Rank-metric codes and applications

Ernst M. Gabidulin
Moscow Institute of Physics and Technology (State University)
Email: ernst.gabidulin@gmail.com

Abstract

The State of Art for rank codes is represented. The theory and applications are considered.

1 Rank Codes

1.1 Definition

There exist two representations of Rank codes: *matrix* representation and *vector* representation.
In *matrix* representation, rank codes are defined as subsets of a normed space $\{\mathbb{F}_q^{N\times n},\ \mathrm{Rk}\}$ of $N \times n$ matrices over a finite (base) field F_q, where the norm of a matrix $M \in \mathbb{F}_q^{N\times n}$ is defined to be the algebraic rank $\mathrm{Rk}(M)$ of this matrix over $\mathbb{F}_q$. The *rank distance* between two matrices M_1 and M_2 is the rank of their difference $\mathrm{Rk}(M_1 - M_2)$. The *rank distance* of a matrix rank code $\mathcal{M} \subset \mathbb{F}_q^{N\times n}$ is defined as the minimal pairwise distance: $d(\mathcal{M}) = d = \min(\mathrm{Rk}(M_i - M_j) : M_i, M_j \in \mathcal{M},\ i \neq j)$.
In *vector* representation, rank codes are defined as subsets of a normed n-dimensional space $\{\mathbb{F}_{q^N}^n,\ \mathrm{Rk}\}$ of n-vectors over an extension field $\mathbb{F}_{q^N}$, where the norm of a vector $\mathbf{v} \in \mathbb{F}_{q^N}^n$ is defined to be the *column* rank $\mathrm{Rk}(\mathbf{v} \mid \mathbb{F}_q)$ of this vector over $\mathbb{F}_q$, i.e., the maximal number of coordinates of $\mathbf{v}$ which are linearly independent over the base field $\mathbb{F}_q$. The *rank distance* between two vectors $\mathbf{v}_1,\ \mathbf{v}_2$ is the column rank of their difference $\mathrm{Rk}(\mathbf{v}_1 - \mathbf{v}_2 \mid \mathbb{F}_q)$. The *rank distance* of a vector rank code $\mathcal{V} \subset \mathbb{F}_{q^N}^n$ is defined as the minimal pairwise distance: $d(\mathcal{V}) = d = \min(\mathrm{Rk}(\mathbf{v}_i - \mathbf{v}_j) : \mathbf{v}_i, \mathbf{v}_j \in \mathcal{V},\ i \neq j)$.

1.2 Background

Algebraic coding theory may be considered as the theory of subsets of a certain *normed* finite-dimensional space Γ over the finite field equipped with a norm function $\mathfrak{N}$. The most known norm in coding theory is the Hamming weight of a vector. It turns out that the rank function $\mathrm{Rk}(A)$ of matrices A over fields can be considered as the norm function. In particular, the well-known inequalities for sums of matrices $|\mathrm{Rk}(A)-\mathrm{Rk}(B)| \leq \mathrm{Rk}(A+B) \leq$

$\mathrm{Rk}(A) + \mathrm{Rk}(B)$ define implicitly the rank distance relations on the space of all matrices of identical size. Explicitly, the concept of the rank metric was introduced by Loo-Keng Hua [1] as "Arithmetic distance". Philippe Delsarte [2] defined the rank distance (or, q-distance) on the set of bilinear forms (equivalently, on the set of rectangular matrices) and proposed the construction of optimal codes in *bilinear form* representation. Ernst M. Gabidulin [3] introduced the rank distance for vector spaces over extension fields and found connections between rank codes in the *vector* representation and in the *matrix* representation. Optimal codes in *vector* representation were described. Fast coding and decoding algorithms were proposed for optimal codes.

2 Theory

The normed spaces $\{\mathbb{F}_q^{N\times n},\ \mathrm{Rk}\}$ and $\{\mathbb{F}_{q^N}^n,\ \mathrm{Rk}\}$ are isomorphic isometrically. Let a basis $\Omega = \{\omega_1, \omega_2, \ldots, \omega_N\}$ of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ be chosen. Then each vector $\mathbf{v} = \begin{bmatrix} v_1 & v_2 & \ldots & v_n \end{bmatrix} \in \mathbb{F}_{q^N}^n$ can be mapped into the $N \times n$ matrix $M \in \mathbb{F}_q^{N\times n}$ by replacing each coordinate v_j with the N-column consisting of coefficients in representing v_j by the basis Ω. This mapping is bijective and isometric.
Given a rank code $\mathcal{M}$ in matrix representation one can construct a rank code $\mathcal{V}$ in vector representation with the same size, code distance and pairwise distances, and vice versa.
The size $|\mathcal{M}| = |\mathcal{V}|$ of related codes with code distance d satisfy the Singleton bound $|\mathcal{M}| = |\mathcal{V}| \leq \min(q^{N(n-d+1)}, q^{n(N-d+1)})$. Codes reaching this bound are called maximum rank distance codes, or, MRD codes.
A rank code $\mathcal{M}$ in matrix representation is called $\mathbb{F}_q$-*linear* if $\mathcal{M}$ is a subspace of $\mathbb{F}_q^{N\times n}$.
A rank code $\mathcal{V}$ in vector representation is called $\mathbb{F}_{q^N}$-*linear* if $\mathcal{V}$ is a subspace of $\mathbb{F}_{q^N}^n$.
Mapping a $\mathbb{F}_{q^N}$-*linear* code $\mathcal{V}$ in vector representation into related code $\mathcal{M}$ in matrix representation results in a $\mathbb{F}_q$-*linear* code.
Mapping a $\mathbb{F}_q$-*linear* code $\mathcal{M}$ in matrix representation into related code $\mathcal{V}$ in vector representation results in *not necessary* a $\mathbb{F}_{q^N}$-*linear* code.
Constructions of $\mathbb{F}_q$-*linear* rank codes in the matrix representation and $\mathbb{F}_{q^N}$-*linear* rank codes in the vector representation will be considered.

2.1 Delsarte's optimal rank codes in matrix representation

Delsarte's construction of rank codes in bilinear form representation is presented here in matrix representation.
Assume that $n \leq N$. Let $\mathrm{Tr}(x) = \sum_{l=0}^{N-1} x^{q^l},\ x \in \mathbb{F}_{q^N}$, be the Trace function from $\mathbb{F}_{q^N}$ into $\mathbb{F}_q$. Let d be an integer in $\{1, 2, \ldots, n\}$. Let $\mathbf{u} = \begin{bmatrix} u_0 & u_1 & \ldots & u_{n-d} \end{bmatrix} \in \mathbb{F}_{q^N}^{n-d+1}$. Let $\mu_1, \mu_2, \ldots, \mu_n$ be linearly independent elements of $\mathbb{F}_{q^N}$. Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_N\}$ be a basis for $\mathbb{F}_{q^N}$.
Define a code in matrix representation as the set of $N\times n$ matrices $\mathcal{M} = \left\{ M(\mathbf{u}) = [M_{ij}(\mathbf{u})] : \mathbf{u} \in \mathbb{F}_{q^N}^{n-d+1} \right\}$

where

$$M_{ij}(\mathbf{u}) = \mathrm{Tr}\left(\sum_{s=0}^{n-d} u_s \omega_i \mu_j^{q^s}\right).$$

Then $\mathcal{M}$ is a rank code with code distance d reaching the Singleton bound $|\mathcal{M}| = q^{N(n-d+1)}$. Let $A_i(n,d),\ i = 0,1,\ldots,n$, be the number of code matrices with rank i. The weight distribution is as follows:

$$\begin{array}{ll} A_0(n,d) = 1, & i = 0 \\ A_i(n,d) = 0, & i = 1,\ldots,d-1. \end{array}$$

$$A_i(n,d) = \begin{bmatrix} n \\ i \end{bmatrix} \sum_{s=0}^{i-d} (-1)^s \begin{bmatrix} i \\ s \end{bmatrix} q^{\frac{s(s-1)}{2}} (q^{N(d-i+1-s)} - 1),$$

if $i = d,\ldots,n$, where $\begin{bmatrix} n \\ i \end{bmatrix} = \prod_{j=0}^{i-1} \frac{q^n - q^j}{q^i - q^j}$ is the Gaussian binomial coefficient.

2.2 Optimal rank codes in vector representation

A $\mathbb{F}_{q^N}$-linear vector code $\mathcal{V}$ is a subspace of the normed space $\{\mathbb{F}_{q^N}^n,\ \mathrm{Rk}\}$. Denote by (n,k,d) a code $\mathcal{V}$ of dimension $k \le n$ and rank distance d. Such a code can be described in terms of a full rank *generator* matrix G_k over the extension field F_{q^N} of size $k \times n$. Code vectors $\{\mathbf{v}\}$ are all linear combinations of this matrix. Thus the size of a code is equal to $|\mathcal{V}| = q^{Nk}$.

Equivalently, a rank code $\mathcal{V}$ can be described in terms of a full rank *parity-check* matrix H_{n-k} over $\mathbb{F}_{q^N}$ of size $(n-k) \times n$. It satisfies the condition $G_k H_{n-k}^\top = O$, where O is the all zero $k \times (n-k)$ matrix. Code vectors $\{\mathbf{v}\}$ are all solutions of the linear system of equation $\mathbf{v} H_{n-k}^\top = \mathbf{0}$.

For optimal (MRD) codes, it must be $k = n - d + 1$, or, $n - k = d - 1$.

General constructions of MRD codes in terms of parity-check matrices can be described as follows. Let $h_1, h_2, \ldots, h_n$ be a set of elements from the extension field $\mathbb{F}_{q^n}$ *linearly independent* over the base field $\mathbb{F}$. Let s be a positive integer such that $\gcd(s,N) = 1$. Then a parity matrix of the form

$$H_{d-1} = \begin{bmatrix} h_1 & h_2 & \ldots & h_n \\ h_1^{q^s} & h_2^{q^s} & \ldots & h_n^{q^s} \\ h_1^{q^{2s}} & h_2^{q^{2s}} & \ldots & h_n^{q^{2s}} \\ \ldots & \ldots & \ldots & \ldots \\ h_1^{q^{(d-2)s}} & h_2^{q^{(d-2)s}} & \ldots & h_n^{q^{(d-2)s}} \end{bmatrix}.$$

defines an MRD (n,k,d) code with code length $n \le N$, dimension $k = n - d + 1$ and rank distance $d = n - k + 1$.

Equivalently, general constructions of MRD codes can be described in terms of generator matrices. Let $g_1, g_2, \ldots, g_n$ be a set of elements from the extension field $\mathbb{F}_{q^n}$ *linearly*

independent over the base field $\mathbb{F}$. Then a generator matrix of the form

$$G_k = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{q^s} & g_2^{q^s} & \cdots & g_n^{q^s} \\ g_1^{q^{2s}} & g_2^{q^{2s}} & \cdots & g_n^{q^{2s}} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{q^{(k-1)s}} & g_2^{q^{(k-1)s}} & \cdots & g_n^{q^{(k-1)s}} \end{bmatrix}.$$

defines an MRD (n, k, d) code with code length $n \leq N$, dimension $k = n - d + 1$ and rank distance $d = n - k + 1$. The weight distribution of vector MRD codes coincides for a given d with the weight distribution of Delsarte's codes above.

The case $s = 1$ is used mostly.

No other constructions of MRD codes are known (2009).

2.3 Correcting rank errors and rank erasures

Let a MRD $(n, k, d = n - k + 1)$ code $\mathcal{V}$ be given. Let a transmitted signal be $\mathbf{v}$ and received signal be $\mathbf{y} = \mathbf{v} + \mathbf{e}_{\text{total}}$, where $\mathbf{e}_{\text{total}}$ is an error. The code $\mathcal{V}$ can correct *in general* vector errors of the form

$$\begin{aligned} \mathbf{e}_{\text{total}} &= \mathbf{e} + \mathbf{e}_{\text{row}} + \mathbf{e}_{\text{col}} \\ &= e_1\mathbf{u}_1 + e_2\mathbf{u}_2 + \cdots + e_t\mathbf{u}_t + \\ &+ a_1\mathbf{r}_1 + a_2\mathbf{r}_2 + \cdots + a_v\mathbf{r}_v + \\ &+ w_1\mathbf{c}_1 + w_2\mathbf{c}_2 + \cdots + w_l\mathbf{c}_l \end{aligned}$$

provided that $2t + v + l \leq d - 1$.

The part $\mathbf{e} = e_1\mathbf{u}_1 + e_2\mathbf{u}_2 + \cdots + e_t\mathbf{u}_t$ is called a *random rank error* of rank t under assumption that elements $e_i \in \mathbb{F}_{q^N}$ are linearly independent over the base field $\mathbb{F}_q$ and *unknown* to the decoder; n-vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_t$ have coordinates in the *base* field $\mathbb{F}_q$, are linearly independent over the base field $\mathbb{F}_q$ and also *unknown* to the decoder. The rank t is *unknown* to the decoder.

The part $\mathbf{e}_{\text{row}} = a_1\mathbf{r}_1 + a_2\mathbf{r}_2 + \cdots + a_v\mathbf{r}_v$ is called a *vector rank* ***row*** *erasure with side information* under assumption that elements $a_i \in \mathbb{F}_{q^N}$ are linearly independent over the base field $\mathbb{F}$ and *known* to the decoder; n-vectors $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_v$ have coordinates in the *base* field $\mathbb{F}_q$, are linearly independent over the base field $\mathbb{F}_q$ and *unknown* to the decoder.

The part $\mathbf{e}_{\text{col}} = w_1\mathbf{c}_1 + w_2\mathbf{c}_2 + \cdots + w_l\mathbf{c}_l$ is called a *vector rank* ***column*** *erasure with side information* under assumption that elements $w_i \in \mathbb{F}_{q^N}$ are linearly independent over the base field $\mathbb{F}_q$ and are *unknown* to the decoder; n-vectors $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_l$ have coordinates in the base field $\mathbb{F}_q$, are linearly independent over the base field $\mathbb{F}_q$ and *known* to the decoder.

First fast correcting random rank errors only was proposed in [3]. The algorithm is based on the extended Euclidean division algorithm for linearized polynomials. There exist several further modifications.

Algorithms for correcting random rank errors and rank erasures simultaneously are proposed in [4], [5], [7].

3 Applications

3.1 Rank codes as space-time codes

Space-time codes are introduced by Tarokh, Jafarkhani, and Calderbank in 1998 [10]. Codes are designed to simultaneously take advantage of two dimensions, namely the spatial diversity of antenna elements, and coding gain introduced by designed redundancy in the time dimension.

It is assumed that the base station is equipped with T transmit antennas and the terminal is equipped with m receiving antennas. A signal is transmitted in time slots $1, 2, \ldots, n$.

The received signal can be written as a $m \times n$ matrix

$$\mathbf{Y} = \mathbf{AC} + \mathbf{N}.$$

$\mathbf{C}$ is a $T \times n$ signal code matrix with entries in some constellation.

$\mathbf{A}$ is a $m \times T$ is a matrix of complex transfer coefficients from the jth transmit antenna to the ith receiving antenna.

$\mathbf{N}$ is an AWGN $m \times n$ matrix.

The Full rank criterion was proposed:

Choose a matrix code $\mathrm{C} = \{\mathbf{C}_i\}$ **in such a manner that the difference** $\mathbf{C}_{i,j} = \{\mathbf{C}_i - \mathbf{C}_j\}$ **has full rank.**

MRD codes over finite fields can not be used directly as space-time codes. However, it is still possible to use MRD codes over finite fields as *templates*.

Non-constructive statement. There exist infinitely many of finite complex or real constellations such that differential MRD codes (i.e. full rank of difference matrices) can be constructed.

Constructive statement. MRD codes over the binary field can be transformed to differential MRD codes over the complex or real constellations of size 2.

Constructive statement. For $T = 2, 4, 8$ and $q = 2^s$, MRD codes over $\mathbb{F}_q$ can be transformed to differential MRD codes over complex constellations of size q.

Constructive statement. MRD codes over $\mathbb{F}_p$, $p \equiv 1 \mod 4$, can be transformed to differential MRD codes over the complex Gaussian field of size p.

Decoding differential MRD codes is reduced to decoding in finite field by hard-decision algorithms.

Problem: For known matrix $\mathbf{A}$, use Gauss elimination in $\mathbf{A}$ for getting rank erasures instead of rank errors.

3.2 Rank codes in network coding

Consider a communication network, where a single source transmits information to a single destination. The model of a network was proposed and investigated in [4]. The source

formats the information to be transmitted into N packets $X(1), \ldots, X(N)$ of length $N+n$ over the finite field $\mathbb{F}_q$ and constructs a $(N \times (N+n))$ matrix X with these packets as rows. The source choose a code $\mathcal{X}$ consisting of matrices X which can be transmitted.

Each intermediate node calculates random linear combinations of ingoing packets, where a packet is represented as an element of a finite field $\mathbb{F}_{q^{N+n}}$. The node retransmits randomly calculated packets. Therefore, the destination collects a random number N_r of packets $Y(1), \ldots, Y(N_r)$ of length $N+n$ and creates a $N_r \times (N+n)$ matrix Y.

The problem is to recover the original packets $X(1), \ldots, X(N)$, or the matrix X from the received matrix Y.

Koetter and Kschischang [6] introduce the concept of subspace codes when an alphabet of transmitted messages consists of subspaces, not symbols. They constructed a family of subspace codes. Silva, Kschischang, Koetter, proposed a rank-metric approach to error control in random network coding [7]. Silva and Kschischang proposed their algorithms of fast encoding and decoding of Gabidulin codes [8].

The basic model of a channel induced by random network coding is described as follows. The transmitted matrix X and the received matrix Y are connected by the relation $Y = AX + BZ$, where A is an $N_r \times N$ matrix corresponding to the overall linear transformation applied by intermediate nodes of the network; Z is an $l \times (N+n)$ matrix whose rows are the error packets $z_1, \cdots, z_l$; B is an $N_r \times l$ matrix corresponding to the overall linear transformation applied to $z_1, \ldots, z_l$ on route to the destination. The number of nonzero rows of Z gives the total number of corrupt packets injected in the network. Random matrices A, B, Z are unknown to the destination.

It is proposed to apply so called lifting construction for constructing a code $\mathcal{X}$. Each matrix $X \in \mathcal{X}$ has the form $X = \begin{bmatrix} I_N & M \end{bmatrix}$, where I_N is the identity matrix of order N while $M \in \mathcal{M}$ is a code matrix of some matrix code $\mathcal{M}$ consisting of $N \times n$ matrices over the field $\mathbb{F}_q$. A code $\mathcal{M}$ is assumed to be a MRD *rank code* with rank distance d, if $n \leq N$, or a transposed MRD rank code, if $N < n$. The corresponding code $\mathcal{X}$ were analyzed in The basic model of a channel induced by random network coding is described as follows. The transmitted matrix X and the received matrix Y are connected by the relation $Y = AX + BZ$, where A is an $N_r \times N$ matrix corresponding to the overall linear transformation applied by intermediate nodes of the network; Z is an $l \times (N+n)$ matrix whose rows are the error packets $z_1, \cdots, z_l$; B is an $N_r \times l$ matrix corresponding to the overall linear transformation applied to $z_1, \ldots, z_l$ on route to the destination. The number of nonzero rows of Z gives the total number of corrupt packets injected in the network. Random matrices A, B, Z are unknown to the destination.

It is proposed in [7] to apply so called lifting construction for constructing a code $\mathcal{X}$. Each matrix $X \in \mathcal{X}$ has the form $X = \begin{bmatrix} I_N & M \end{bmatrix}$, where I_N is the identity matrix of order N while $M \in \mathcal{M}$ is a code matrix of some matrix code $\mathcal{M}$ consisting of $N \times n$ matrices over the field $\mathbb{F}_q$. A code $\mathcal{M}$ is assumed to be a MRD *rank code* with rank distance d, if $n \leq N$, or a transposed MRD rank code, if $N < n$. The corresponding code $\mathcal{X}$ were analyzed in [7]. Decoding codes $\mathcal{X}$ can be reduced to decoding embedded rank codes $\mathcal{M}$. If the matrix $X = \begin{bmatrix} I_N & M \end{bmatrix}$ is transmitted, then the matrix $Y = AX + BZ = \begin{bmatrix} A + BZ_1 & AM + BZ_2 \end{bmatrix}$ is received with unknown to the destination matrices A, B, Z_1, Z_2. By a linear transformation

of rows and injecting all zero rows, the part $\left[A + BZ_1\right]$ can be reduced to the upper triangular matrix of order N. Elements of the main diagonal are "0"'s or "1"'s. The number of "1"'s is equal to the rank of $\left[A + BZ_1\right]$. The same operations over the matrix $\left[AM + BZ_2\right]$ allows to extract the submatrix of the form $R = M + LM + DC$, where R, L and C are known matrices. Thus, the result is a matrix M of the rank code $\mathcal{M}$ corrupted by a *row* rank erasure LM and a *column* rank erasure DC. The unknown matrix M can be uniquely recovered from R provided that $\mathrm{Rk}(L) + \mathrm{Rk}(C) \leq d - 1$.
Other network codes are known generalizing constructions above (see,[9]).. Decoding codes $\mathcal{X}$ can be reduced to decoding embedded rank codes $\mathcal{M}$. If the matrix $X = \left[I_N \quad M\right]$ is transmitted, then the matrix $Y = AX + BZ = \left[A + BZ_1 \quad AM + BZ_2\right]$ is received with unknown to the destination matrices A, B, Z_1, Z_2. By a linear transformation of rows and injecting all zero rows, the part $\left[A + BZ_1\right]$ can be reduced to the upper triangular matrix of order N. Elements of the main diagonal are "0"'s or "1"'s. The number of "1"'s is equal to the rank of $\left[A + BZ_1\right]$. The same operations over the matrix $\left[AM + BZ_2\right]$ allows to extract the submatrix of the form $R = M + LM + DC$, where R, L and C are known matrices. Thus, the result is a matrix M of the rank code $\mathcal{M}$ corrupted by a *row* rank erasure LM and a *column* rank erasure DC. The unknown matrix M can be uniquely recovered from R provided that $\mathrm{Rk}(L) + \mathrm{Rk}(C) \leq d - 1$.
Other network codes are known generalizing constructions above (see, GabBoss:2009).

It is shown that decoding this subspace code is equivalent to correcting random errors and generalized erasures in the rank code [5].

3.3 Rank codes in cryptography

The McEliece like public key cryptosystem but based on *rank* error correcting codes was proposed by Gabidulin, Paramonov, Tretjakov in 1991 [**?**]. The cryptosystem is described as follows. The public key $\mathbf{G}_{\mathrm{pub}}$ is a left and right scrambled generator matrix of a rank code:

$$\mathbf{G}_{\mathrm{pub}} = \mathbf{S}\mathbf{G}_k\mathbf{P}.$$

The matrix $\mathbf{G}_k$ is used to correct rank errors of rank not greater than $t = \left\lfloor \frac{n-k}{2} \right\rfloor$.
A matrix $\mathbf{S}$ over the extension field $\mathbb{F}_{q^n}$ is called the row scrambling matrix. It is used to destroy any visible structure of the matrix $\mathbf{G}_k$ by mixing its rows.
A matrix $\mathbf{P} = \left[p_{ij}\right]$ is called the column scrambler. This matrix is a non singular square matrix of order n. It is used to mix columns of $\mathbf{G}_k$.

Another generator matrix has the form

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

Plaintext is any k-vector

$$\mathbf{m} = (m_1, m_2, \ldots, m_k), m_s \in \mathbb{F}_{q^n},\ s = 1, 2, \ldots, k.$$

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

Encryption.The ciphertext is given by

$$\mathbf{c} = \mathbf{mG}_{pub} + \mathbf{e} = \mathbf{mS}[\mathbf{X}|\mathbf{G}_k]\mathbf{P} + \mathbf{e},$$

where $\mathbf{e}$ is an artificial vector of errors of rank t_2.
Decryption The legitimate receiver upon receiving $\mathbf{c}$ calculates

$$\mathbf{c}' = \mathbf{cP}^{-1} = \mathbf{mS}[\mathbf{X}|\mathbf{G}_k] + \mathbf{eP}^{-1}.$$

Then he extracts from $\mathbf{c}'$ the plaintext $\mathbf{m}$ using decoding algorithms and properties of public keys.

Attacks and counter-attacks

Rank codes are well structured. It makes easier creation of attacks.

Subsequently in a series of works, Gibson [12], [13], [14] developed attacks that break the system for practical instances.

Several variants of PKC were introduced to withstand Gibson's attacks [15].

Recently, R. Overbeck [16], [17] proposed a new attack which is more effective than Gibson's attacks. His method is based on the fact that a column scrambler $\mathbf{P}$ is defined over the *base field*.

It was found [18], [19] that a cryptographer can define a proper column scrambler over the *extension field without violation* of the standard mode of the PKC. Overbeck's attack fails in this case.

Conclusion

- Theory of rank codes is of great interest for many researchers.
- Fast decoding algorithms are developed.
- Applications in many areas are possible and recommended. Space-time coding, random network coding, public key cryptosystems are areas of such applications.

References

[1] Hua, Loo-Keng, *A theorem on matrices over a sfield and its applications*, Chinese mathematical society. Vol. 1, No. 2, pp. 109-163, 1951.

[2] Delsarte, P., *Bilinear Forms over a Finite Field, with Applications to Coding Theory*, Journal of Combinatorial Theory A, vol. 25, pp. 226-241, 1978.

[3] Gabidulin, E. M., *Theory of codes with maximum rank distance*, Problems on Information Transmission, vol. 21, no. 1, pp. 1-12, Jan. 1985.

[4] Gabidulin, E.M., Paramonov, A.V., Tretjakov O.V., *Rank Errors and Rank Erasures Correction*, Proceedings of the 4th International Colloquium on Coding Theory, 30 Sept. - 7 Oct. 1991, Dilijan, Armenia, pp. 11-19, Yerevan, 1992.

[5] Gabidulin, E.M., Pilipchuk, N.I., *Error and erasure correcting algorithms for rank codes*, Designs, Codes and Cryptography, Springer Netherlands, DOI 10.1007/s10623-008-9185-7. V.49, 2008, pp.105-122.

[6] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," in *Proceedings of 2007 IEEE International Symposium on Information Theory (ISIT 2007)*, Nice, France, 24-29 June 2007, pp. 791-795.

[7] Silva, D., Kschischang, F.R., Koetter, R., *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54, pp. 3951-3967, No. 9, Sept. 2008.

[8] D. Silva and F. R. Kschischang, "Fast Encoding and Decoding of Gabidulin Codes." *Proc. of 2009 IEEE International Symposium on Information Theory*, ISIT'09, 2009.

[9] Gabidulin, E.M., Bossert, M. *Algebraic Codes in Network Coding*. Probl. Inform. Transm. Vol. 45. Issue 4, pp. 3–17. December, 2009.

[10] Tarokh, V., Jafarkhani, H., and Calderbank, A.R. *Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction*, IEEE Transactions on Information Theory, vol. 44, pp. 744-765, No. 2, March 1998.

[11] Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V. *Ideals over a Non-commutative Ring and Their Application in Cryptology*. Advances in Cryptology — Eurocrypt '91. Editor: Davies, D.W. Lecture Notes in Computer Science, No. 547, pp. 482–489, Berlin and Heidelberg: Springer-Verlag, 1991.

[12] J.K. Gibson, "Severely Denting the Gabidulin Version of the McEliece Public Key Cryptosystem," in: *Designs, Codes and Cryptography*, 1993.

[13] J. K. Gibson, "Severely denting the Gabidulin version of the McEliece public key cryptosystem," // *Designs, Codes and Cryptography, 6(1)*, 1995, pp. 37–45.

[14] J. K. Gibson, "The security of the Gabidulin public-key cryptosystem," // *Advances in Cryptology – EUROCRYPT'96, LNCS 1070*, 1996, pp. 212–223.

[15] Ourivski A.V., Gabidulin E.M. *Column scrambler for the GPT cryptosystem*// Discrete Applied Mathematics.-128 (2003)P.207-221.

[16] Overbeck R. *A new structural attack for GPT and variants*. Proc of Mycrypt'2005, V. 3517 of LNCS P.5-63, Springer–Verlag, 2005.

[17] Overbeck R., "Brute-force attacks Public Key Cryptosystem Based on Gabidulin codes." *J. Cryptology*, 21(2): 280-301 (2008).

[18] Gabidulin E.M. *Attacks and counter-attacks on GPT public key cryptosystem*. Designs, Codes and Cryptography, Springer Netherlands, DOI 10.1007/s10623-008-9185-7. V.49, N 2, 2008. P.171-177.

[19] E. M. Gabidulin, H.Rashwan and B. Honary,, "On improving security of GPT cryptosystems." IEEE International Symposium on Information Theory , June 2009.