The modified Niederreiter cryptosystem based on new metric

Marina Churusova churuss@yandex.ru
Ernst M. Gabidulin gab@mail.mipt.ru
Moscow Institute of Physics and Technology

Abstract

In the original Niederreiter cryptosystem, a ciphertext is a syndrome $\underline{c} = \underline{m}\mathbf{H}^{\mathbf{T}}_{\mathbf{cr}}$, where $\underline{m}$ is a plaintext and $\mathbf{H}_{cr}$ is a scrambled parity check matrix of a generalized Reed – Solomon code. This system was broken by Sidel'nikov and Shestakov. Later on, a modification was proposed with $\underline{c} = \underline{m}(\mathbf{H}^T_{cr} + \mathbf{X})$, where $\mathbf{X}$ is a generator matrix of a code in *the Vandermonde metric*. This version is unbroken. We extend the idea above in two directions: we use a scrambled parity check matrix of a *rank* code and we introduce a *new metric* associated with rank codes instead of generalized Reed – Solomon codes.

1 Introduction

Let $GF(q)$ be a base field and $GF(q^N)$ be an extension field of degree N. Let $GF(q^N)^n$ be the vector space of dimension n over $GF(q^N)$. Two basic public-key cryptosystems based on linear codes were proposed: the McEliece system [1] and the Niederreiter system [2]. We consider the Niederreiter system and its modifications.

The idea of the Niederreiter cryptosystem is as follows.

Private key consists of:

- a parity check matrix $\mathbf{H} = \left[z_j x_j^i\right]$, $z_j, x_j \in GF(q)$, $z_j \neq 0$, x_j different, $i = 0, 1, \ldots, r-1$; $j = 1, 2, \ldots, n$, of a generalized Reed – Solomon code and a fast decoding algorithm for this code;
- a random nonsingular scrambling $r \times r$ matrix $\mathbf{S}$. This matrix destroys a visible structure of the parity check matrix.

Public key is a scrambled parity check matrix $\mathbf{H}_{cr} = \mathbf{SH}$.

A plaintext $\underline{m}$ is an n-vector with coordinates in $GF(q)$ and with the Hamming weight less or equal to $\lfloor \frac{r}{2} \rfloor$.

The corresponding ciphertext is calculated as

$$\underline{c} = \underline{m}\mathbf{H}_{cr}^{T} = \underline{m}\mathbf{H}^{T}\mathbf{S}^{T}.$$

Upon receiving a ciphertext $\underline{c}$, an authorized user multiplies a ciphertext to the right by matrix $(\mathbf{S^T})^{-1}$ and applies his secret fast decoding algorithm to extract the initial plaintext $\underline{m}$.

The Niederreiter cryptosystem was broken in [3, 4].

In [5] and [6], modifications of the Niederreiter system were proposed. In [5], a method of random distortion of the parity check matrix was used, still in frame of the Hamming metric. Rank of the distortion matrix is equal to 1. In [6], an idea was proposed to use the so-called Vandermonde metric associated with generalized general Reed-Solomon codes. In this case, rank of a distortion matrix can be chosen greater than 1.

In this paper, we propose a new metric associated with rank codes to modify the Niederreiter system.

This metric is a special case of the general family of metrics (see, [7] for details). We proposed optimal codes that correct errors in the new metric. Errors to be corrected have large weights in the rank metric but rather small weight in the new metric.

It is shown that correcting of errors in the new metric can be replaced by decoding some rank code.

We proposed a new modification of the Niederreiter cryptosystem.

2 Metric associated with rank code

2.1 Definition

Let $\mathbf{F}$ be a $N \times n$ matrix in a field $\mathcal{F}$ such that $N \geq n$ and $\mathrm{rank}(\mathbf{F}) = n$. Denote by $\underline{f}_1, \underline{f}_2, \ldots, \underline{f}_N$ rows of $\mathbf{F}$. We can introduce a *metric* associated with the matrix $\mathbf{F}$ as follows [7].

Denote $\mathcal{A} = \{\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_N),\ \alpha_j \in \mathcal{F}\}$ the set of all vectors such that

$$\underline{x} = \sum_{i=1}^{N} \alpha_i \underline{f}_i.$$

This set is not empty because $\mathrm{rank}(\mathbf{F}) = n$. Let $d_H(\underline{\alpha})$ be the Hamming weight of $\underline{\alpha}$.

Definition 1 *The* $\mathbf{F}$*-norm of* $\underline{x}$ *is defined as*

$$N_F(\underline{x}) = \min_{\underline{\alpha}=(\alpha_1,\ldots,\alpha_N)\in\mathcal{F}^N} \left(d_H(\underline{\alpha}) \mid \underline{\alpha} \in \mathcal{A},\ \sum_{i=1}^{N} \alpha_i \underline{f}_i = \underline{x} \right).$$

If we take as $\mathbf{F}$ the transposed parity check matrix $\mathbf{H}$ of a generalized Reed – Solomon code, then we define the Vandermonde metric associated with that code and proposed in [6].

In this paper, we consider as $\mathbf{F}$ the $N_1 \times n,\ N_1 \geq n$, transposed parity check matrix of a rank code:

$$\mathbf{F} = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \dots & \dots & \dots & \dots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \end{pmatrix}, \tag{2.1}$$

where each entry of the matrix is in $GF(q^N)$ and elements $h_1, h_2, \dots, h_{N_1}$ are linearly independent over the base field $GF(q)$.

It is clear that $\text{rank}(\mathbf{F}) = n$ (see, [8]). Thus this matrix defines a new metric which is the metric associated with rank codes. We refer to this metric as ARC-metric.

Note that vectors of weight 1 in ARC-metric are multiples of rows of the matrix A. On the other hand, they have the maximal weight n in the Hamming metric.

2.2 Code construction

Let $N = N_1 + k$. Consider a concatenation of matrices $\mathbf{F}$ and $\mathbf{G_k}$:

$$\mathbf{Q} = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \\ g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} \mathbf{F} \\ \mathbf{G_k} \end{pmatrix}, \tag{2.2}$$

where $h_1, h, \dots, h_{N_1}, g_1, g, \dots, g_k$ are linearly independent over the base field $GF(q)$. We have also $k < n < N_1, N_1 + k = N$.

In Eq's. (2.2) the matrix

$$\mathbf{F} = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \end{pmatrix}$$

defines ARC-metric, and the matrix

$$\mathbf{G_k} = \begin{pmatrix} g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix},$$

is used as a generator code matrix. Let

$$\underline{a} = (\ a_1 \quad a_2 \quad \dots \quad a_k\ )$$

be a vector of k information symbols in $GF(q)$. A code vector is calculated as

$$\underline{y} = \underline{a}\mathbf{G_k},$$

or,

$$\underline{y} = \left(\ a_1g_1 + a_2g_2 + \dots + a_kg_k, \quad a_1g_1^q + a_2g_2^q + \dots + a_kg_k^q \quad \dots \quad a_1g_1^{q^{n-1}} + a_2g_2^{q^{n-1}} + \dots + a_kg_k^{q^{n-1}}\ \right). \tag{2.3}$$

Code distance is defined as the minimal $\mathcal{F}$-norm of code vectors $\underline{y}$. Let us determine its value. Assume that a vector $\underline{y}$ in ARC-metric has norm $N_F = m$. Then the vector $\underline{y}$ can be represented as:

$$\underline{y} = \left(\ b_1h_1 + b_2h_2 + \dots + b_mh_m \quad b_1h_1^q + b_2h_2^q + \dots + b_mh_m^q \quad \dots \quad b_1h_1^{q^{n-1}} + b_2h_2^{q^{n-1}} + \dots + b_mh_m^{q^{n-1}}\ \right). \tag{2.4}$$

It follows from Eq's. (2.3) and (2.4) that $s + m$ rows of matrix $\mathbf{Q}$ are *linearly dependent*. Hence $s+m \geq n+1$, or, $N_F(\underline{y}) \geq n-s+1$. Since $k \geq s$, we can write $d_F \geq n-k+1$. Thus we can conclude that $d_F = n - k + 1$, or, a code with the generator matrix $\mathbf{G_k}$ reaches the generalized Singleton bound.

2.3 Decoding

Let

$$\underline{c} = \underline{g} + \underline{e},$$

where $\underline{g} = (\ g_1, \ g_2, \ \dots, \ g_{N_1}\ )$ is a code vector, $\underline{e} = (\ e_1, \ e_2, \ \dots, \ e_{N_1}\ )$ is an error vector. Assume that ARC-norm of the error vector is equal to t. Then

$$\underline{e} = m_1h_1 + m_2h_2 + \ldots + m_{N_1}h_{N_1},$$

and $d_H(\underline{m}) = t$, where $\underline{m} = (m_1, m_2, \ldots, m_{N_1})$. We show that a fast decoding algorithm exists for described codes. Let us consider matrix concatenation:

$$\mathbf{Q} = \begin{pmatrix} \mathbf{F} \\ \mathbf{G_k} \end{pmatrix}$$

where

$$\mathbf{F} = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \end{pmatrix}$$

and

$$\mathbf{G_k} = \begin{pmatrix} g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix}.$$

Let $\mathbf{R}$ be the matrix which consists of last n rows of the matrix $\mathbf{Q}$:

$$\mathbf{R} = \begin{pmatrix} h_{N_1-n+k} & h_{N_1-n+k}^q & \dots & h_{N_1-n+k}^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \\ g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix}.$$

The matrix $\mathbf{R}$ is the nonsingular matrix. Let us consider the matrix $\mathbf{QR^{-1}}$. It can be represented in a block form as follows:

$$\mathbf{QR^{-1}} = \begin{pmatrix} \mathbf{B_1} & \mathbf{B_2} \\ \mathbf{E_{n-k}} & \mathbf{0} \\ \mathbf{0} & \mathbf{E_{n-k}} \end{pmatrix},$$

where $\mathbf{E_l}$ means the identity matrix of order l. Multiply $\underline{c}$ by matrix $\mathbf{R^{-1}}$ to the right:

$$\underline{c}\mathbf{R^{-1}} = (\underline{g} + \underline{e})\mathbf{R^{-1}} = (\underline{g} + \underline{m}\mathbf{F})\mathbf{R^{-1}} = \underline{g}\mathbf{R^{-1}} + \underline{m}\mathbf{F}\mathbf{R^{-1}} = \tilde{\underline{g}} + \tilde{\underline{e}}.$$

Then

$$\widetilde{\underline{e}} \equiv \underline{m}\mathbf{F}\mathbf{R^{-1}} = \begin{pmatrix} m_1 & m_2 & \dots & m_{N_1} \end{pmatrix} \begin{pmatrix} \mathbf{B_1} & \mathbf{B_2} \\ \mathbf{E_{n-k}} & \mathbf{0} \end{pmatrix}. \tag{2.5}$$

Let us consider first $n-k$ columns of the system (2.5):

$$\begin{pmatrix} m_1 & m_2 & \dots & m_{N_1} \end{pmatrix} \begin{pmatrix} \mathbf{B_1} \\ \mathbf{E_{n-k}} \end{pmatrix} = \begin{pmatrix} \widetilde{e}_1 & \widetilde{e}_2 & \dots & \widetilde{e}_{n-k} \end{pmatrix}. \tag{2.6}$$

It can be shown that there is a matrix ψ, such that

$$\begin{pmatrix} \mathbf{B_1} \\ \mathbf{E_{n-k}} \end{pmatrix} \psi = V,$$

where matrix $\mathbf{V}$ looks like

$$\mathbf{V} = \begin{pmatrix} v_1 & v_1^q & \dots & v_1^{q^{n-k-1}} \\ v_2 & v_2^q & \dots & v_2^{q^{n-k-1}} \\ \vdots & \vdots & \dots & \vdots \\ v_{N_1} & v_{N_1}^q & \dots & v_{N_1}^{q^{n-k-1}} \end{pmatrix}.$$

Multiply the left part of(2.6) by ψ, where ψ is some nonsingular square matrix:

$$(\ m_1 \quad m_2 \quad \dots \quad m_{N_1} \ ) \begin{pmatrix} \mathbf{B_1} \\ \mathbf{E_{n-k}} \end{pmatrix} \psi = (\ \widetilde{e}_1 \quad \widetilde{e}_2 \quad \dots \quad \widetilde{e}_{n-k} \ )\psi.$$

Thus, it is necessary to solve the system:

$$\underline{m}\mathbf{H}' = \underline{\widetilde{e}}\psi, \tag{2.7}$$

where the right part of the equation is known as well as the matrix

$$\mathbf{H}' = \begin{pmatrix} \mathbf{B_1} \\ \mathbf{E_{n-k}} \end{pmatrix} \psi.$$

The solution of Eq's. (2.7) is reduced to decoding of a rank code. Then we can find plaintext $\underline{m} = (m_1, m_2, \dots, m_{N_1})$ from Eq's. (2.6). It allows to find the error vector from following equation: $\underline{e} = m_1 h_1 + m_2 h_2 + \dots + m_{N_1} h_{N_1}$.

3 New modification of the Niederreiter cryptosystem

The new cryptosystem is based on a new ARC-metric associated with rank codes. To construct the system we have to do the following.

1. Choose a parity check matrix $\mathbf{F}$ of a rank code. This matrix defines ARC-metric.
2. Choose a generator matrix $\mathbf{G_k}$. A code generated by this matrix is optimal with respect to correcting errors in ARC-metric. A fast decoding algorithm exists for this code.
3. Choose a nonsingular scrambling matrix $\mathbf{S}$ with entries in $GF(q^N)$ and a nonsingular matrix $\mathbf{P}$ with entries in $GF(q)$.

Private key is a set of matrices

$$(\ \mathbf{F} \quad \mathbf{G_k} \quad \mathbf{S} \quad \mathbf{U} \quad \mathbf{P} \ ).$$

Public key is the matrix

$$\mathbf{H_{pub}} = \mathbf{P}(\mathbf{F} + \mathbf{U}\mathbf{G_k})\mathbf{S},$$

where $\mathbf{U}$ is some matrix. Code vectors are rows of the matrix $\mathbf{UG_k}$. Matrix $\mathbf{U}$ is not needed for decryption but it has to be inaccessible for cryptanalyst.

Plaintexts are N_1-dimensional vectors

$$\underline{m} = (\ m_1 \quad m_2 \quad \ldots \quad m_{N_1}\ )$$

such that

$$\mathrm{rank}(\underline{m}) = t_{min} = \min(\ t_k,\ \ t_p\ ),$$

where t_k is the error capacity in ARC-metric of a code with the generator matrix $\mathbf{G_k}$, t_p is the error capacity in rank metric of a code with the parity check matrix $\mathbf{F^T}$.

Encryption:
A ciphertext is calculated as a syndrome:

$$\underline{c} = \underline{m}\mathbf{H_{pub}} = \underline{m}\mathbf{P}(\mathbf{UG_k} + \mathbf{F})\mathbf{S} = \underline{\widetilde{m}}(\mathbf{F} + \mathbf{UG_k})\mathbf{S},$$

$$\underline{c} = (m_1(F_1 + G_{k_1}) + m_2(F_2 + G_{k_2}) + \ldots + m_{N_1}(F_{N_1} + G_{k_{N1}}))\,\mathbf{S} = (\underline{g} + \underline{e})\mathbf{S},$$

where $\underline{\widetilde{m}} = \underline{m}\mathbf{P}$, F_i and G_i are rows of matrices $\mathbf{F}$ and $\mathbf{UG}$ correspondingly.

The sum $(\underline{g} + \underline{e})$ can be described as: the code vector $\underline{g}$ is defined by the matrix $\mathbf{G_k}$ and $\underline{e}$ is the error vector with ARC-norm which equals or less than t.

Decryption:
An authorized user multiplies the obtained ciphertext $(\underline{g} + \underline{e})\mathbf{S}$ by $\mathbf{S^{-1}}$. Then user has to use the fast decoding algorithm in ARC-metric. As a result, the user will obtain vectors $\underline{g}$ and $\underline{e}$. The user applies then the fast decoding algorithm for the parent rank code and obtains a vector $\underline{\widetilde{m}}$. Finally, $\underline{\widetilde{m}}\mathbf{P^{-1}}$ gives the required initial plaintext $\underline{m}$.

References

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

[2] Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory, 1986. - Vol. 15 - P. 19-34.

[3] Sidelnikov V. M., Shestakov S. O. About cryptosystem based on generalized Reed-Solomon codes // Discrete mathematics, 1992. - T.4, No. 3. (in Russian)

[4] Sidelnikov V. M., Shestakov S. O. About cryptosystem seted on generalized Reed-Solomon codes // Perspective communication facilities and integrated communication / Moscow, 1992. - P. 48-61. (in Russian)

[5] Gabidulin E. M., "Public Key Cryptosystems Based on Linear Codes Over Large Alphabets: Efficiency and Weekness," Invited paper, P.Farrell (Ed.), Codes and Ciphers, 1995.

[6] Gabidulin E. M., Obernikhin V. A., Codes in Vandermonds F-metric and its application. *Problems of Information Transmission*. V. 39. No. 2. Pp. 3-14, 2003 .

[7] Gabidulin E.M., Simonis J. Metrics Generated by Families of Subspaces // IEEE Trans. Inform. Theory. 1998. V. 44 5 P. 1336-1341.

[8] F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error Correcting Codes," 8th ed, North Holland Press, Amsterdam, 1993.