permutation $(n_1n_2 \times n_1n_2)$-matrices

$$\Theta(n_2, n_1) = \{(M \otimes I_{n_2})\mathrm{diag}(D_1, ..., D_{n_1}) | M \in \mathrm{MP}_{n_1}, D_i \in \mathrm{MP}_{n_2}, i = 1, ..., n_1\}. \quad (17)$$

is a subgroup of the group $\mathrm{MP}_{n_1n_2}$, $|\Theta(n_2, n_1)| = (n_2!)^{n_1}n_1!$. For an arbitrary permutation matrix P from the group $\mathrm{MP}_{n_1n_2}$ by the symbol $\Theta(n_2, n_1)P$ we denote the coset $\{QP : Q \in \Theta(n_2, n_1)\}$ of $\mathrm{MP}_{n_1n_2}/\Theta(n_2, n_1)$. Any matrix from $\Theta(n_2, n_1)P$ will be called the representative of this coset. Let Ω_{n_2,n_1} be the set of representatives of all cosets:

$$\Omega_{n_2,n_1} = \{P_1, ..., P_{N_{n_1,n_2}}\},\ N_{n_1,n_2} = \frac{(n_1n_2)!}{(n_2!)^{n_1}n_1!}, \quad (18)$$

i.e. $\mathrm{MP}_{n_1n_2} = \cup_{P \in \Omega_{n_2,n_1}} \Theta(n_2, n_1)P$ and $\Theta(n_2, n_1)P_i \cap \Theta(n_2, n_1)P_j = \varnothing$ for $i \neq j$. Note that for large n_1n_2 the problem of constructing the set Ω_{n_2,n_1} can be computationally difficult. One of the possible algorithms for constructing representatives of factor classes is MakeRepresentatives.

Data: $\mathrm{MP}_{n_1n_2}$, $\Theta(n_2, n_1)$
Result: Ω_{n_2,n_1} – set of representatives of factor-set classes $\mathrm{MP}_{n_1n_2}/\Theta(n_2, n_1)$
1. $\Omega_{n_2,n_1} = \varnothing$
2. **while** $|\Omega_{n_2,n_1}| < N_{n_1,n_2}$ **do**
  Arbitrary generate a matrix $P' \in \mathrm{MP}_{n_1n_2}$
  if $P' \notin \Theta(n_2, n_1)$ *u* $PQ^{-1} \notin \Theta(n_2, n_1)\ \forall Q \in \Omega_{n_2,n_1}$ **then**
    $\Omega_{n_2,n_1} = \Omega_{n_2,n_1} \cup \{P'\}$
  end if
end while
return Ω_{n_2,n_1}

Algorithm 1: MakeRepresentatives

Using the Stirling formula we get

$$|\Omega_{n_2,n_1}| = \frac{(n_1n_2)!}{(n_2!)^{n_1}n_1!} \approx \left(\frac{e}{\sqrt{2\pi n_2}}\right)^{n_1} \sqrt{n_2}(n_1^{n_1})^{n_2-1} \geq \left(\frac{1}{\sqrt{n_2}}\right)^{n_1-1} (n_1^{n_1})^{n_2-1}.$$

Since $n_2 < 2^{2n_2}$, then

$$|\Omega_{n_2,n_1}| \geq \left(\frac{1}{\sqrt{n_2}}\right)^{n_1-1} (n_1^{n_1})^{n_2-1} \geq \frac{(n_1^{n_1})^{n_2-1}}{2^{n_2(n_1-1)}}. \quad (19)$$

Let π_M be the permutation acting on the set $\{0, ..., n_1 - 1\}$ that corresponds to the permutation matrix $M(\in \mathrm{MP}_{n_1})$, i.e. π_M is a permutation such that for the matrix $X = (\mathbf{x}^0, ..., \mathbf{x}^{n_1-1})$, where $\mathbf{x}^i$ – vector-column, the following equality holds:

$$X \cdot M = (\mathbf{x}^{\pi_M(0)}, ..., \mathbf{x}^{\pi_M(n_1-1)}).$$

Next we need the following technical lemma.

Lemma 1. *Let the matrix $\widetilde{G}$ has the form* (13), $L = VP$, $V \in \Theta(n_2, n_1)$. *Then*
1) there are matrices $M \in \mathrm{MP}_{n_1}, D_i \in \mathrm{MP}_{n_2}, i = 1, ..., n_1$, such that

$$\widetilde{G}L^{-1} = \left(\mathbf{\Gamma}_{\pi_M(0)}D_0 \,\middle|\, ... \,\middle|\, \mathbf{\Gamma}_{\pi_M(n_1-1)}D_{n_1-1} \right), \quad (20)$$

where $\mathbf{\Gamma}_i$ *has the form* (16)*;*

2) if (20) *satisfied and* P_l *and* P_r *are such permutation matrices, that* $G^1 \otimes G^2 = P_l(G^2 \otimes G^1)P_r$*, then there are matrices* $\widetilde{\mathbf{H}}'_i$ *of rank not exceeding* k_1 *such that*

$$\widetilde{G}L^{-1}(\mathrm{diag}(D_0^{-1}, ..., D_{n_1-1}^{-1}))P_r^{-1} = \left(\mathbf{\Gamma}'_0 \,\middle|\, ... \,\middle|\, \mathbf{\Gamma}'_{n_2-1} \right), \tag{21}$$

where $\mathbf{\Gamma}'_i = \widetilde{\mathbf{H}}'_i G^1 M$*.*

Proof.

Let us prove the first statement. Since (13) we get

$$\widetilde{G}L^{-1} = \widetilde{G}P^{-1}V^{-1} = H \cdot (G^1 \otimes G^2)V^{-1}. \tag{22}$$

As $V^{-1} \in \Theta(n_2, n_1)$, then for some $M \in \mathrm{MP}_{n_1}$, $D_i \in \mathrm{MP}_{n_2}$, $i = 0, ..., n_1 - 1$ we have $V^{-1} = (M \otimes I_{n_2})\mathrm{diag}(D_0, ..., D_{n_1-1})$ due to (17). From (22) we get:

$$\widetilde{G}L^{-1} =$$

$$H \cdot (G^1 \otimes G^2)(M \otimes I_{n_2})\mathrm{diag}(D_0, ..., D_{n_1-1}) \overset{(a)}{=} H \cdot (G^1 M \otimes G^2)\mathrm{diag}(D_0, ..., D_{n_1-1}) \overset{(b)}{=} \tag{23}$$

$$=(\mathbf{\Gamma}_{\pi_M(0)} \,|\, ... \,|\, \mathbf{\Gamma}_{\pi_M(n_1-1)})\mathrm{diag}(D_0, ..., D_{n_1-1}) \overset{(c)}{=} (\mathbf{\Gamma}_{\pi_M(0)}D_0 \,|\, ... \,|\, \mathbf{\Gamma}_{\pi_M(n_1-1)}D_{n_1-1}), \tag{24}$$

where the equality (a) follows from the properties of the tensor product of matrices, (b) follows from (16) and the fact that matrix $H \cdot (G^1 M \otimes G^2)$ differs from $H \cdot (G^1 \otimes G^2)$ in that in the first matrix the columns of G^1 are permuted in accordance with M, and the equality (c) follows from the block-diagonal form of the matrix $\mathrm{diag}(D_0, ..., D_{n_1-1})$.

Now we prove the second assertion. It is not difficult to derive directly from (20) the following equality:

$$\widetilde{G}L^{-1}(\mathrm{diag}((D_0)^{-1}, ..., (D_{n_1-1})^{-1}))P_r^{-1} = HP_l(G^2 \otimes G^1 M).$$

We express the matrix HP_l in column form: $HP_l = \left(\widehat{H}'_0 \,\middle|\, ... \,\middle|\, \widehat{H}'_{k_2-1} \right)$. Then

$$HP_l(G^2 \otimes G^1 M) = \left(\mathbf{\Gamma}'_0 \,\middle|\, ... \,\middle|\, \mathbf{\Gamma}'_{n_2-1} \right), \mathbf{\Gamma}'_i = \widetilde{\mathbf{H}}'_i G^1 M,\ \widetilde{\mathbf{H}}'_i = \sum_{j=0}^{k_2-1} \widehat{H}'_j g^2_{j,i}.$$

In each matrix $\widehat{H}'_j$ exactly k_1 columns, therefore the rank of $\widetilde{\mathbf{H}}'_i$ does not exceed k_1.

□

2.2. Finding a Suitable Key

On the basis of the observations made in the previous section we reduce the cryptanalysis of the system on the tensor product of codes to the cryptanalysis of systems on the code-multipliers.

2.2.1. Cryptanalysis by Code-multiplier C^2

Consider the matrix $\widetilde{G}$ of the public key (see (13)). Below we will assume that a cryptanalyst knows the matrix L from the coset $\Theta(n_2, n_1)P$, however, the matrix P

is unknown. Then from lemma 1, there are such matrices $M \in \mathrm{MP}_{n_1}$, $D_i \in \mathrm{MP}_{n_2}$, $i = 1, ..., n_1$, that the equality (20) is holds. But like P these matrices are not known too.

We transform the blocks from the right side of this equality (20) in such a way that we can apply algorithms from the family $\mathcal{A}(C^2)$ (see (8)). To do this we consider the matrix $\mathbf{\Gamma}_i = \widetilde{\mathbf{H}}_i G^2$, $i \in \{0, ..., n_1 - 1\}$ (see (16)). As $\mathrm{rank}(G^2) = k_2$ and in the matrix $\widetilde{\mathbf{H}}_i$ exactly k_2 columns, then from these observations we get that $\mathrm{rank}(\mathbf{\Gamma}_i) \leq k_2$. If we use the permutation π_M acting on the set $\{0, ..., n_1 - 1\}$ and the corresponding permutation matrix $M(\in \mathrm{MP}_{n_1})$, then we get:

$$k^{2,i} := \mathrm{rank}(\mathbf{\Gamma}_{\pi_M(i)} D_i) \leq k_2. \tag{25}$$

Let us consider $(k' \times n_2)$-matrix $\mathbf{\Gamma}_{\pi_M(i)} D_i$ from (20). By the (25), using an algorithm Gauss_{k',n_2} (see the begining of section 1), it is not difficult to construct a $(k^{2,i} \times k')$-matrix X_i, that $\mathrm{rank}(X_i \mathbf{\Gamma}_{\pi_M(i)} D_i) = k^{2,i}$. Let be $\widetilde{G}^{2,i} = X_i \mathbf{\Gamma}_{\pi_M(i)} D_i$, $H^{2,i} = X_i \widetilde{\mathbf{H}}_i$, then

$$\widetilde{G}^{2,i} = H^{2,i} G^2 D_i, \;\; \mathrm{rank}(H^{2,i}) = k^{2,i}. \tag{26}$$

Let us note that the matrix (26), which is a transformed block from the right side of equality (20), is a public key of the cryptosystem $\mathrm{BL}_{k^{2,i}}(C^2)$. Therefore, an algorithm $\mathrm{Attack}^{C^2}_{k^{2,i}}$ from the family $\mathcal{A}(C^2)$ can be applied to the matrix $\widetilde{G}^{2,i}$:

$$(\hat{H}^{2,i}, \hat{D}_i) = \mathrm{Attack}^{C^2}_{k^{2,i}}(\widetilde{G}^{2,i}). \tag{27}$$

Remark 2. Further, in the case when the matrices M and M' of the same rank m generate the same space, two notations $\mathrm{Attack}^{C^2}_m(M)$ and $\mathrm{Attack}^{C^2}_m(M')$ will be considered equivalent. For example, we will consider notations $\mathrm{Attack}^{C^2}_{k^{2,i}}(\widetilde{G}^{2,i})$ and $\mathrm{Attack}^{C^2}_{k^{2,i}}(\mathbf{\Gamma}_{\pi_M(i)} D_i)$ as equivalent, since the matrix $\widetilde{G}^{2,i}$ is obtained from $\mathbf{\Gamma}_{\pi_M(i)} D_i$ by linear combination of rows and the ranks of these matrices coincide.

Lemma 2. *Consider the public key matrix $\widetilde{G} = HGP$ which has a form* (13)*. Suppose that the matrix $L \in \Theta(n_2, n_1)P$, for which the representation* (20) *is satisfied. Then*

1) permutation matrices $\hat{D}_0$,...,$\hat{D}_{n_1-1}$ can be found such that

$$\widetilde{G} L^{-1} \mathrm{diag}(\hat{D}_0^{-1}, ..., \hat{D}_{n_1-1}^{-1}) = \left(\mathbf{\Gamma}_{\pi_M(0)} A_0 \;\middle|\; ... \;\middle|\; \mathbf{\Gamma}_{\pi_M(n_1-1)} A_{n_1-1} \right), \tag{28}$$

where M and $\mathbf{\Gamma}_{\pi_M(i)}$ – unknown matrices from (20)*, and $A_i = D_i \hat{D}_i^{-1}$, $i = 0, ..., n_1 - 1$;*

2) for each $i = 0, ..., n_1 - 1$ one can calculate the rank $\widetilde{\mathbf{H}}_{\pi_M(i)}$ from the (16)*;*

3) if for some i the equality $\mathrm{rank}(\widetilde{\mathbf{H}}_{\pi_M(i)}) = k_2$ holds, then $A_i \in \mathrm{PAut}(C^2)$.

Proof.

First we prove the first statement. The matrices $\hat{D}_i$ we can get as a result of the action of the attacks (27). To complete the proof of the lemma, it suffices to use the equality (23).

Due to the fact that $\mathrm{rank}(G^2) = k_2$, rank of the matrix $\widetilde{\mathbf{H}}_{\pi_M(i)}$ is equal to the rank of the matrix $\mathbf{\Gamma}_{\pi_M(i)} = \widetilde{\mathbf{H}}_{\pi_M(i)} G^2$. The matrix A_i is, as follows from the first statement of the lemma, permutation matrix, therefore the ranks of the matrices $\mathbf{\Gamma}_{\pi_M(i)}$ and $\mathbf{\Gamma}_{\pi_M(i)} A_i$ coincide. So $\mathrm{rank}(\widetilde{\mathbf{H}}_{\pi_M(i)}) = \mathrm{rank}(\mathbf{\Gamma}_{\pi_M(i)} A_i)$ and this rank can be calculated by applying to the matrix $\mathbf{\Gamma}_{\pi_M(i)} A_i$ the method of sequential elimination.

Now we prove the third statement. As $\operatorname{rank}(\widetilde{\mathbf{H}}_i) = k_2$, then $\operatorname{rank}(\mathbf{\Gamma}_i) = k_2$ and, consequently, for the submatrix $\mathbf{\Gamma}_{\pi_M(i)}D_i$ in the presentation of (20) the equality $\operatorname{rank}(\mathbf{\Gamma}_{\pi_M(i)}D_i) = k_2$ holds. Therefore from (7) we get that $D_i\hat{D}_i^{-1} \in \operatorname{PAut}(C^2)$, where $\hat{D}_i$ is permutation matrix obtained from the attack $\operatorname{Attack}_{k_2}^{C^2}$ on the matrix $\mathbf{\Gamma}_{\pi_M(i)}D_i$. □

We note that in the case of cryptanalysis by the multiplier C^2, in place of the unknown matrices $D_0, ..., D_{n_1-1}$, in the general case there are other matrices $\hat{D}_0, ..., \hat{D}_{n_1-1}$. However, these matrices in some cases help to advance in cryptanalysis in two variables. In the following paragraphs, we will consider situations in which the matrix

$$\operatorname{diag}(A_0, ..., A_{n_1-1}) = \operatorname{diag}(D_0\hat{D}_0^{-1}, ..., D_{n_1-1}\hat{D}_{n_1-1}^{-1}) \tag{29}$$

belongs to or does not belong to the group $\operatorname{PAut}(\mathcal{L}(G^1M \otimes G^2))$.

2.2.2. Cryptanalysis by C^1 in the Case of $\operatorname{diag}(A_0, ..., A_{n_1-1}) \in \operatorname{PAut}(\mathcal{L}(G^1M \otimes G^2))$

Recall that the cryptanalyst knows the matrix $L \in \Theta(n_2, n_1)P$, for which (20) is satisfied. In the previous section, the goal of cryptanalysis with respect to the multiplier C^2 was to obtain information about unknown matrices $D_0, ..., D_{n_1-1}$. Now let's try to use cryptanalysis by C^1 in the particular case and get information about the matrix M, and then get suitable key (H', P').

Suppose that $\operatorname{diag}(A_0, ..., A_{n_1-1}) \in \operatorname{PAut}(\mathcal{L}(G^1M \otimes G^2))$. This is done for example in the case when

$$\forall i, j : i \neq j \;\; D_i\hat{D}_i^{-1} = D_j\hat{D}_j^{-1}, \;\; D_i\hat{D}_i^{-1} \in \operatorname{PAut}(C^2).$$

By (4) for $\operatorname{diag}(A_0, ..., A_{n_1-1})$ there is a $(k_1k_2 \times k_1k_2)$-matrix R, that

$$H(G^1M \otimes G^2)\operatorname{diag}(A_0, ..., A_{n_1-1}) = HR(G^1M \otimes G^2). \tag{30}$$

We note that in (30) matrices H, M and $\operatorname{diag}(A_0, ..., A_{n_1-1})$ are unknown. If one can find such a matrix $\hat{M}$, that $M\hat{M}^{-1} \in \operatorname{PAut}(C^1)$, then, as will be shown below in the proof of Theorem 1, matrix $HR(G^1M \otimes G^2)(\hat{M}^{-1} \otimes I_{n_2})$ will be the generator matrix for some subcode of the code $C^1 \otimes C^2$. Therefore in this case a matrix H' can be found from equation

$$H'(G^1 \otimes G^2) = HR(G^1M \otimes G^2)(\hat{M}^{-1} \otimes I_{n_2}).$$

Below we show how to find the matrix $\hat{M}$. From (30) and (10) we get:

$$H(G^1M \otimes G^2)\operatorname{diag}(A_0, ..., A_{n_1-1})P_r^{-1} = HRP_l(G^2 \otimes G^1M).$$

Represent HRP_l as a concatenation $(\widehat{H}''_0|...|\widehat{H}''_{k_2-1})$ (see (15)), then

$$H(G^1M \otimes G^2)\operatorname{diag}(A_0, ..., A_{n_1-1})P_r^{-1} = HRP_l(G^2 \otimes G^1M) = \left(\mathbf{\Gamma}''_0 \;\middle|\; ... \;\middle|\; \mathbf{\Gamma}''_{n_2-1} \right), \tag{31}$$

where by analogy with (16): $\mathbf{\Gamma}''_i = \widetilde{\mathbf{H}}''_i G^1M$, $\widetilde{\mathbf{H}}''_i = \sum_{j=0}^{k_2-1} \widehat{H}''_j g^2_{j,i}$.

Let $k^{1,i} = \operatorname{rank}(\mathbf{\Gamma}''_i)$, $i = 0, ..., n_2 - 1$. By analogy with the way it was done in Section 2.2.1 in preparation for the use of cryptoalgorithm $\operatorname{Attack}_{k^{2,i}}^{C^2}$, we will construct $(k^{1,i} \times k')$-matrix Y_i, such that $\operatorname{rank}(Y_i\mathbf{\Gamma}''_i) = k^{1,i}$, and denote $\widetilde{G}^{1,i} = Y_i\mathbf{\Gamma}''_i$, $H^{1,i} = Y_i\widetilde{\mathbf{H}}''_i$. Then

$$\widetilde{G}^{1,i} = H^{1,i}G^1M, \;\; \operatorname{rank}(H^{1,i}) = k^{1,i} \tag{32}$$

(cf (26)). Note that the matrix (32) is a public key of the cryptosystem $\mathrm{BL}_{k^{1,i}}(C^1)$. Therefore, an algorithm $\mathrm{Attack}^{C^1}_{k^{1,i}}(\in \mathcal{A}(C^1))$ can be applied to this matrix (see remark 2):

$$(\hat{H}^{1,i}, \hat{M}) = \mathrm{Attack}^{C^1}_{k^{1,i}}(\widetilde{G}^{1,i}) = \mathrm{Attack}^{C^1}_{k^{1,i}}(\mathbf{\Gamma}''_i).$$

Remark 3. If in (31) there is no submatrix $\mathbf{\Gamma}''_i$ with rank k_1, then some permutation matrix $\hat{M}$ can be found using an algorithm from the family $\mathcal{A}(C^1)$. However, for this matrix condition $M\hat{M}^{-1} \in \mathrm{PAut}(C^2)$ as a equality (a) in (33) may not be fulfilled.

In the particular case when the matrix $\mathrm{diag}(A_0, ..., A_{n_1-1})$ belongs to the automorphism group of a code with a generator matrix $G^1M \otimes G^2$, to find a suitable secret key we construct an algorithm SimpleAttackTensorBL. The input of this algorithm is the public key $\widetilde{G}$ and a set representatives of coset classes Ω_{n_2,n_1}, constructed using an algorithm MakeRepresentatives. It is assumed that the algorithm MakeRepresentatives is performed by the cryptanalyst in advance. If the input of the algorithm $\mathrm{Attack}^{C}_{k'}$ is a matrix that can not be represented in the form (5), then the output of the algorithm will be an error message $\perp$. The output of the algorithm SimpleAttackTensorBL is the pair (H', P'), which, as proved below, is a suitable secret key of $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ with a public key $(\widetilde{G}, t)$.

Theorem 1. *Let C^i is $[n_i, k_i, d_i]$-code, $i = 1, 2$, $\widetilde{G}$ is public key of the form (13) for $\mathrm{BL}_{k'}(C^1 \otimes C^2)$, Ω_{n_2,n_1} is set of representatives of the factor set $\mathrm{MP}_{n_1n_2}/\Theta(n_2, n_1)$, $\mathrm{diag}(A_0, ..., A_{n_1-1}) \in \mathrm{PAut}(\mathcal{L}(G^1M \otimes G^2))$ and in the form (31) there is at least one submatrix $\mathbf{\Gamma}''_i$ with rank k_1. Then: 1) in the set Ω_{n_2,n_1} there exists a unique matrix L, for which the conditions of the lemma 1 are satisfied; 2) if for the matrix $L(\in \Omega_{n_2,n_1})$ the conditions of the lemma 1 are satisfied, then the algorithm $\mathrm{SimpleAttackTensorBL}(\widetilde{G}, \Omega_{n_2,n_1})$ finds the suitable secret key and the complexity of the algorithm* SimpleAttackTensorBL *is $\mathcal{O}\left(\frac{(n_1n_2)!}{(n_2!)^{n_1}n_1!}\right)$.*

Proof.

The existence of the matrix L for which condition (20) is satisfied follows from the definition of Ω_{n_2,n_1}. Let us prove uniqueness. Suppose that there exists a $\widetilde{L} \neq L$ from Ω_{n_2,n_1}, that condition (20) holds, i.e there are such matrices $\widetilde{M} \in \mathrm{MP}_{n_1}, \widetilde{D}_0, ..., \widetilde{D}_{n_1} \in \mathrm{MP}_{n_2}$, that

$$\widetilde{G}\widetilde{L}^{-1} = \left(\mathbf{\Gamma}_{\pi_{\widetilde{M}}(0)}\widetilde{D}_0 \,\middle|\, ... \,\middle|\, \mathbf{\Gamma}_{\pi_{\widetilde{M}}(n_1-1)}\widetilde{D}_{n_1-1} \right).$$

From the proof of the first statement of the lemma 1 we get that the matrices L and $\widetilde{L}$ belong to the same coset of $\mathrm{MP}_{n_1n_2}/\Theta(n_2, n_1)$, which contradicts the definition of Ω_{n_2,n_1}.

Let us prove the second assertion. Since for $L(\in \Omega_{n_2,n_1})$ the condition of the lemma 1 is satisfied, then the matrix $\widetilde{G}'$ in algorithm SimpleAttackTensorBL has the form (20). Therefore, by lemma 2 such permutation matrices $\hat{D}_0, ..., \hat{D}_{n_1-1}$ can be found, that for $\widetilde{G}'\mathrm{diag}(\hat{D}_0^{-1}, ..., \hat{D}_{n_1-1}^{-1}) = \widetilde{G}L^{-1}\mathrm{diag}(\hat{D}_0^{-1}, ..., \hat{D}_{n_1-1}^{-1})$ the representation (28) holds. Since $\mathrm{diag}(A_0, ..., A_{n_1-1}) \in \mathrm{PAut}(\mathcal{L}(G^1M \otimes G^2))$ then there exists such nonsingular $(k_1k_2 \times k_1k_2)$-matrix R, that the equality (30) holds. Therefore, the matrix $\widetilde{G}'' = (\ \mathbf{G}'_0 \,|\, ... \,|\, \mathbf{G}'_{n_2-1}\ )$ in the algorithm SimpleAttackTensorBL has the form (31), i.e. $\mathbf{G}'_i = \mathbf{\Gamma}''_i$. Note that the blocks $\mathbf{G}'_i = \widetilde{\mathbf{H}}''_i G^1M$ for different i can have a different rank. By the hypothesis of the theorem there is a block $\mathbf{G}'_r$ of rank k_1 in the form (31). Therefore the permutation matrix $\hat{M}$ from

Data: $\widetilde{G}$, Ω_{n_2,n_1}
Result: (H', P') – suitable secret key
$\mathbf{k}'_{\text{sec}} = \perp$ //suitable secret key
for each $L \in \Omega_{n_2,n_1}$ **do**
present the matrix $\widetilde{G}' = \widetilde{G}L^{-1}$ in the form of concatenation of n_1 submatrices of size $(k' \times n_2)$ each:

$$\widetilde{G}' = \left(\mathbf{G}_0 \,\middle|\, ... \,\middle|\, \mathbf{G}_{n_1-1} \right),\ k'_{2,i} = \text{rank}(\mathbf{G}_i),\ i \in \{0, ..., n_1 - 1\}$$

if $\text{Attack}^{C^2}_{k'_{2,i}}(\mathbf{G}_i) \neq \perp$ *for all* $i \in \{0, ..., n_1 - 1\}$ **then**
$(\hat{H}^{2,i}, \hat{D}_i) = \text{Attack}^{C^2}_{k'_{2,i}}(\mathbf{G}_i),\ i \in \{0, ..., n_1 - 1\}$
$\widetilde{G}'' = \widetilde{G}'\text{diag}(\hat{D}_0^{-1}, ..., \hat{D}_{n_1-1}^{-1})P_r^{-1}$
Matrix $\widetilde{G}''$ represent as a concatenation of n_2 submatrices of size $(k' \times n_1)$ each:

$$\widetilde{G}'' = \left(\mathbf{G}'_0 \,\middle|\, ... \,\middle|\, \mathbf{G}'_{n_2-1} \right),\ k'_{1,j} = \text{rank}(\mathbf{G}'_j),\ j \in \{0, ..., n_2 - 1\}$$

if $\text{Attack}^{C^1}_{k'_{1,j}}(\mathbf{G}'_j) \neq \perp$ *for all* $j \in \{0, ..., n_2 - 1\}$ **then**
if *There is a* $r \in \{0, ..., n_2 - 1\}$, *that* $k'_{1,r} = k_1$ **then**
$(\hat{H}^{1,r}, \hat{M}) = \text{Attack}^{C^1}_{k'_{1,r}}(\mathbf{G}'_r)$
$P' = (\hat{M} \otimes I_{n_2})\text{diag}(\hat{D}_0, ..., \hat{D}_{n_1-1})L$
if *the equation* $H'(G^1 \otimes G^2) = \widetilde{G}P'^{-1}$ *has a solution* **then**
From equation $H'(G^1 \otimes G^2) = \widetilde{G}P'^{-1}$ find H'
$\mathbf{k}'_{\text{sec}} = (H', P')$
Exit the cycle
end if
end if
end if
end if
end for
return $\mathbf{k}'_{\text{sec}}$

Algorithm 2: SimpleAttackTensorBL

the output of $\text{Attack}^{C^1}_{k'_{1,r}}(\mathbf{G}'_r)$ is such that $M\hat{M}^{-1} \in \text{PAut}(C^1)$ (see (7)). The latter means that such a nonsingular $(k_1 \times k_1)$-matrix K can be found, that $KG^1 = G^1M\hat{M}^{-1}$. Let $P' = (\hat{M} \otimes I_{n_2})\text{diag}(D'_0, ..., D'_{n_1-1})L$. Then the following chain of equalities holds:

$$\begin{aligned}
\widetilde{G}P'^{-1} &= \widetilde{G}L^{-1}\text{diag}(D_0'^{-1}, ..., D'^{-1}_{n_1-1})(\hat{M}^{-1} \otimes I_{n_2}) \\
&= H(G^1 \otimes G^2)(M \otimes I_{n_2})\text{diag}(D_0, ..., D_{n_1-1})\text{diag}(D_0'^{-1}, ..., D'^{-1}_{n_1-1})(\hat{M}^{-1} \otimes I_{n_2}) \\
&= H(G^1M \otimes G^2)\text{diag}(A_0, ..., A_{n_1})(\hat{M}^{-1} \otimes I_{n_2}) \\
&= HR(G^1M \otimes G^2)(\hat{M}^{-1} \otimes I_{n_2}) = HR(G^1M\hat{M}^{-1} \otimes G^2) \\
&\overset{(a)}{=} HR(KG^1 \otimes G^2) \overset{(b)}{=} HR(K \otimes I_{k_2})(G^1 \otimes G^2).
\end{aligned} \tag{33}$$

From (b) it follows that equation $H'(G^1 \otimes G^2) = \widetilde{G}P'^{-1}$ with unknown H' (see SimpleAttackTensorBL) has a solution. Then (H', P') is suitable secret key.

The complexity of the algorithm SimpleAttackTensorBL follows from the fact that it enumerates the elements of the set Ω_{n_2,n_1}, and at each iteration, effective (polynomial) algorithms are performed.

□

Remark 4. It follows from the theorem that even with the onerous condition that the matrix $\mathrm{diag}(A_0, ..., A_{n_1-1})$ belongs to the automorphism group of a code with a generator matrix $G^1 M \otimes G^2$, the complexity of the cryptanalytical algorithm SimpleAttackTensorBL nonpolynomially depends on the length of the code $C^1 \otimes C^2$.

Remark 5. If there is not a single submatrix in the (31) form $\mathbf{\Gamma}''_i$ of rank k_1, then some permutation matrix $\hat{M}$can be found, for example, using an algorithm from the family $\mathcal{A}(C^1)$. However, for this matrix the condition $M\hat{M}^{-l} \in \mathrm{PAut}(C^2)$ may not be fulfilled, therefore the equality (a) in (33) in this case will be not fulfilled.

2.2.3. Cryptanalysis over C^1 in the Case of $\mathrm{diag}(A_0, ..., A_{n_1-1}) \notin \mathrm{PAut}(\mathcal{L}(G^1 M \otimes G^2))$

The assumption made in the theorem 1 concerning the membership of the matrix $\mathrm{diag}(A_0, ..., A_{n_1-1})$ to the automorphism group of the code with the generator matrix $G^1 M \otimes G^2$, is pretty strong. In the general case

$$\mathrm{diag}(A_0, ..., A_{n_1-1}) \notin \mathrm{PAut}(\mathcal{L}(G^1 M \otimes G^2)) \tag{34}$$

(see (12)), i.e there may not exist a matrix R such that (30) holds. Therefore, in order to find the unknown component M the matrix $\mathrm{diag}(A_0, ..., A_{n_1-1})$ will have to be searched, for example, by a brute force. However, then, as in the algorithm SimpleAttackTensorBL it is necessary to scour through the set Ω_{n_2,n_1} (or Ω_{n_1,n_2}, see (10)), since before using cryptanalysis, it is necessary to find a matrix satisfying the condition 1) of the lemma 1. The scan through the set of representatives has complexity $\mathcal{O}\left(\min\left\{|\Omega_{n_1,n_2}|; |\Omega_{n_2,n_1}|\right\}\right)$ with rough estimate

$$\mathcal{O}\left(\min\left\{\frac{(n_1^{n_1})^{n_2-1}}{2^{n_2(n_1-1)}}; \frac{(n_2^{n_2})^{n_1-1}}{2^{n_1(n_2-1)}}\right\}\right), \tag{35}$$

(see (19)). The estimate (35) does not depend on k', so for the system $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ the search for multiple representatives is similar to the search performed in the cryptoalgorithm from [17] for the system $\mathrm{McE}(C^1 \otimes C^2)$. The difference is manifested only in the implementation of each iteration in the enumeration cycle: for $\mathrm{McE}(C^1 \otimes C^2)$ an algorithm for breaking $\mathrm{McE}(C^i)$ is used, but for $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ no less sophisticated algorithm for $\mathrm{BL}_{k'_i}(C^i)$ is used. Therefore, the Berger – Loidreau-type cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ has no less strength to structural attacks than $\mathrm{McE}(C^1 \otimes C^2)$.

In conclusion, we note the Theorem 1 proposes conditions under which the complexity of finding a suitable secret key is $\mathcal{O}\left(\frac{(n_1 n_2)!}{(n_2!)^{n_1} n_1!}\right)$. However, in the general case of (34) additional conditions that greatly facilitate cryptanalysis are not found. So a suitable secret key can be found by a complete search of the permutation matrices, that is, the complexity of finding a suitable secret key is $\mathcal{O}\left((n_1 n_2)!\right)$.

3. Examples of Evaluating the Strength of a System $\mathrm{BL}_{k'}(C^1 \otimes C^2)$

In this section, we will evaluate the strength of a cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ in the case when C^1, C^2 are binary Reed – Muller codes (see [7]). We will assume that the cryptanalyst is strong and he succeeds in using the conditions of Theorem 1. Specifically, it is assumed that the cryptanalyst has a set Ω_{n_2,n_1} (or Ω_{n_1,n_2}), $\mathrm{diag}(A_0, ..., A_{n_1-1})(\in \mathrm{PAut}(\mathcal{L}(G^1 M \otimes G^2)))$ has the form (29) and there is at least one submatrix $\mathbf{\Gamma}_i''$ of rank k_1 in the presentation (31). In other words, the cryptanalyst is placed in the most favorable conditions for cryptanalysis of the system $\mathrm{BL}_{k'}(C^1 \otimes C^2)$, found in this paper. Suppose, for example, $C^1 = C^2$ is binary Reed – Muller code of order m, length $n = 2^m$, $m \in \mathbb{N}$. From (35) we get, that scour through the set $\Omega_{n,n}$ has a complexity of at least $\mathcal{O}(2^{(m-1)(2^{2m}-2^m)})$. At present, according to [1], it is considered computationally not applicable to search through a key set of power 2^{128} and more. Therefore, for all m such that $(m-1)(2^{2m}-2^m) \geq 128$, corresponding cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ will have high strength. In particular, high strength is provided for $m \geq 4$.

Besides high strength to structural attacks public-key cryptosystems must have high strength to attacks on the ciphertext. For McEliece code cryptosystems typical attacks on the ciphertext are based on decoding by information sets, including attacks on a repeated message. To ensure high strength to such attacks, a popular method of adding «padding» to the encrypted block is used (see [16], [21],[22]). In [22] proved, that such cryptosystems are semantically secure. In [21] for an arbitrary finite field $\mathbb{F}_q$ general formulas for estimating the probability of success of attacks based on decoding by information sets are found. In particular, in Theorem 3 from [21] the probability p evaluation formula is obtained for successful illegitimate decryption of the message on two ciphertexts in the case, when the padding method is applied. We note that the formulas in [21] do not depend on the structure of the public key, but depend only on its size, the number of errors corrected by the error code and the length of the encrypted information block. Therefore, these formulas are applicable to $\mathrm{BL}_{k'}(C^1 \otimes C^2)$.

Let's consider an example when C^1 is $[128, 29, 32]$-Reed – Muller code, C^2 is $[256, 93, 32]$-Reed – Muller code, and $C^1 \otimes C^2$ is $[32768, 2697, 1024]$–code. In this case, $n_1 = 2^{m_1}$, $n_2 = 2^{m_2}$, where $m_1 = 7$, $m_2 = 8$, therefore for a cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ provides high strength to the above-mentioned attacks on the key, since $m_i > 4$. In [21] it is shown, that the cryptosystem $\mathrm{McE}(C^1 \otimes C^2)$ in the case where in the encrypted block of length 2697 bits the first 1348 bits are allocated for the information message, and the remaining 1349 bits are selected randomly (padding) provides high strength to attack on a repeated message: probability p of successful illegitimate decryption of the message on two ciphertexts using the method of decoding on information sets does not exceed $1.7 \cdot 10^{-18}$ (see [21], table 3, row 3). However, similar calculations performed for a cryptosystem $\mathrm{BL}_{k'}(C^1 \otimes C^2)$ show that its strength to attacks on the ciphertext is less than that of the system $\mathrm{McE}(C^1 \otimes C^2)$. The table 1 contains the results of calculating p for $\mathrm{BL}_{k'}(C^1 \otimes C^2)$. As one can see, p increases with decreasing k', since with decreasing k' increases probability of choosing coordinates in the ciphertext, which are not spoiled by the error vector added during encryption (see (1)). We also note that with decreasing k', the coding rate R also decreases.

The authors are sincerely grateful to O. Turchenko for assistance in preparing the manuscript.

Table

Probability p of success of attack on two ciphertexts of the Berger – Loidreau cryptosystem

k'	$\lfloor k'/2 \rfloor$	R	p
2497	1248	$0,03811$	$2.92 \cdot 10^{-18}$
2297	1148	$0,03506$	$7.86 \cdot 10^{-17}$
2097	1048	$0,03201$	$2.09 \cdot 10^{-15}$
1897	948	$0,02896$	$5.52 \cdot 10^{-14}$
1697	848	$0,02590$	$1.43 \cdot 10^{-12}$
1497	748	$0,02285$	$3.71 \cdot 10^{-11}$
1297	648	$0,01980$	$9.48 \cdot 10^{-10}$
1097	548	$0,01675$	$2.39 \cdot 10^{-8}$
897	448	$0,01370$	$5.99 \cdot 10^{-7}$
697	348	$0,01065$	$1.48 \cdot 10^{-5}$
497	248	$0,00759$	$3.63 \cdot 10^{-4}$
297	148	$0,00454$	$8.81 \cdot 10^{-3}$

References

1. Lenstra A.K., Verheul E.R. Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 2001, vol. 14, pp. 255–293. doi: 10.1007/978-3-540-46588-1_30.
2. Bernstein D.J., Buchmann J., Dahmen E. *Post-Quantum Cryptography*. Berlin, Springer, 2009.
3. Sendrier N., Tillich J.P. *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, available at: https://hal.archives-ouvertes.fr/hal-01410068/document (accessed on June 4, 2018).
4. McEliece R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *JPL Deep Space Network Progress Report*, 1978, no. 42, pp. 114–116.
5. Bernstein D.J. Grover vs. McEliece. *Lecture Notes in Computer Science*, 2010, vol. 6061, pp. 73–80. doi: 10.1007/978-3-642-12929-2_6.
6. Eisenbarth T., Guneysu T., Heyse S., Paar C. MicroEliece: McEliece for Embedded Devices. *CHES '09 Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*. Berlin, Springer, 2009, pp. 49–64.
7. Sidel'nikov V.M. [*Coding Theory*]. Moscow, FIZMATLIT Publ., 2008. (in Russian)
8. Sidel'nikov V.M., Shestakov S.O. On an Encoding System Constructed on the Basis of Generalized Reed – Solomon Codes. *Discrete Mathematics and Applications*, 1992, vol. 2, no. 4, pp. 439–444.
9. Deundjak V.M., Druzhinina M.A., Kosolapov Yu.V. [Modification of Sidelnikov – Shestakov Cryptanalytical Algorithm for Generalized Reed – Solomon Codes and Its Software Implementation]. *University News. North-Caucasian Region. Technical Sciences Series*, 2006, no. 4, pp. 15–19. (in Russian)
10. Wieschebrink C. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes. *Third International Workshop, PQCrypto*. Berlin, Springer, 2010, pp. 61–72.

11. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem. *Lecture Notes in Computer Science*, 2007, vol. 4515, pp. 347–360.
12. Borodin M.A., Chizhov I.V. Efficiency of Attack on the McEliece Cryptosystem Constructed on the Basis of Reed – Muller Codes. *Discrete Mathematics and Applications*, 2014, vol. 24, no. 5, pp. 273–280. (in Russian) doi: 10.4213/dm1264.
13. Berger T., Loidreau P. How to Mask the Structure of Codes for a Cryptographic Use. *Designs, Codes and Cryptography*, 2005, vol. 35, no. 1, pp. 63–79.
14. Baldi M., Bianchi M., Chiaraluce F., Rosenthal J., Schipani D. Enhanced Public Key Security for the McEliece Cryptosystem. *Journal of Cryptology*, 2016, vol. 29, issue 1, pp. 1–27. doi: 10.1007/s00145-014-9187-8.
15. Chizhov I.V., Borodin M.A. Cryptanalysis of the McEliece PKC Based on $(k-1)$-Reed – Muller Subcodes. *Prikl. Diskr. Mat. Suppl.*, 2016, issue 9, pp. 73–75. (in Russian) doi: 10.17223/2226308X/9/29.
16. Deundyak V.M., Kosolapov Yu.V. Cryptosystem Based on Induced Group Codes. *Modeling and Analysis of Information Systems*, 2016, vol. 23, no. 2, pp. 137–152. (in Russian) doi: 10.18255/1818-1015-2016-2-137-152.
17. Deundyak V.M., Kosolapov Yu.V., Leluk E.A. Decoding the Tensor Product of MLD Codes and Applications for Code Cryptosystems. *Modeling and Analysis of Information Systems*, 2017, vol. 24, no. 2, pp. 239–252. (in Russian) doi: 10.18255/1818-1015-2017-2-239-252.
18. Deundyak V.M., Kosolapov Yu.V. Algorithms for Majority Decoding of Group Codes. *Modeling and Analysis of Information Systems*, 2015, vol. 22, no. 4, pp. 464–482. (in Russian) doi: 10.18255/1818-1015-2015-4-464-482.
19. Henderson H.V., Searle S.R. The Vec-Permutation Matrix, the Vec Operator and Kronecker Products: A Review. *Linear and Multilinear Algebra*, 1981, no. 9, pp. 271–288.
20. Morelos-Zaragoza R.H. *The Art of Error Correcting Coding*. Chichester, John Wiley & Sons, 2006.
21. Deundyak V.M., Kosolapov Yu.V. The Use of the Tensor Product of Reed – Muller Codes in Asymmetric McEliece Type Cryptosystem and Analysis of Its Resistance to Attacks on the Cryptogram. *Computational Technologies*, 2017, vol. 22, no. 4, pp. 43–60. (in Russian)
22. Nojima R., Imai H., Kobara K., Morozov K. Semantic Security for the McEliece Cryptosystem without Random Oracles. *Designs, Codes and Cryptography*, 2008, vol. 49, no. 1-3, pp. 289–305.

Vladimir M. Deundyak, PhD (Math), Associate Professor, Institute for Mathematics, Mechanics, and Computer Science in the name of I.I. Vorovich, Southern Federal University; FGNU NII "Specvuzavtomatika" (Rostov-on-Don, Russian Federation), vl.deundyak@gmail.com.

Yury V. Kosolapov, PhD (Tech), Institute for Mathematics, Mechanics, and Computer Science in the name of I.I. Vorovich, Southern Federal University (Rostov-on-Don, Russian Federation), itaim@mail.ru.

Received May 25, 2018.

УДК 517.9 **DOI: 10.14529/jcem180202**

О КОДОВОЙ КРИПТОСИСТЕМЕ БЕРГЕРА – ЛОЭДРЕ НА ОСНОВЕ ТЕНЗОРНОГО ПРОИЗВЕДЕНИЯ КОДОВ

В. М. Деундяк, Ю. В. Косолапов

В постквантовую эпоху асимметричные криптосистемы на основе линейных кодов (кодовые криптосистемы) рассматриваются как альтернатива современным асимметричным криптосистемам. Однако результаты исследования стойкости кодовых криптосистем типа Мак-Элиса показывают, что алгебраически структурированные коды не обеспечивают достаточную стойкость этих криптосистем. С другой стороны, использование случайных кодов в таких криптосистемах невозможно из-за высокой сложности декодирования таких кодов. Усиление кодовых криптосистем в настоящее время ведется, обычно, либо путем использования кодов, для которых не известны атаки, либо путем модификации криптографического протокола. В настоящей работе строится кодовая криптосистема, где используются оба этих подхода. С одной стороны, предлагается применять тензорное произведение $C^1 \otimes C^2$ известных кодов C^1 и C^2, так как для $C^1 \otimes C^2$ в ряде случаев удается построить эффективный алгоритм декодирования. С другой стороны, вместо криптосистемы типа Мак-Элиса предлагается использовать ее модификацию – криптосистему типа Бергера – Лоэдре. В работе показана высокая стойкость построенной кодовой криптосистемы к атакам на ключ даже в случае, когда кодовые криптосистемы на кодах C^1 и C^2 взломаны.

Ключевые слова: криптосистема Бергера – Лоэдре; тензорное произведение кодов; атака на ключ.

Литература

1. Lenstra, A.K. Selecting Cryptographic Key Sizes / A.K. Lenstra, E.R. Verheul // Journal of Cryptology. – 2001. – V. 14. – P. 255–293.

2. Bernstein, D.J. Post-Quantum Cryptography / D.J. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009.

3. Sendrier, N. Code-Based Cryptography: New Security Solutions Against a Quantum Adversary / N. Sendrier, J.P. Tillich. – url: https://hal.archives-ouvertes.fr/hal-01410068/document (запрос 4 июня 2018 г.).

4. McEliece, R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory / R.J. McEliece // JPL Deep Space Network Progress Report. – 1978. – № 42. – P. 114–116.

5. Bernstein, D.J. Grover vs. McEliece / D.J. Bernstein // Lecture Notes in Computer Science. – 2010. – V. 6061. – P. 73–80.

6. Eisenbarth, T. MicroEliece: McEliece for Embedded Devices / T. Eisenbarth, T. Guneysu, S. Heyse, C. Paar // Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems. – 2009. – P. 49–64.

7. Сидельников, В.М. Теория кодирования / В.М. Сидельников. – М.: ФИЗМАТЛИТ, 2008.

8. Sidel'nikov, V.M. On an Encoding System Constructed on the Basis of Generalized Reed – Solomon Codes / V.M. Sidel'nikov, S.O. Shestakov // Discrete Mathematics and Applications. – 1992. – V. 2, № 4. – P. 439–444.

9. Деундяк, В.М. Модификация криптоаналитического алгоритма Сидельникова-Шестакова для обобщенных кодов Рида – Соломона и ее программная реализация / В.М. Деундяк, М.А. Дружинина, Ю.В. Косолапов // Известия высших учебных заведений. Северо-Кавказский регион. Технические науки. – 2006. – № 4. – С. 15–19.

10. Wieschebrink, C. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes / C. Wieschebrink // Third International Workshop, PQCrypto. – Berlin: Springer, 2010. – P. 61–72.

11. Minder, L. Cryptanalysis of the Sidelnikov Cryptosystem / L. Minder, A. Shokrollahi // Lecture Notes in Computer Science. – 2007. – V. 4515. – P. 347–360.

12. Бородин, М.А. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида – Маллера / И.В. Чижов, М.А. Бородин // Дискретная математика. – 2014. – Т. 26, № 1. – С. 10–20.

13. Berger, T. How to Mask the Structure of Codes for a Cryptographic Use / T. Berger, P. Loidreau // Designs, Codes and Cryptography. – 2005. – V. 35, № 1. – P. 63–79.

14. Baldi, M. Enhanced Public Key Security for the McEliece Cryptosystem / M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani // Journal of Cryptology. – 2016. – V. 29, № 1. – P. 1–27.

15. Чижов, И.В. Криптоанализ криптосистемы Мак-Элиса, построенной на $(k-1)$-подкодах кода Рида – Маллера / И.В. Чижов, М.А. Бородин // ПДМ. Приложение. – 2016. – № 9. – С. 73–75.

16. Деундяк, В.М. Криптосистема на индуцированных групповых кодах / В.М. Деундяк, Ю.В. Косолапов // Модел. и анализ информ. систем. – 2016. – Т. 23, № 2. – С. 137–152.

17. Деундяк, В.М. Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам / В.М. Деундяк, Ю.В. Косолапов, Е.А. Лелюк // Модел. и анализ информ. систем. – 2017. – Т. 24, № 2. – С. 239–252.

18. Деундяк, В.М. Алгоритмы для мажоритарного декодирования групповых кодов / В.М. Деундяк, Ю.В. Косолапов // Модел. и анализ информ. систем. – 2015. – Т. 22, № 4. – С. 464–482.

19. Henderson, H.V. The Vec-Permutation Matrix, the Vec Operator and Kronecker Products: A Review / H.V. Henderson, S.R. Searle // Linear and Multilinear Algebra. – 1981. – № 9. – P. 271–288.

20. Morelos-Zaragoza, R.H. The Art of Error Correcting Coding / R.H. Morelos-Zaragoza. – Chichester: John Wiley & Sons, 2006.

21. Деундяк, В.М. Использование тензорного произведения кодов Рида – Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифрограмму / В.М. Деундяк, Ю.В. Косолапов // Вычислительные технологии. – 2017. – Т. 22, № 4. – С. 43–60.

22. Nojima, R. Semantic Security for the McEliece Cryptosystem without Random Oracles / R. Nojima, H. Imai, K. Kobara, K. Morozov // Designs, Codes and Cryptography. – 2008. – V. 49, № 1-3. – P. 289–305.

Деундяк Владимир Михайлович, кандидат физико-математических наук, доцент, Институт математики, механики и компьютерных наук им. И.И. Воровича, Южный федеральный университет; ФГНУ НИИ «Спецвузавтоматика» (г. Ростов-на-Дону, Российская Федерация), vl.deundyak@gmail.com.

Косолапов Юрий Владимирович, кандидат технических наук, Институт математики, механики и компьютерных наук им. И.И. Воровича, Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация), itaim@mail.ru.

Поступила в редакцию 25 мая 2018 г.