Modified GPT Cryptosystem for Information Network Security

Ernst Gabidulin, Nina Pilipchuk
Department of Radio Engineering and Telecommunications
Moscow Institute of Physics and Technology (State University)

Abstract

To provide information security in network we use the public key GPT (Gabidulin–Paramonov–Tretiyakov) cryptosystem based on rank codes. This cryptosystem was the subject of several attacks. Some of them were structural attacks, others were decoding attacks. In our opinion the most dangerous are structural attacks because decoding attacks can be prevented by proper choice of parameters. To prevent structural attacks, we change some of its secret keys. We called the modified GPT cryptosystem as GPT-M. We consider network communication with adversaries where we use the GPT-M cryptosystem and obtain conditions for network security.

1. Introduction

The first code based public-key cryptosystem (PKC) was proposed by McEliece in 1978 year [1]. It is based on Goppa codes in the Hamming metric. The size of a public key is 500 000 bits. It is too large for practical implementations to be efficient.

In 1986 year Niederreiter [2] introduced a new version of PKC based on a family of Generalized Reed-Solomon codes. It turned out that this cryptosystem is insecure. It was broken in 1992 year [3].

Gabidulin–Paramonov–Tretiyakov version of McEliece's public key cryptosystem is based on codes correcting *rank* errors. It was proposed in 1991 year[4] and now it is referred to as the GPT cryptosystem. The GPT cryptosystem has two advantages over McEliece's cryptosystem. Firstly, it is more robust against decoding attacks than McEliece's cryptosystem; secondly, the key size of the GPT is much smaller. This property is more useful in terms of practical applications.

Rank codes are well structured. Subsequently, using this fact it was shown in a series of works (for example,[5], [6],[7]) that the first version of the GPT system is insecure for practical values of parameters $n \leq 30$, where n is the length of a rank code over the field $GF(2^N), N \geq n$ as an alphabet. New structural attacks were proposed by Overbeck in 2008 year [8], which are more effective than the previous attacks. The attack is based on the fact that one of parameters, the column scrambler, is defined over the *base field*.

In this paper, we focus on using GPT public key cryptosys-tem with new parameters in order to transmit short cipher texts.

We analyze known Gibson's and Overbeck's structural attacks. To prevent structural attacks, we change some of secret keys. We denote the modified GPT cryptosystem as GPT-M. We describe also how the GPT-M cryptosystem can be implemented in secure network coding.

The paper is structured as follows. Section **2.** introduces the rank metric and optimal rank codes. Section **3.** describes the GPT cryptosystem. Section **4.** discusses Gibson's and Overbeck's attacks against the GPT cryptosystem. The new approach for choosing parameters is presented in Section **5**. Section **6.** describes a secure communication in the network with random network coding and GPT-M. Finally, Section 7. concludes the paper with some remarks.

2. Rank metric and rank codes

Let $GF(q)$ be a finite field of q elements. Let $GF(q^N)$ be an extension field of degree N. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a vector with coordinates in $GF(q^N)$.
The *Rank norm* of a vector $\mathbf{x}$ is defined as the maximal number of x_i which are linearly independent over the *base* field $GF(q)$. It is denoted as $\mathrm{Rk}_{\mathrm{col}}(\mathbf{x} \mid GF(q))$.
The *Rank distance* between vectors $\mathbf{x}$ and $\mathbf{y}$ is defined as the rank norm of their difference $\mathbf{x}-\mathbf{y}$: $d(\mathbf{x},\mathbf{y}) = \mathrm{Rk}_{\mathrm{col}}(\mathbf{x}-\mathbf{y} \mid GF(q))$.

Let $\mathbf{M}$ be a matrix with entries in the extension field $GF(q^N)$. We distinguish two types of ranks for this matrix:

1) The usual rank $\mathrm{Rk}(\mathbf{M} \mid GF(q^N))$ of a matrix $\mathbf{M}$ is defined as the maximal number of *rows or columns* which are linearly independent over the *extension* field $GF(q^N)$.
2) The column rank $\mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid GF(q))$ of the same matrix $\mathbf{M}$ is defined as the maximal number of *columns* which are linearly independent over the *base field* $GF(q)$.

The column rank of the matrix $\mathbf{M}$ depends on the field. In particular, $\mathrm{Rk}_{\mathrm{col}}(\mathbf{M} \mid GF(q)) \geq \mathrm{Rk}(\mathbf{M} \mid GF(q^N))$.

Let $\mathbf{M}$ be a $k \times n$ matrix over $GF(q^N)$ with the ordinary rank s and with the column rank Δ. Then it can be represented as

$$\mathbf{M} = \mathbf{AB}, \tag{1}$$

where $\mathbf{A}$ is a $k \times s$ matrix of ordinary rank s over the extension field $GF(q^N)$, $\mathbf{B}$ is a $s \times n$ matrix of ordinary rank s over

the extension field $GF(q^N)$. Another representation is

$$\mathbf{M} = \mathbf{CD}, \tag{2}$$

where $\mathbf{C}$ is a $k \times \Delta$ matrix over the extension field $GF(q^N)$, and $\mathbf{D}$ is a $\Delta \times n$ matrix over the *base field* $GF(q)$ with column rank Δ.

Any set $\mathcal{C} \subset GF(q^N)^n$ is called a vector rank code. A code $\mathcal{C}$ is called a linear (n, k, d) code if it is a k-dimensional subspace of the space $GF(q^N)^n$ and has minimal pairwise rank distance d. Any vector rank (n, k, d) code fulfils the Singleton-style bound for the rank distance:

$$Nk \leq Nn - (d-1)\max\{N, n\}. \tag{3}$$

A code $\mathcal{C}$ reaching that bound is called a Maximal Rank Distance (MRD) code. Constructions of optimal MRD (Maximal Rank Distance) codes are given in [9].

The notation $g^{[i]} := g^{q^{i \bmod N}}$ means the i-th Frobenius power of g. It allows to consider both positive and negative Frobenius powers i.

For $n \leq N$, a generator matrix $\mathbf{G}_k$ of a (n, k, d) MRD code is defined by a matrix of the following form:

$$\mathbf{G}_k = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ g_1^{[2]} & g_2^{[2]} & \cdots & g_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix} \tag{4}$$

where $g_1, g_2, \ldots, g_n$ are a set of elements of the extension field $GF(q^N)$ which are linearly independent over the base field $GF(q)$. A code with the generator matrix (4) is referred to as (n, k, d) code, where n is code length, k is the number of information symbols, d is code distance. For MRD codes, $d = n - k + 1$. Let $\mathbf{m} = (m_1, m_2, \ldots, m_k)$ be an information vector of dimension k with coordinates in the extension field $GF(q^N)$. The corresponding code vector is the n-vector

$$\mathbf{g}(\mathbf{m}) = \mathbf{m}\mathbf{G}_k.$$

If $\mathbf{y} = \mathbf{g}(\mathbf{m}) + \mathbf{e}$ and $\mathrm{Rk}_{\mathrm{col}}(\mathbf{e}) = s \leq t = \frac{d-1}{2}$, then the information vector $\mathbf{m}$ can be recovered uniquely from $\mathbf{y}$ by some decoding algorithm. There exist fast decoding algorithms for MRD codes (for instance, [9], [10]). A decoding procedure requires elements of the $(n-k) \times n$ parity check matrix $\mathbf{H}$ such that $\mathbf{G}_k\mathbf{H}^T = \mathbf{0}$. For decoding, the matrix $\mathbf{H}$ should be of the form

$$\mathbf{H} = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \\ h_1^{[1]} & h_2^{[1]} & \cdots & h_n^{[1]} \\ h_1^{[2]} & h_2^{[2]} & \cdots & h_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{bmatrix}, \tag{5}$$

where elements $h_1, h_2, \ldots, h_n$ are in the extension field $GF(q^N)$ and are linearly independent over the base field $GF(q)$.

The optimal code design parameters:

1) Code length $n \leq N$.
2) Dimension $k = n - d + 1$.
3) Rank code distance $d = n - k + 1$.

3. The GPT cryptosystem

The GPT cryptosystem is described as follows:
A **Plaintext** is any k-vector $\mathbf{m} = (m_1, m_2, \ldots, m_k)$, $m_s \in GF(q^N)$, $s = 1, 2, \ldots, k$.
The Public key is a $k \times (n + t_1)$ generator matrix

$$\mathbf{G}_{pub} = \mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right](\mathbf{P} + \mathbf{Z}) \tag{6}$$

This is a general form of the public key. Let us explain roles of the factors.

- The main matrix $\mathbf{G}_k$ of size $k \times n$ is given by (4). It is used to correct rank errors. Errors of rank not greater than $t = \lfloor \frac{n-k}{2} \rfloor$ can be corrected.
- A matrix $\mathbf{S}$ is a row scrambler. This matrix is a non singular square matrix of order k over the extension field $GF(q^N)$. It is used to hide any visible row structure of matrices used for deciphering.
- A matrix $\mathbf{Y}$ is the first distortion $(k \times t_1)$ matrix over $GF(q^N)$ with *full* column rank $\mathrm{Rk}_{\mathrm{col}}(Y \mid GF(q)) = t_1$ and with the ordinary rank $\mathrm{Rk}(\mathbf{Y} \mid GF(q^N)) = t_Y$, $t_Y \leq t_1$. The matrix $\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right]$ has full column rank $\mathrm{Rk}_{\mathrm{col}}(\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right] \mid GF(q)) = n + t_1$.
- A matrix $\mathbf{X}$ is the second distortion $k \times n$ matrix having the column rank t_2 and the ordinary rank t_X.
- A matrix $(\mathbf{P} + \mathbf{Z})$ is a square *column scramble* matrix of order $(t_1 + n)$. The matrix $\mathbf{P}$ has entries in the base field $GF(q)$. The matrix $\mathbf{Z}$ is the third distortion matrix and should have entries in the extension field $GF(q^N)$. Also its column rank should be not greater than an integer Δ (a design parameter). The matrix $(\mathbf{P} + \mathbf{Z})$ should be nonsingular.

The Private keys are matrices $\mathbf{S}$, $\mathbf{G}_k$, $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{P} + \mathbf{Z}$ separately and (explicitly) a fast decoding algorithm of an MRD code.

Encryption: Let $\mathbf{m} = (m_1, m_2, \ldots, m_k)$, $m_j \in GF(q^N)$, be a plaintext. The corresponding ciphertext is given by

$$\mathbf{c} = \mathbf{m}\mathbf{G}_{\mathrm{pub}} + \mathbf{e}_{\mathrm{art}} = \mathbf{m}\mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right](\mathbf{P} + \mathbf{Z}) + \mathbf{e}_{\mathrm{art}}, \tag{7}$$

where $\mathbf{e}_{\mathrm{art}}$ is an *artificial vector of errors* of rank t_3.

Decryption: The legitimate receiver upon receiving $\mathbf{c}$ calculates

$$\mathbf{c}' = (c_1', c_2', \ldots, c_{t_1+n}') =$$

$$\mathbf{c}\,(\mathbf{P} + \mathbf{Z})^{-1} = \mathbf{m}\mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right] + \mathbf{e}_{\mathrm{art}}(\mathbf{P} + \mathbf{Z})^{-1}$$

Then from $\mathbf{c}'$ he extracts the subvector

$$\mathbf{c}'' = (c_{t_1+1}', c_{t_1+2}', \ldots, c_{t_1+n}') = \mathbf{m}\mathbf{S}\mathbf{G}_k + \mathbf{m}\mathbf{S}\mathbf{X} + \mathbf{e}_{\mathrm{art}}'', \tag{8}$$

where $\mathbf{e}_{\mathrm{art}}''$ is the subvector of $\mathbf{e}_{\mathrm{art}}(\mathbf{P} + \mathbf{Z})^{-1}$. Note that the rank of $\mathbf{m}\mathbf{S}\mathbf{X}$ is not greater than t_2 and the rank of $\mathbf{e}_{\mathrm{art}}''$ is not greater than $t_3 + \Delta$. If $t_2 + t_3 + \Delta \leq t = \lfloor \frac{n-k}{2} \rfloor$, then the legitimate receiver applies the fast decoding algorithm to correct the error $\mathbf{m}\mathbf{S}\mathbf{X} + \mathbf{e}_{\mathrm{art}}''$, extracts $\mathbf{m}\mathbf{S}$ and recovers m as $\mathbf{m} = (\mathbf{m}\mathbf{S})\mathbf{S}^{-1}$.

In this system, the size of the public key is $V = k(t_1+n)N$ bits, and the information rate is $R = \frac{k}{t_1+n}$.

4. Attacks against the GPT cryptosystem

There are two types of attacks against the GPT cryptosystem and its variants. The first one is the decoding attacks. The second is the structural attacks, for example Gibson and Overbeck's attacks. The decoding attacks are presented in details in the works [11], [12], [13], [14]. The focus of our attention is the known structural attacks against the GPT cryptosystem and its variants.

4.1. Gibson's attacks

Gibson analyzed in [5], [6] the variant of the GPT cryptosystem with the public key

$$\mathbf{G}_{pub} = \mathbf{S}(\mathbf{G}_k + \mathbf{X}),$$

where the distortion matrix $\mathbf{X}$ has the column rank t_2 and the ordinary rank $1 \leq t_X \leq t_2$. He obtained using $\mathbf{G}_{pub}$ three matrices $\widehat{\mathbf{S}}$, $\widehat{\mathbf{G}}_k$, $\widehat{\mathbf{X}}$ such that

$$\mathbf{G}_{pub} = \widehat{\mathbf{S}}(\widehat{\mathbf{G}}_k + \widehat{\mathbf{X}}).$$

It has runtime

$$\mathcal{O}\left(N^3(n-k)^3 q^{Nt_X}\right),$$

or,

$$\mathcal{O}\left(k^3 + (k+t_2)f \cdot q^{f(k+2)} + (m-k)t_2 \cdot q^f\right),$$

where $f = \max(0, t_2 - 2t_X, t_2 + 1 - k)$.

4.2. The first Overbeck attack

The variant of the GPT cryptosystem with the public key

$$\mathbf{G}_{pub} = \mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}_k + \mathbf{X}\right]\mathbf{P}$$

was analyzed in [7]. The column rank and length of the matrix $\mathbf{Y}$ is t_1. The matrix $\mathbf{X}$ has the column rank t_2. The Overbeck attack is as follows. The public key is written over the extension field $GF(q^N)$ but one can rewrite it over the super extension field $GF(q^{aN})$, where $a = \left\lceil \frac{n+t_1}{N} \right\rceil$. It allows to represent the public key in the form

$$\mathbf{G}_{pub} = \mathbf{S}\left[\widehat{\mathbf{G}}_k + \widehat{\mathbf{X}}\right],$$

where $\widehat{\mathbf{G}}_k$ is a virtual rank code of length $t_1 + n$ over the super extension field $\mathbb{F}_{q^{aN}}$ and a virtual distortion matrix $\widehat{\mathbf{X}}$ has the column rank $t_1 + t_2$. Thus one reduced the problem to Gibson's case.

4.3. The second Overbeck attack

An artificial error $\mathbf{e}_{\mathrm{art}}$ is a correctable rank error. The column scrambler $\mathbf{P} + \mathbf{Z}$ must be chosen in such a manner that the vector $\mathbf{e}_{\mathrm{art}}(\mathbf{P} + \mathbf{Z})^{-1}$ is a correctable rank error too. First variants of GPT cryptosystems used matrices $\mathbf{P}$ and $\mathbf{P}^{-1}$ over the base field $GF(q)$, i.e. $\mathbf{Z} = \mathbf{0}$. In this case

$$\mathrm{Rk}_{col}(\mathbf{e}_{\mathrm{art}}) = \mathrm{Rk}(\mathbf{e}_{\mathrm{art}}\mathbf{P}^{-1}) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Overbeck shows in [8] that in this case the GPT cryptosystem with the public key of the form

$$\mathbf{G}_{pub} = \mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}\right]\mathbf{P}$$

can be broken in polynomial time. The crucial point of the attack is based on the condition that all entries of the matrix $\mathbf{P}$ are in the base field $GF(q)$.

We recall briefly this attack. For $x \in GF(q^N)$ let $\sigma(x) = x^q$ be the Frobenius automorphism. For the matrix $\mathbf{T} = (t_{ij})$ over $GF(q^N)$, let $\sigma(\mathbf{T}) = (\sigma(t_{ij})) = (t_{ij}^q)$.
For any integer s, let $\sigma^s(\mathbf{T}) = \sigma(\sigma^{s-1}(\mathbf{T}))$. It is clear that $\sigma^N = \sigma$. Thus the inverse exists $\sigma^{-1} = \sigma^{N-1}$.
The following simple properties if σ are well known:

- $\sigma(a+b) = \sigma(a) + \sigma(b)$.
- $\sigma(ab) = \sigma(a)\sigma(b)$.
- In general, for matrices $\sigma(\mathbf{T}) \neq \mathbf{T}$.
- If $\mathbf{P}$ is a matrix over the *base* field $GF(q)$, then $\sigma(\mathbf{P}) = \mathbf{P}$.

Description of Overbeck's attack: To break a system, a cryptanalyst constructs for some integer u from the public key $\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\left[\mathbf{Y} \quad \mathbf{G}_k\right]\mathbf{P}$ the *extended* public key $\mathbf{G}_{\mathrm{ext,pub}}$ as follows:

$$\mathbf{G}_{\mathrm{ext,pub}} = \begin{Vmatrix} \mathbf{G}_{\mathrm{pub}} \\ \sigma(\mathbf{G}_{\mathrm{pub}}) \\ \sigma^2(\mathbf{G}_{\mathrm{pub}}) \\ \cdots \\ \sigma^u(\mathbf{G}_{\mathrm{pub}}) \end{Vmatrix} =$$

$$\begin{Vmatrix} \mathbf{S} & \begin{bmatrix}\mathbf{Y} & \mathbf{G}_k\end{bmatrix} & \mathbf{P} \\ \sigma(\mathbf{S}) & \begin{bmatrix}\sigma(\mathbf{Y}) & \sigma(\mathbf{G}_k)\end{bmatrix} & \mathbf{P} \\ \sigma^2(\mathbf{S}) & \begin{bmatrix}\sigma^2(\mathbf{Y}) & \sigma^2(\mathbf{G}_k)\end{bmatrix} & \mathbf{P} \\ \cdots & \cdots\cdots \cdots & \cdots \\ \sigma^u(\mathbf{S}) & \begin{bmatrix}\sigma^u(\mathbf{Y}) & \sigma^u(\mathbf{G}_k)\end{bmatrix} & \mathbf{P} \end{Vmatrix} \tag{9}$$

The property that $\sigma(\mathbf{P}) = \mathbf{P}$, if $\mathbf{P}$ is a matrix over the *base* field $GF(q)$, is used in (9).

Rewrite this matrix as

$$\mathbf{G}_{\mathrm{ext,pub}} = \mathbf{S}_{\mathrm{ext}}\left[\mathbf{W}_{\mathrm{ext}} \quad \mathbf{G}_{\mathrm{ext}}\right]\mathbf{P}, \tag{10}$$

where

$$\mathbf{S}_{\mathrm{ext}} = \mathrm{Diag}\left[\mathbf{S} \quad \sigma(\mathbf{S}) \quad \ldots \quad \sigma^u(\mathbf{S})\right]$$

$$\mathbf{W}_{\mathrm{ext}} = \begin{bmatrix} \mathbf{Y} \\ \sigma(\mathbf{Y}) \\ \vdots \\ \sigma^u(\mathbf{Y}) \end{bmatrix}, \quad \mathbf{G}_{\mathrm{ext}} = \begin{bmatrix} \mathbf{G}_k \\ \sigma(\mathbf{G}_k) \\ \vdots \\ \sigma^u(\mathbf{G}_k) \end{bmatrix}$$

Choose

$$u = n - k - 1 \tag{11}$$

For a $k \times t_1$ matrix

$$\mathbf{Y} = \begin{bmatrix} Y_{11} & Y_{12} & \dots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \dots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \dots & Y_{k-1,t_1} \\ Y_{k,1} & Y_{k,2} & \dots & Y_{k,t_1} \end{bmatrix}, \qquad (12)$$

let

$$\mathbf{Y}_1 = \begin{bmatrix} Y_{11} & Y_{12} & \dots & Y_{1,t_1} \\ Y_{21} & Y_{22} & \dots & Y2,t_1 \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \dots & Y_{k-1,t_1} \end{bmatrix} \qquad (13)$$

be the $(k-1) \times t_1$ matrix, obtained from $\mathbf{X}$ by deleting the last row. Let

$$\mathbf{Y}_2 = \begin{bmatrix} Y_{21} & Y_{22} & \dots & Y_{2,t_1} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{k-1,1} & Y_{k-1,2} & \dots & Y_{k-1,t_1} \\ Y_{k,1} & Y_{k,2} & \dots & Y_{k,t_1} \end{bmatrix} \qquad (14)$$

be the $(k-1) \times t_1$ matrix, obtained from $\mathbf{Y}$ by deleting the first row.

Define a linear mapping $T : GF(q^N)^{k \times t_1} \to GF(q^N)^{(k-1) \times t_1}$ by the rule: if $\mathbf{Y} \in GF(q^N)^{k \times t_1}$, then

$$T(\mathbf{Y}) = \mathbf{W} = \sigma(\mathbf{Y}_1) - \mathbf{Y}_2.$$

Let

$$\mathbf{W}_{\text{ext}} = \begin{bmatrix} \mathbf{W} \\ \sigma(\mathbf{W}) \\ \sigma^2(\mathbf{W}) \\ \dots \\ \sigma^{u-1}(\mathbf{W}) \end{bmatrix}. \qquad (15)$$

Using suitable transformations of rows, one can rewrite for analysis (10) in the form

$$\tilde{\mathbf{G}}_{\text{pub,ext}} = \tilde{\mathbf{S}}_{\text{ext}} \begin{bmatrix} \mathbf{Z} & | & \mathbf{G}_{n-1} \\ \mathbf{W}_{\text{ext}} & | & 0 \end{bmatrix} \mathbf{P} \qquad (16)$$

where $\mathbf{G}_{n-1}$ is the generator matrix of the $(n, n-1, 2)$ MRD code.

Let us try to find a solution $\mathbf{u}$ of the system

$$\tilde{\mathbf{S}}_{\text{ext}} \begin{bmatrix} \mathbf{Z} & | & \mathbf{G}_{n-1} \\ \mathbf{W}_{\text{ext}} & | & 0 \end{bmatrix} \mathbf{P}\mathbf{u}^T = \mathbf{0}, \qquad (17)$$

where $\mathbf{u}$ is a vector-row over the extension field $GF(q^N)$ of length $t_1 + n$. Represent the vector $\mathbf{P}\mathbf{u}^T$ as

$$\mathbf{P}\mathbf{u}^T = \begin{bmatrix} \mathbf{y} & \mathbf{h} \end{bmatrix}^T,$$

where the subvector $\mathbf{y}$ has length t_1 and the subvector $\mathbf{h}$ has length n. Then the system (17) is equivalent to the following system:

$$\mathbf{Z}\mathbf{y}^T + \mathbf{G}_{n-1}\mathbf{h}^T = \mathbf{0}, \qquad (18)$$

$$\mathbf{W}_{\text{ext}}\mathbf{y}^T = \mathbf{0} \qquad (19)$$

Assume that the next condition is valid:

$$\text{Rk}(\mathbf{W}_{\text{ext}} \mid GF(q^N)) = t_1 \qquad (20)$$

Then the equation (19) has only the trivial solution $\mathbf{y}^T = \mathbf{0}$. The equation (18) becomes

$$\mathbf{G}_{n-1}\mathbf{h}^T = \mathbf{0} \qquad (21)$$

It allows to find the first row of the parity check matrix for the code with the generator matrix (16) (see,[8], for details). Hence this solution breaks a GPT cryptosystem in polynomial time. The Overbeck attack requires $\mathcal{O}((n+t_1)^3)$ operations over $GF(q^N)$ in order to break the system.

Note 1: The Overbeck attack requires $\mathcal{O}((n+t_1)^3) \cdot q^{aN}$ operations over $GF(q^N)$ in order to break the system, if

$$\text{Rk}(\mathbf{W}_{\text{ext}} \mid GF(q^N)) = t_1 - a,\ a \geq 2 \qquad (22)$$

.

4.4. How to prevent the second Overbeck attack

The Overbeck attack completely fails if one replaces in the public key the matrix $\mathbf{P}$ over the base field $GF(q)$ by a matrix $\mathbf{P} + \mathbf{Z}$ where a matrix $\mathbf{Z}$ is chosen over the extension field $GF(q^N)$. Nevertheless another problem rises: the artificial error vector $\mathbf{e}_{\text{art}}(\mathbf{P} + \mathbf{Z})^{-1}$ may become an uncorrectable error. In [15], this problem was overcome. Our main contribution is the construction of the set of matrices $(\mathbf{P} + \mathbf{Z})^{-1}$ such that for any vector $\mathbf{e}$ we will have

$$\text{Rk}_{col}(\mathbf{e}(\mathbf{P} + \mathbf{Z})^{-1} \mid GF(q)) \leq \text{Rk}_{\text{col}}(\mathbf{e} \mid GF(q) + \Delta,$$

where Δ is a given positive integer.

First of all, consider the case when $(\mathbf{B} + \mathbf{Z})^{-1} = \mathbf{I} + \mathbf{E}$ where $\mathbf{I}$ is the identity matrix of order $t_1 + n$ and a matrix $\mathbf{E}$ has column rank Δ.

Lemma 1: If $\mathbf{E}$ is a $(t_1+n) \times (t_1+n)$ matrix with column rank Δ, then for any vector $\mathbf{e}$ with column rank s we have

$$\text{Rk}_{\text{col}}(\mathbf{e}(\mathbf{I} + \mathbf{E}) \mid GF(q)) \leq s + \Delta.$$

Proof: The function of the column rank is a norm. Thus we have

$$\text{Rk}_{\text{col}}(\mathbf{e}(\mathbf{I} + \mathbf{E}) \mid GF(q)) \leq \text{Rk}_{\text{col}}(\mathbf{e} \mid GF(q)) + \text{Rk}_{\text{col}}(\mathbf{e}\mathbf{E} \mid GF(q)) \leq s +$$

■

Lemma 2: Assume that the matrix $\mathbf{E}$ satisfies the condition

$$\mathbf{E}^2 = \gamma\mathbf{E} \qquad (23)$$

and $\gamma \neq -1$. Then the matrix $\mathbf{I} + \mathbf{E}$ is nonsingular and

$$(\mathbf{I} + \mathbf{E})^{-1} = \mathbf{I} - \frac{1}{1+\gamma}\mathbf{E}. \qquad (24)$$

Proof: Calculate the product

$$(\mathbf{I} + \mathbf{E})(\mathbf{I} - \frac{1}{1+\gamma}\mathbf{E}) = \mathbf{I} - \frac{1}{1+\gamma}\mathbf{E} + \mathbf{E} - \frac{1}{1+\gamma}\mathbf{E}^2 = \qquad (25)$$

$$= \mathbf{I} - \frac{1}{1+\gamma}\mathbf{E} + \mathbf{E} - \frac{\gamma}{1+\gamma}\mathbf{E} = \mathbf{I}. \qquad (26)$$

■

A construction of matrices $\mathbf{E}$ satisfying the condition (23) and having column rank Δ is given by the following Lemma.

Lemma 3: Let a matrix $\mathbf{E}$ be of the form

$$\mathbf{E} = \mathbf{AB},$$

where $\mathbf{A}$ is a $(t_1 + n) \times \Delta$ matrix of full rank Δ and $\mathbf{B}$ is a $\Delta \times (t_1 + n)$ of *column* rank Δ. There exist matrices $\mathbf{A}$ and $\mathbf{B}$ such that

$$\mathbf{BA} = \gamma \mathbf{I}_\Delta,$$

where $\mathbf{I}_\Delta$ is the identity matrix of order Δ.

Proof: Choose a matrix $\mathbf{B}$ with column rank Δ as $\mathbf{B} = \begin{bmatrix}\mathbf{B}_1 & \mathbf{B}_2\end{bmatrix}$, where the square $\Delta \times \Delta$ submatrix $\mathbf{B}_1$ is nonsingular.

Choose a matrix $\mathbf{A}$ as $\mathbf{A} = \begin{bmatrix}\mathbf{A}_1 \\ \mathbf{A}_2\end{bmatrix}$, where the square $\Delta \times \Delta$ submatrix $\mathbf{A}_1$ will be chosen later. Let us require that

$$\mathbf{BA} = \mathbf{B}_1\mathbf{A}_1 + \mathbf{B}_2\mathbf{A}_2 = \gamma \mathbf{I}_\Delta,$$

where $\gamma \in GF(q^N)$ and $\gamma \neq -1$. Take from this equation

$$\mathbf{A}_1 = \mathbf{B}_1^{-1}\left(\gamma \mathbf{I}_\Delta - \mathbf{B}_2\mathbf{A}_2\right).$$

■

Corollary 1: It follows that

$$\mathbf{E}^2 = \mathbf{ABAB} = \mathbf{A}(\gamma \mathbf{I}_\Delta)\mathbf{B} = \gamma \mathbf{AB} = \gamma \mathbf{E}.$$

Theorem 1: Let $(\mathbf{P} + \mathbf{Z})^{-1} = \mathbf{R}(\mathbf{I} + \mathbf{E})\mathbf{Q}$, where $\mathbf{R}$ and $\mathbf{Q}$ are nonsingular matrices over $GF(q)$. Then

$$\mathrm{Rk}_{\mathrm{col}}(\mathbf{e}(\mathbf{P} + \mathbf{Z})^{-1}) \leq \mathrm{Rk}_{\mathrm{col}}(\mathbf{e}) + \Delta.$$

The column scrambler $\mathbf{P} + \mathbf{Z}$ is represented as $\mathbf{P} = \mathbf{Q}^{-1}\mathbf{R}^{-1}$; $Z = -\frac{1}{1+\gamma}\mathbf{Q}^{-1}\mathbf{E}\mathbf{R}^{-1}$.

Proof: It follows from lemmata above. ■

5. Secure variants of the GPT cryptosystem

Consider a public key of the form

$$\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k\end{bmatrix}(\mathbf{P} + \mathbf{Z}),$$

where $\mathbf{Y}$ is a $k \times t_1$ distortion matrix with column rank t_1, $\mathbf{G}_k$ is a $k \times n$ generator matrix of a MRD code, $\mathbf{P}$ is a square $(t_1 + n) \times (t_1 + n)$ nonsingular matrix over the base field $GF(q)$, $\mathbf{Z}$ is a $(t_1 + n) \times (t_1 + n)$ matrix with column rank Δ. A ciphertext for a plaintext $\mathbf{m}$ has the form

$$\mathbf{c} = \mathbf{m}\mathbf{G}_{\mathrm{pub}} + \mathbf{e} = \mathbf{m}\mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k\end{bmatrix}(\mathbf{P} + \mathbf{Z}) + \mathbf{e}, \qquad (27)$$

where an artificial error $\mathbf{e}$ has column rank t_3. An authorized party choose $t_3 + \Delta = \frac{n-k}{2}$. It allows to correct the emergent artificial error $\mathbf{e}(\mathbf{P} + \mathbf{Z})^{-1}$.

An unauthorized party does not know the matrix $(\mathbf{P} + \mathbf{Z})^{-1}$. Also one can not apply the second Overbeck attack since a scramble matrix $(\mathbf{P} + \mathbf{Z})$ is chosen over the extension field. There is still a possibility to use the first Overbeck attack. An unauthorized party tries to represent the public key over the superextension field $GF(q^{aN})$, where $a = \left\lceil \frac{t_1+n}{N} \right\rceil$. It allows to introduce a virtual generator matrix of extended MRD code of the form

$$\widehat{\mathbf{G}}_k = \begin{bmatrix}\mathbf{G}_k(t_1) & \mathbf{G}_k\end{bmatrix},$$

where $\mathbf{G}_k(t_1)$ is a $k \times t_1$ matrix of Frobenius-type over the superextension field. A column $\mathbf{f}$ is called Frobenius-type if it has the form $\mathbf{f} = \begin{pmatrix} f & f^{[1]} & \dots & f^{[k-1]}\end{pmatrix}^\top$. A matrix $\mathbf{F}$ is called Frobenius-type if it consists of Frobenius-type columns. By this assumption, the public key can be considered as follows:

$$\begin{aligned}\mathbf{G}_{\mathrm{pub}} &= \mathbf{S}\left[\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}}\right](\mathbf{P} + \mathbf{Z}) = \\ &= \mathbf{S}\left(\widehat{\mathbf{G}}_k\mathbf{P} + \widehat{\mathbf{Y}}\mathbf{P} + (\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}})\mathbf{Z}\right),\end{aligned} \qquad (28)$$

where

$$\widehat{\mathbf{Y}} = \begin{bmatrix}\mathbf{Y} - \mathbf{G}_k(t_1) & \mathbf{0}\end{bmatrix}.$$

The term $\widehat{\mathbf{G}}_k\mathbf{P}$ is a virtual $k \times (t_1 + n)$ generator matrix of an MRD code over the superextension field $\mathbb{F}_{q^{aN}}$. The term $\widehat{\mathbf{Y}}\mathbf{P}$ has column rank t_1. The term $(\widehat{\mathbf{G}}_k + \widehat{\mathbf{Y}})\mathbf{Z}$ has column rank Δ. The Overbeck–Gibson attack does not work if

$$t_1 + \Delta > \frac{t_1 + n - k}{2}.$$

Recall that an authorized user has chosen $t_3 + \Delta = \frac{n-k}{2}$. Hence we should choose $t_1 > 2t_3$ to prevent the Overbeck–Gibson attack.

Nevertheless it is possible to rewrite the public key (28) as an instance of Overbeck's attack:

$$\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y_1} + \mathbf{F}_1 & \mathbf{F}_2\end{bmatrix}(\mathbf{Q}),$$

where $\mathbf{F}_1$ is a $r \times t_1 + \Delta$ matrix, $\mathbf{F}_2$ is $k \times n - \Delta$ matrix such that the matrix $\begin{bmatrix}\mathbf{F}_1 & \mathbf{F}_2\end{bmatrix}$ is a generator matrix of a MRD $(t_1 + n, k, d)$ code over the superextension field $GF(q^{aN})$. The matrix $\mathbf{Y}_1$ is a new $k \times (t_1 + \Delta)$ distortion matrix. This approach is under investigation now.

Another way to prevent Overbeck's attack is given in Note 1. The cryptographer should choose a distortion $k \times t_1$ matrix $\mathbf{Y}$ such that the rank of the matrix $\mathbf{W}_{ext}$ satisfies the condition (22). Choose the matrix $\mathbf{Y}$ as follows:

$$\mathbf{Y} = \begin{bmatrix} \mathbf{m}_0 \\ \mathbf{m}_0^{[1]} + \mathbf{m}_1 \\ \mathbf{m}_0^{[2]} + \mathbf{m}_1^{[1]} + \mathbf{m}_2 \\ \mathbf{m}_0^{[3]} + \mathbf{m}_1^{[2]} + \mathbf{m}_2^{[1]} + \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_0^{[k-1]} + \mathbf{m}_1^{[k-2]} + \dots + \mathbf{m}_{k-1} \end{bmatrix}, \qquad (29)$$

where $\mathbf{m}_0$ is a vector of column rank t_1. Calculating the matrix $\mathbf{W}$ gives

$$\mathbf{W} = \sigma(\mathbf{Y}_1) - \mathbf{Y}_2 = -\begin{bmatrix} \mathbf{m}_1 \\ \mathbf{m}_2 \\ \mathbf{m}_3 \\ \vdots \\ \mathbf{m}_{k-1} \end{bmatrix}. \qquad (30)$$

Choose all vectors $\mathbf{m}_i$ over the *base field* $GF(q)$ in such a manner that the column rank of the matrix $\mathbf{W}$ is equal to

$t_1 - a$. Hence

$$\mathbf{W}_{\text{ext}} = \begin{bmatrix} \mathbf{W} \\ \sigma(\mathbf{W}) \\ \sigma^2(\mathbf{W}) \\ \dots \\ \sigma^{k-1}(\mathbf{W}) \end{bmatrix} = \begin{bmatrix} \mathbf{W} \\ \mathbf{W} \\ \mathbf{W} \\ \dots \\ \mathbf{W} \end{bmatrix}. \quad (31)$$

Therefore

$$\text{Rk}(\mathbf{W}_{\text{ext}} \mid GF(q^N)) = \text{Rk}(\mathbf{W} \mid GF(q^N) = t_1 - a,$$

and the condition (22) is satisfied.

In a similar manner we can show that even more secure variant of the GPT cryptosystem can be obtained if we use the general public key

$$\mathbf{G}_{\text{pub}} = \mathbf{S}\begin{bmatrix}\mathbf{Y} & \mathbf{G}_k + \mathbf{X}\end{bmatrix}(\mathbf{P} + \mathbf{Z}).$$

6. GPT-M in random network coding

We denote secure variants as GPT-M.

We consider the GPT cryptosystem which has been presented in [15].

We took the matrix $\mathbf{P} + \mathbf{Z}$ over the extension field $GF(q^N)$, or, the proper choice of the distortion matrix $\mathbf{Y}$. Then the Overbeck attack completely fails: all equations since (13) do not work.

Now, we consider a network with one source and one destination. The similar model was used in the work [18]. The difference is the following: we implement the GPT-M instead of the GPT.

The source transmits messages $\overline{\mathbf{u}} = (u_1 \dots u_k)$ which are enciphered by the cryptosystem GPT-M. As a result we have a ciphertext in vector representation $\mathbf{c} = (c_1 \dots c_n)$. The enciphered messages c_j are represented as n packets over the extension field. Each of them can be converted into vectors of length m over the base field. These packets are gathered in the matrix $\mathbf{M}$ with elements over the base field. A concatenation $\mathbf{V}$ of two matrices $\mathbf{M}$ and $\mathbf{I}_n$ is created.

$$\mathcal{V} = \left\{\mathbf{V} : \mathbf{V} = \begin{bmatrix}\mathbf{I}_n & \mathbf{M}\end{bmatrix}\right\}, \quad (32)$$

where $\mathbf{I}_n$ is the identity matrix of order n.

$V(1), \dots, V(n)$ are rows of the matrix $\mathbf{V}$. Then each row is a packet which has length $n+m$ and consists of elements over the base field $GF(q)$. The matrix $\mathbf{V}$ has size $n \times (n+m)$. Every packet is also an element of the finite field $GF(q^{n+m})$. In the Silva–Kötter–Kschischang network model [16] a message is a row spanned subspace of the matrix $\mathbf{V}$. Hence, the matrix $\mathbf{V}$ can be considered as a generator matrix of the subspace.

In this paper, to provide secure transmission in random network coding we focus on using the GPT public key cryptosystem to transmit encrypted messages and information on secret keys distribution. Both random network coding and the GPT cryptosystem are based on rank codes. It allows to combine in a most effective way the problems of deciphering and decoding. It is shown that our system provides secure communication in random network coding under definite conditions on the system parameters. In the GPT cryptosystem, a plaintext is an information vector $\mathbf{u}$ of dimension k over the extension field $GF(q^m)$. The corresponding ciphertext $\mathbf{c}$ is calculated as

$$\mathbf{c} = \mathbf{u}\mathbf{G}_{\text{pub}} + \mathbf{e}_{\text{art}}, \quad (33)$$

where the public key $\mathbf{G}_{\text{pub}}$ is a generator matrix of size $k \times n$ over the extension field $GF(q^m)$. It is a product of three matrices:

$$\mathbf{G}_{\text{pub}} = \mathbf{S}[\mathbf{Y}_k \;\; \mathbf{G}_k]\mathbf{P} + \mathbf{Z}.$$

In the network, every inner node calculates a random linear combination of the received packets which is express as operation:

$$\mathbf{Y} = \mathbf{A}\mathbf{V}, \quad (34)$$

where $\mathbf{A}$ is a matrix of the size $n_r \times n$ corresponding to all linear transformations at all inner nodes. If inside of the network there is an adversary, who insert his own packets in common flow, the network channel model is the following:

$$\mathbf{Y} = \mathbf{A}\mathbf{V} + \mathbf{E}_{\text{out}}, \quad (35)$$

where $\mathbf{A}$ is the same matrix as in (35), $\mathbf{E}_{\text{out}}$ is a matrix of size $n_r \times (n+m)$, which corresponds to the adversary messages. These messages are errors which a legal user has to correct.

At the receiver, packets $Y(1), \dots, Y(n_r)$ of length $n+m$ are gathered. The matrix $\mathbf{Y}$ of size $n_r \times (n+m)$ is constructed. For the random number n_r, we have three possibilities: be equal to n, or greater than, or less than n. The problem is to reconstruct $\mathbf{V}$ from $\mathbf{Y}$. To solve this problem it is necessary to do two rounds of linear transformations (see, [18] for details).

$\mathbf{A}$ is the matrix of size $n_r \times n$ corresponding to all the linear transformations at inner nodes. For the noncoherent network model, the matrix $\mathbf{A}$ is unknown but in our case we can find it. Represent the matrix $\mathbf{Y}$ as the concatenation of matrices $\mathbf{Y}_1$ and $\mathbf{Y}_2$, where the matrix $\mathbf{Y}_1$ has size $n_r \times n$.

We get at the receiver side the matrix $\mathbf{Y} = [\mathbf{A}\ \mathbf{A}\mathbf{M}]$, or, $\mathbf{Y}_1 = \mathbf{A}$. Therefore the matrix $\mathbf{A}$ is known in this case. Assume that the rank of $\mathbf{A}$ is equal to r, where $r \le n$.

Before decoding we fulfill the preliminary linear transformations over the matrix $\mathbf{Y}$ which correspond to the Gauss elimination procedure over $\mathbf{Y}_1 = \mathbf{A}$ and create the row reduced echelon form of the matrix $\mathbf{Y}_1$.

As a result of the first round we have (see, [17], for details)

$$\widehat{\mathbf{R}} = \mathbf{M} + \mathbf{L}\mathbf{M} + \mathbf{D}\mathbf{C} + \mathbf{E}_{\text{rest}}, \quad (36)$$

where the matrix $\mathbf{L}$ of rank $n - r$, and the matrix $\mathbf{C}$ of rank $n_r - r$ are known. Convert the matrix $\widehat{\mathbf{R}}$ over the base field into a vector $\widehat{\mathbf{r}}$ over the extended field:

$$\widehat{\mathbf{r}} = \mathbf{u}\mathbf{G}_{\text{pub}} + \mathbf{e}_{\text{art}} + \mathbf{a}(\mathbf{M}_1 + \mathbf{E}_{\text{art}}) + \mathbf{d}\mathbf{C} + \mathbf{e}_{\text{rest}}, \quad (37)$$

where the matrix $\mathbf{M}$ is converted into a vector $\mathbf{u}\mathbf{G}_{\text{pub}} + e_{\text{art}}$; the matrix $\mathbf{L}$ is converted into a vector $\mathbf{a}$ of rank $n - r$ with known coordinates; the matrix $\mathbf{D}$ is converted into a vector $\mathbf{d}$ of rank $n_r - r$ with unknown coordinates; the matrix $\mathbf{E}_{\text{rest}}$ is converted into an error vector $\mathbf{e}_{\text{rest}}$.

Then we have to do the second round of transformations. Choose a matrix $(\mathbf{P} + \mathbf{Z})^{-1}$ as in Eq. (**??**). Multiply on

the right the both sides of the equation (37) by the matrix $(\mathbf{P}+\mathbf{Z})^{-1}$:

$$\widehat{\mathbf{v}} \stackrel{def}{=} \mathbf{r}(\mathbf{P}+\mathbf{Z})^{-1} = \mathbf{uSG} + \mathbf{e}_{\mathrm{art}}(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{a}(\mathbf{M}_1+\mathbf{E}_{\mathrm{art}})(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{dC}(\mathbf{P}+\mathbf{Z})^{-1} + \mathbf{e}_{\mathrm{rest}}(\mathbf{P}+\mathbf{Z})^{-1}. \quad (38)$$

The first member $\mathbf{uSG}$ is a vector of the rank code. It corresponds to the information vector $\mathbf{u}$. The second member $\mathbf{e}_{\mathrm{art}}\mathbf{P}+\mathbf{Z}^{-1}$ is a vector of rank $t_2+\Delta$. The last three members we can take as row erasures, column erasures and additional errors. The rank of row erasures is $n-r$. The rank of column erasures (the matrix $\mathbf{C}$) is n_r-r. Denote the rank of the additional error by p. The next operation is rank decoding. Decoding will be successful, if the following inequality satisfies:

$$2(t_2+\Delta+p)+(n-r)+(n_r-r) \le d-1,$$

where $d=n-k+1$ is the rank distance of the code.

7. Conclusion

Secure capability of all versions GPT cryptosystems depends on values of its parameters.

The known decoding attacks can be prevent by a proper choice of parameters.

Overbeck's structural attack of 2008 year was successful, it had broken a version of GPT cryptosystem. To prevent new structural attacks of such type we have introduced structure and parameter changes. We propose a new family of column scramble matrices $\mathbf{P}+\mathbf{Z}$ to prevent structural attacks.

We use GPT-M cryptosystem in the network with random network coding. We show it provides secure communication in network under a definite condition on the system parameters.

8. Acknowledgment

This work was partially supported by Grant RFBR 12-07-00122-a.

9. References

[1] McEliece R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory// JPL DSN Progress Report 42–44, Pasadena, CA. P. 114–116, 1978.

[2] Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory// Probl. Control and Inform. Theory. V. 15. P. 19-34, 1986.
[3] Sidelnikov V.M., Shestakov S.O. On insecurity of cryptosystems based on generalized Reed-Solomon codes// Discrete Mathematics and Applications 2.

[4] Gabidulin E.M., Paramonov A.V., Tretjakov O.V. Ideals over a Noncommutative
Ring and Their Application in Cryptology// in: Advances in Cryptology — Eurocrypt '91, LNCS 547. P. 482–489.1991.

[5] Gibson J. K. Severely denting the Gabidulin version of the McEliece public key cryptosystem// J-DESIGNS-CODES-CRYPTOGR, 6(1):3745, July 1995.

[6] Gibson J. K. The security of the Gabidulin public-key cryptosystem", in: U. M. Maurer, ed. // Advances in Cryptology – EUROCRYPT'96, LNCS 1070. P. 212–223, 1996.

[7] R. Overbeck: "Extending Gibsons Attacks on the GPT Cryptosystem", Coding and Cryptography International Workshop, WCC 2005 Bergen, Norway, March 14-18, 2005. Lecture Notes in Computer Science 3969. P. 178-188.

[8] R.Overbeck Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes// Journal of Cryptology. V. 21, no 2, April 2008.

[9] Gabidulin E.M. Theory of Codes with Maximum Rank Distance// Probl. Inform. Transm. V. 21, No. 1. P. 1–12, July, 1985.

[10] Gabidulin E. M. A Fast Matrix Decoding Algorithm for Rank-Error-Correcting Codes// In G. Cohen, S. Litsyn, A. Lobstein, G. Zemor (Eds.) ALGEBRAIC CODING, pp. 126 - 133; Lecture Notes in Computer Science. V. 573, Springer-Verlag, 1991.

[11] Johansson T., Ourivski A.V. New technique for decoding codes in the rank metric and its cryptography applications//Problems Inform. Transm. 38(3). P. 237-246, 2002.

[12] Gaborit P., Ruatta O., Schrek J. On the complexity of the Rank Syndrome Decoding Problem//arXiv:1301.1026v1[cs.CR] 6 Jan 2013.

[13] Levy-dit-Vehel1 F., Jean-Charles Faug'ere J.-Ch., Perret L. Cryptanalysis of MinRank, in: Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008, Proceedings. Series: Lecture Notes in Computer Science. Subseries: Security and Cryptology , Vol. 5157. Wagner, David (Ed.). P. 280-296.2008.

[14] Gabidulin E.M, Pilipchuk N.I., Ourivski A.V. Security of the modified GPT cryptosystem// Proc. ITA, San Diego, February 2014.

[15] Gabidulin E.M., Pilipchuk N.I. GPT Cryptosystem for Information Network Security // International Conference on Information Society (i-Society 2013). i-Society 2013 Proceedings. June 24-26, 2013, Toronto, Canada. P. 21-25.

[16] Silva D., Kschischang F. R., Koetter R. A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. 9. P. 3951-3967.

[17] Gabidulin E.M., Pilipchuk N.I., Bossert M. Decoding of the random network codes// Problems of Information Transmission. V.46, issue 4. P.300-320. 2010.

[18] Gabidulin E.M., Pilipchuk N.I., Honary B., Rashwan H. Information security in a random network coding network// Problems of Information Transmission. V.49, issue 2. P.179-191, 2013.