As a manuscript

The Thesis Abstract

Marina Samokhina

M.Sc. (applied mathematics and physics)

B.Sc. (applied mathematics and physics)

The field of the dissertation specialty 05.13.17 – «Theoretical computer science and mathematics»

to obtain the degree of candidate of Mathematical and Physical Sciences

Assessed by AEI-NOOSR as Doctoral Degree qualifications *

Moscow 2009
Scientific leader: Ernst Mukhamedovich Gabidulin, D.Sc., Phd, Professor

Official opponents:
- Evgeny Avramovich Kruk, D.Sc, Phd, Professor, Saint Petersburg State University of Aerospace Instrumentation
- Kabatyansky Gregory Anatolevich, Phd, Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)

Lead organization: Sobolev Institute of Mathematics SB RAS

The dissertation would be presented at Moscow Institute of Physics and Technology Scientific Council «Д 212.156.04» on 24th March 2009, at 5 pm, the address: 1Institutskiy per., 9, Dolgoprudnyy, Moskovskaya oblast', Russia, 141701, New building, room 204

The thesis is available in the library of Moscow Institute of Physics and Technology

The thesis abstract has been shared in February 2009.

Scientific Secretary
of the Scientific Council «Д 212.156.04»

Kuklev L.P., Phd
GENERAL DESCRIPTION OF THE PHD THESIS

Current Importance of the Topic. For many years, researchers have used linear codes for creation of public key cryptosystems, starting from first publications by McEliece (1978) and Niederreiter (1986).

The classic system designed by Niederreiter is characterised by high algorithm performance. Six years after the description of the classic encryption system was published, cryptographers V.M. Sidelnikov and S.O. Shestakov came forward with a successful attack on the Niederreiter system. This was followed by several different modifications to the classic Niederreiter cryptosystem to increase its cryptographic strength.

The Thesis proposes a new cryptosystem which is designed based on the Niederreiter principle. One of the features of the new cryptosystem is introduction of an additional error in the new metric. This allows to make the structure of the public key more complex thus rendering any Sidelnikov-Shestakov-like attacks ineffective.

Systems which ensure the unauthorised access prevention are often used in noisy channels. The suggested new cryptosystem can be used in channels with various types of noises, and in addition to preventing unauthorised access it can correct channel errors. Use of two separate systems for error correction and for unauthorised access prevention involves a number of complex computational tasks to coordinate the operation of these systems.

The described new integrated system of error correction and cryptosecurity can be successfully applied in transmission of moving
images. This application is useful for videoconferences, video surveillance and video monitoring systems.

**Thesis goal** is to design and explore Niederreiter system-based cryptosystems using new metrics and new codes with an intended application as part of integrated systems of error correction and unauthorised access prevention.

**Thesis Objectives:**

1. Examination and cryptanalysis of existing Niederreiter system modifications.
4. Computer simulation of a new cryptosystem as part of an experimental integrated system of error correction and unauthorised access prevention.
5. Computer simulation and exploration of a new cryptosystem as part of a system of moving images transmission, error correction, and unauthorised access prevention.

**Research Approaches.** In order to achieve the set goal, the Thesis uses methods of information theory, discrete mathematics, computer simulation, linear algebra and algebraic coding theory.

**Main Propositions for Defence:**

1. Description and exploration of a new metric, building codes in this metric.
2. Encryption and decryption algorithms of the new Niederreiter system-based cryptosystem.
3. Cryptanalysis of the new cryptosystem. Selection of the cryptosystem parameters.
4. Integrated system of multiple error correction and unauthorised access prevention.

**Scientific Novelty:**
1. A class of projective metrics was introduced. This allowed to upgrade linear code-based cryptosystems.
2. A new metric was chosen to be used in the design of a public-key cryptosystem and to increase the cryptographic strength of the system.
3. A public-key cryptosystem was designed. It used a new metric associated with Frobenius matrix and rank codes.
4. An algorithm was developed which allowed to use the new cryptosystem features for error correction.
5. Characteristics of an integrated system of error correction and cryptosecurity were defined as applicable to video transmission.

**Practical Value and Implementation of Results**

The Thesis results were obtained as part of the following research papers:
- Contract No. 32/07 dated 18 May 2007 with A. Kharkevich Institute of Information Transmission Problems executed in
pursuance of State Research Contract No. 02.514.11.4025 dated 1 May 2007 between Federal Agency for Science and Innovations and A. Kharkevich Institute of Information Transmission Problems. Thesis results are used for education purposes at the Radio Engineering Department of Moscow Institute for Physics and Technology as part of the Information Security course.

**Approval of the Thesis Results**

Main results of the Thesis were presented and discussed at the following conferences and seminars.


**Publications**

There were 11 publications on the Thesis topic; two of them were published in reviewed journals, approved by the Higher Assessment
Committee. The list of publications is given in the end of the Thesis Abstract.

**Structure and Volume of the Thesis**

The Thesis is composed of introduction, six chapters, conclusion, list of references containing 45 items, and annex. It is presented on 146 pages, contains 15 figures and 5 tables.

**THESIS CONTENTS**

**Introduction** sets out the objective, justifies the importance of the research, scientific novelty and practical value of the results, gives a summary of the Thesis structure.

**Chapter I** describes basic concepts of cryptography and essentials of the coding theory. It reviews symmetric and asymmetric cryptosystems, describes main approaches to a system cryptanalysis, and provides a definition of the cryptographic strength of a system. It examines Reed-Solomon codes and rank codes. It mainly focuses on algebraic methods of encoding and decoding of rank codes.

It details the encoding and decoding of Reed-Solomon codes, provides definition of a rank code. It takes notice of maximum rank distance codes. It describes algorithms of encoding and decoding of rank codes. As an example, it examines various errors and their correction using rank codes.

**Chapter II** describes classic linear code-based cryptosystems. It examines the general design principles of these types of cryptosystems. It describes McEliece and Niederreiter cryptosystems.
In the McEliece public-key system, the main idea of a cryptosystem design is to create a code and disguise it as common linear code. The McEliece algorithm is rather fast and operates tenfold times faster than a standard RSA system, but has a significant disadvantage—the public key is large. Due to the large public key the cipher text is twice as long as public key. This means that a larger message must be transmitted and the system application becomes more complicated.

The Niederreiter system has no disadvantages of McEliece system as described above, and is also based on generalised Reed-Solomon codes. Secret codes in the Niederreiter system are:

- parity check matrix \[ H = \begin{bmatrix} z_j x_j^i \end{bmatrix} \] \[ H = \begin{bmatrix} z_j x_j^i \end{bmatrix} \], where \( j = 1, \ldots, n \) \( j = 1, 2, \ldots, n \), \( i = 0, \ldots, r - 1 \) \( i = 0, 1, 2, \ldots, r - 1 \) of generalised Reed-Solomon code over field \( GF(q) \) \( GF(q) \);

- random non-singular scrambling matrix \( S \) \( S \) of rank \( r \) \( r \) over \( GF(q) \) \( GF(q) \). This matrix is introduced in order to conceal visible patterns from a cryptanalyst by corrupting the structure of the check matrix.

Scrambled check matrix \( H_{cr} = SH \) \( H_{cr} = SH \) is a public key.

Messages are all vectors with coordinates from field \( GF(q) \) \( GF(q) \) the weight of which is no greater than \( r/2 \).
Messages are not codewords of the chosen Reed-Solomon code, but represent all kinds of errors which this code can correct.

Cipher text which corresponds to message $m$ is a syndrome vector and is calculated as follows:

$$c = m H_{cr}^T = m H^T S^T$$

Upon receiving cipher text $c$, an authorised user multiplies it from the right side by matrix $(S^T)^{-1} (ST)^{-1}$, then applies a fast decoding algorithm, known to this user only, this returns the transmitted message $m$.

The Chapter details cryptanalysis algorithms for linear code-based cryptosystems. The Niederreiter cryptosystem proved vulnerable and was hacked by Sidelnikov and Shestakov. The cryptanalysts managed to find such matrices $\tilde{S}$ and $\tilde{H}$, that $H_{cr} = \tilde{S} \tilde{H}$, where $\tilde{H}$ had the same structure as $H$ though possibly with different parameters.

Later, the system would be modified to be able to withstand the Sidelnikov-Shestakov attack. By comparing McEliece and Niederreiter cryptosystems, it can be decided in which cases each of these algorithms would be more useful. The Chapter states main problems which arise in cryptosystem application.

**Chapter III** deals with projective metrics and examples of creating the codes in various projective metrics.
The first paragraph provides definition of norm and distance in a projective metric. The Chapter examines the examples of projective metrics, paying special attention to the metric associated with Frobenius-type matrix.

It provides definition of an optimum code in the projective metric, and of the parent code. Through the examples of projective metrics it examines the examples of codes in metrics which are based on Vandermonde and Frobenius matrix. It details the fast decoding algorithm for the metric associated with Frobenius matrix.

Chapter IV details main approaches to the modification of the Niederreiter cryptosystem.

In recent years, the main idea of modification was to conceal the structure of the syndrome in the best possible way. This is done in order to prevent structural attacks, similar to Sidelnikov-Shestakov attacks. The structure of the private key becomes so complex that the syndrome of the parent code acts as an artificially created error of the new code in the new metric. Table 1 presents possible modifications to the Niederreiter system.

### Possible Modifications to the Niederreiter Cryptosystem

<table>
<thead>
<tr>
<th>No.</th>
<th>Code</th>
<th>Metric</th>
<th>Type of Cipher Text</th>
<th>Cryptosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Codes with maximum rank distance</td>
<td>Rank metric</td>
<td>$m H^T_{pub} = m(SH)^T$</td>
<td>Described by T. Berger and P. Loidreau in 2004</td>
</tr>
<tr>
<td></td>
<td>Generalised Reed-Solomon codes</td>
<td>Based on Vandermonde matrix</td>
<td>$H_{pub} \overline{m} = S(F + G^T U) P \overline{m}$</td>
<td>Designed by E. Gabidullin and V. Obernikhin in 2002</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Modified rank code</td>
<td>Based on Frobenius matrix</td>
<td>$H_{pub} \overline{m} = S(F + G^T U) P \overline{m}$</td>
<td>Designed by E. Gabidullin and M. Samokhina in 2005</td>
</tr>
</tbody>
</table>

The first row of Table 1 shows Berger-Loidreau modification which uses codes with maximum rank distance. Apparently, a Sidelnikov-Shestakov attack can be possible for such a system, though no results of this sort have been reported.

Examples in the second and third rows of Table 1 use a new idea: cipher text can be presented as a sum of vectors $g + e$, 

\[
(g + e)\]

multiplied by a randomly selected matrix $S$.

In order to decrypt, a legitimate user must first find the error vector by applying the fast decoding algorithm to a new code, which is a syndrome of the parent code. The second stage of decryption is to apply the fast decoding algorithm to the parent code. Having applied the fast decoding algorithm to the parent code, a legitimate user obtains the public text.

The design of a cryptosystem corresponding to the second row of Table 1, with a metric based on the Vandermonde matrix, begins with choosing matrix $F$ with elements from an extended field $GF(q^N)$. Matrix $F$ is a parity check matrix for the parent code. This code must be designed in such a way that it has a fast decoding
algorithm in the parent metric. Next step is to choose the generator matrix $G$ of some linear code, which must have a fast decoding algorithm in the new metric.

Before encryption, a secret key must be chosen, consisting of a set of matrices $\{F, G^T, S, P\}$ and matrix $U$. Then the public key is calculated:

$$H_{pub} = \mathcal{S}(F + G^T U) P$$  $$H_{pub} = \mathcal{S}(\mathcal{G} T U) P$$

During encryption, the public text $m$ is multiplied by public-key matrix: $c = H_{pub} m$, $c = m H_{pub}^T$. Upon receiving the cipher text, a legitimate user multiplies $c$ by matrix $(S^T)^{-1} c S^{-1}$. This results in a vector which can be represented as a sum:

$$(g + e) (g + e)$$

Then a fast decoding algorithm is applied in the Vandermonde metric. As a result, it straight away returns vector $\tilde{m}$. In order to obtain the public text, $m = \tilde{m} (P^T)^{-1} \tilde{m} P^{-1}$ must be calculated.

The modification given in the third row of Table 1 is the main result of the Thesis and is described in Chapter V. Besides, the Thesis analyses earlier linear code-based cryptosystems and explores possible cryptoattacks on such systems. The performed analysis leads to a
conclusion that earlier modifications to the Niederreiter cryptosystem use rank 1 matrices for noise, thus making such systems potentially vulnerable.

In Chapter V a new cryptosystem is designed based on the metric associated with Frobenius matrix.

The following Frobenius matrix is used as matrix $F$ of size $N_1 \times n \times n$ with elements from field $GF(q^N)$:

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

where each matrix element is selected from field $GF(q^N)$.

Elements $h_1, h_2, \ldots, h_{N_1}$ are linearly independent over the base field. Then, matrix $G_k$ is used for creating the code. It is of the same form as matrix $F$:

$$
G_k = \begin{pmatrix}
    g_1 & g_1^q & \ldots & g_1^{q^{n-1}} \\
    g_2 & g_2^q & \ldots & g_2^{q^{n-1}} \\
    \vdots & \vdots & \ddots & \vdots \\
    g_K & g_K^q & \ldots & g_K^{q^{n-1}}
\end{pmatrix}.
$$
Then, concatenated matrices $F$ and $G_k$ are used:

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

where $N = N_1 + K$, $h_i, g_j$ are elements of field $GF(q^N)$, collectively linearly independent over the base field. The upper part of matrix $Q$ with elements $h_j^{q^i}$ is used to define the metric; and the lower part with elements $g_j^{q^i}$ is used as a code generator matrix.

The public key is $H_{pub} = S(F + G^T U)P$. During encryption, the public text $m$ is multiplied by public-key matrix: $c = H_{pub} m$. 

During decryption, a legitimate user multiplies the obtained cipher text $(g + e)S^T$ by $(S^T)^{-1}$. Then the fast decoding algorithm is applied in the new metric. As a result, the user will obtain vectors $g$ and $e$. After applying the fast decoding algorithm of the parent code, a legitimate user will obtain vector $\tilde{m}$. Further multiplication of vector $\tilde{m}$ by matrix $(P^T)^{-1}$ will give the legitimate user the public text $m$. 

14
The Chapter then proceeds with describing an attack on the presented new cryptosystem. There are two main types of attacks applicable to the described cryptosystem: direct attacks and structural attacks. Structural attacks are various modifications of the Gibson attack, adapted to the modifications of the cryptosystem, and variants of the Sidelnikov-Shestakov attack. When assessing the complexity of each attack, it is important to consider the size of the public key.

The cryptanalysis showed, that for the most successful structural attack algorithm, the computational complexity is of the $2^{140}$ order for a public key of 1024 bytes. As of today, this computational complexity is more than sufficient to consider the cryptosystem to be secure. Thus, it can be concluded that a new cryptographically strong system has been designed.

**Chapter VI** focuses on the application of a cryptosystem which is based on the metric associated with Frobenius matrix in systems of transmission and unauthorised access prevention. It describes a system of simultaneous error correction and unauthorised access prevention. The Chapter explores the operation of the new cryptosystem within the information security system during video transfer.

For error correction, additional restrictions must be placed on selecting the matrices in the initialisation module. It is necessary to collect statistical data, pre-analyse it to determine the types of errors and modify the cryptosystem to correct these errors. In the base field,
the cipher text is represented by a matrix with elements from field $GF(q)$:

$$C = \begin{pmatrix}
  c_{11} & \cdots & c_{1n} \\
  \vdots & \ddots & \vdots \\
  c_{N1} & \cdots & c_{Nn}
\end{pmatrix}.$$ 

Elements of matrix $C$ are as follows:

$$c_{ij} = s_{ij}u_{ij} + g_{1}u_{ij} + \cdots + h_{i}u_{ij} + s_{jj}u_{jj} + g_{1}q_{j} - 1 u_{jj} + \cdots + h_{j}q_{j} - 1 u_{jj}.$$ 

At the decryption stage, a corrupted text is input to the receiver in the form of $(g + \varepsilon + \tilde{\varepsilon})$. To ensure the error correction, additional restrictions must be placed on selecting the matrix $Q$. Code with generator matrix $G_k$ must correct even more errors. Additional restrictions increase the size of the cryptosystem keys. This slightly affects the speed of encryption and decryption. In Table 2, $\varepsilon$ represents the number of vectors of rank 1 over the base field; $\eta$ is the number of vectors of rank 2; $\xi$ is the number of vectors in the metric defining matrix.

In error representation $\tilde{\varepsilon} = \sum_{i} \zeta f_{i}$, let the minimum number of non-zero coefficients $\zeta$ equal $\tau$. Then in order to ensure the error correction during decoding, the following
must be true: \( t = \frac{d - 2\tau - 1}{2} \), where \( t \) is norm \( e \) \( \ell \).

Table 2

<table>
<thead>
<tr>
<th>Rank ( \tilde{\ell} / \tilde{e} )</th>
<th>Norm ( \tilde{\ell} / \tilde{e} )</th>
<th>Number of Matrices</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>( \xi \times \varepsilon )</td>
<td>Rank over the base field of one of the vectors equals 1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>( \xi \times (\xi - 1) \times q^2 \times \varepsilon )</td>
<td>Rank of linear combination of any pare of vectors equals 1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>( \xi \times \eta )</td>
<td>Rank over the field of one of the vectors equals 2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>( \xi \times (\xi - 1) \times q^2 \times \eta )</td>
<td>Rank of linear combination of any pare of vectors equals 2</td>
</tr>
</tbody>
</table>

The new modification to the Niederreiter cryptosystem was used during the work under Contract No. 32/07 dated 18 May 2007 for Development and Analysis of Signal-Code Structures for Transmission and Security of Moving Images. The work showed that the cryptosystem could be successfully applied as part of the public-key system for transmission and protection of moving images. Figure 1 shows the relation between the algorithm performance and the cryptosystem key size for a modified Niederreiter system which is based on Frobenius matrix and for an RSA cryptosystem for a noiseless channel. The algorithm performance in the new
cryptosystem proved to be higher than performance of an RSA cryptosystem.

**Figure 1. Relation between the Algorithm Performance and the Cryptosystem Key Size**

In the diagram in Figure 1, red line represents values of the supported frame rate for an RSA cryptosystem with 512 bit key in a noiseless channel. The supported rate for RSA is twice as low as the same value for the newly developed cryptosystem. This comparison is not truly accurate for a noisy channel, as the use of RSA in a noisy channel requires to encode with a bit error probability of no more than $10^{-8}$. Encoding with such bit error probability is not practically possible. As a result, in addition to the performance superiority, the new cryptosystem does not require additional efforts in software development or in increasing the hardware computational capacity.
One of the main characteristics of a cryptosystem is its cryptographic strength. The cryptosystem strength is characterised by the number of simple bit operations required for the most effective cryptoattack on the system.

The new cryptosystem can support various frame rates; the supported rate depends on the system parameters. The strength of this cryptosystem also depends on the choice of parameters. Figure 2 shows the relation between the new cryptosystem strength and the supported frame rate in a noiseless channel with a frame rate as in a SonyEricsson W900 mobile phone. With the use of today’s compression methods, the frame size is 12 kilobits.

The diagram in Figure 2 shows that for a standard frequency of 25 frames per second, the cryptosystem security is so strong, that any losses in strength for error correction are insignificant.

The research provided results for two different values of frame size and frame rate, compliant with requirements. Figure 3 shows the relation between the supported frame rate and the key size at different frame sizes when the newly developed cryptosystem is used. The ordinate axis represents the maximum possible supported frame rate in frames per second, and the abscissa axis represents the corresponding key size in bits.

In case of High-Definition Television (HDTV) video transmission, the frame rate supported by the system drops 20 times as low.
The most frequently used format of today is Standard Definition (SD) with the frame rate of 25 frames per second. The diagram in Figure 3 shows that such supported rate corresponds to the key size of 384 bits.

The system performance can be boosted by encrypting the images with more efficient symmetric algorithms, and the session key can then be encrypted with the new system. This modification can only be applied in a noiseless channel. For example, for symmetric algorithm, either AES or Russian GOST28147-89 can be used. If the transmitted message is encrypted with one of the symmetric algorithms, and the session key is encrypted with the newly developed cryptosystem, HDTV video transmission can be guaranteed.
Figure 2. Relation between the Cryptographic Strength and the Supported Frame Rate
Figure 3. Relation between the Frame Rate and the Key Size

Figure 4 shows the relation between the supported frame rate and the frame size for symmetric algorithm AES256 and for the new modification to the Niederreiter cryptosystem. The size of the session key is 256 bits, and the public key of the system is 512 bits.

The light-green line in the diagram represents the standard AES implementation without acceleration, and the dark-green line corresponds to a theoretically maximum performance of AES implementation. Diagram in Figure 4 shows that with the standard non-accelerated AES implementation, the supported frame rate
increases tenfold as compared to implementation with no symmetric algorithm.

Figure 4. Relation between the Frame Rate and the Frame Size

MAIN RESULTS AND CONCLUSIONS

1. A new cryptosystem was designed, which uses the Niederreiter principle and a new metric associated with Frobenius matrix. The new cryptosystem ensures high algorithm performance at high cryptographic strength.
2. Computer simulation of the new cryptosystem showed that it could be successfully applied for simultaneous error correction coding and unauthorised access prevention.

3. A set of mathematical methods was developed based on the presented algorithms. These methods ensure successful error correction while encrypting and decrypting the transmitted data.

4. The presented algorithms were tested and approved for use in a system of secure video transmission. Computer simulation of the system proved its high performance and reliability.

LIST OF RELEVANT ARTICLES CAN BE SHARED ON A REQUEST