INFORMATION AND CONTROLLING SYSTEMS

CONSTRUCTION OF
HYBRID SECURITY
SYSTEMS BASED
ON THE CRYPTO-
CODE STRUCTURES
AND FLAWED
CODES

S. Yevseiev
PhD, Associate Professor*
E-mail: serhii.yevseiev@m.hneu.edu.ua

O. Korol
PhD, Associate Professor*
E-mail: olha.korol@m.hneu.edu.ua

H. Kots
PhD, Associate Professor*
E-mail: dekanstei@gmail.com

*Department of Information Systems
Simon Kuznets Kharkiv National University
of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

UDC 621.391
DOI: 10.15587/1729-4061.2017.108461

1. Introduction

The evolutionary development of the global Internet computer network based on open protocols and interconnection models of open systems, rapid development of informational, communication, computer, collaborative technologies have led to the creation of new patterns in the functioning of educational organizations in the world, transition to control systems with a critical cybernetic infrastructure (SCCI) [1–8]. Further informatization of corporate educational systems (CES), development of remote access to information assets based on the intensive development of information and computing networks (ICS) of educational institutions creates on their basis the informational educational systems (IES). The negative aspect, however, is the reduction in the level of literacy of users, significant growth of cybercrimes in recent months, using social networks in IES, modernization of the old, and the emergence of new, cyberattacks leads to the aggravation of problems that are related to data protection and security of information assets of SCCI [9, 10]. In this regard, one of the most relevant tasks facing developers and users of IES is the full-scale solution to the problem of information security – from envisaging the strategy, policy and standards of information security in IES all the way to developing specific technologies, as well as procedures to ensure information security [1]. For this purpose, authors of the present work propose a completely new approach to the formation of hybrid (integrated) cryptosystems, allowing us to build multichannel cryptosystems based on crypto-code structures with flawed codes (CCSFC) that ensure the required indicators of safety, reliability, and efficiency. The key feature of constructing the proposed structures is the use of crypto-code systems (CCS), which provide integrated security (they make it possible to build asymmetric cryptosystems of provable stability), and reliability (they employ noise-resistant codes on elliptic curves). Performance efficiency (rate of transformations in CCS is comparable to the crypto-transformations of block symmetric ciphers) of the transmitted information, and the use of flawed codes make it possible to reduce the power of the CCS alphabet, without compromising crypto stability that expands the scope of their use in many applied applications.

2. Literature review and problem statement

Development of computing equipment and communication technologies make it possible to create elements of IES based on the services provided by the global Internet technologies, further development of remote access technologies, and the informatization of educational processes and services. This has led to the fact that more and more components and technologies of CES, its software applications and
tools, e-courses and educational modules, data in the distributed databases become available to more users who are geographically dispersed. This creates considerable advantages and benefits in their work and makes it possible to consider IES as a system with critical cybernetic infrastructure objects [10, 11]. In article [7], authors address issues on providing an access to information assets of CES through a remote connection, which is one of the most promising directions in the development of information systems. In addition to the benefits attained from the mobilization of IES users, the problematic areas are also evident – first of all, this relates to the security of data that are available at remote access. An integral part of CES (IES) of educational institutions is social networks whose portals contain personal data from millions of users, thereby representing huge online directories that are available to everyone at will [5]. Modern university stores and processes a huge amount of various data related not only to supporting the educational process, but also to scientific research as well as design and engineering, personal data on students and staff, service, commercial and other confidential information [6]. The conceptual strategy, however, policies and procedures that would ensure safety of information assets, utilized and stored in IES, are lacking at the legislative level. In paper [1], authors systematized the concepts of policies, standards, technologies, and procedures of information security (IS) of CES, as well as proposed methods for ensuring IS based on the construction of virtual private networks – VPN-networks. In [4], authors dealt with the concept of integrated protection of network resources of IES based on a three-level process-service model of IS control system. In article [9], authors propose a synergistic approach to the model of safety assessment of IES and proposed a procedure for the construction of a modified system for electronic document management at a university on the basis of electronic digital signature in line with the X.509 standard. An analysis of protection tools, performed in [4], revealed that modern information-computing networks (ICN) are still dominated by the traditions of using standard hardware and software tools to protect information, which practically exhausted their potential in terms of the neutralization of possible informational threats.

Under such circumstances, one of the promising directions to provide security of the information flows (SFI), utilized in IES, might prove to be creation of a system of integrated protection of network resources based on the asymmetric crypto-code systems (ACCs). Their application makes it possible to ensure with one integrated mechanism the required levels of reliability indicators, security and efficiency in the processing and transmission of confidential information using open channels of the Global Internet (GIN).

Contemporary developers of communication technologies have to simultaneously resolve multiple tasks and to provide not only the safety of the information transmitted, but also the efficiency of transferring large amounts of data. In article [12], authors propose employing the McEliece cryptosystem in the Sequitur software, which makes it possible to integrally solve the tasks on performance efficiency and security when transmitting confidential information. In paper [13], authors use the McEliece cryptosystem as a mechanism to ensure integrity in the stegasystems, which enables storing in a MPEG Layer III or an MP3 file performer’s information, a song lyric, and its performance. The cryptosystem is applied to store both personal (private) and open key in the tag format ID3v2. In papers [14, 15], authors propose using the McEliece cryptosystem for solving the tasks on authentication and the formation of a digital signature based on algebraic coding theory, as well as for transmitting confidential (medical) information. Authors of article [16] propose employing the McEliece cryptosystem in the software Secure Key Management (SKM, a framework with a high degree of scalability relative to memory) to generate the key sequences and their allocation.

In paper [17], authors examined basic principles and a formal notation of the mathematical model for a modified asymmetric crypto-code system based on the McEliece theoretical-code scheme (TCS) on the modified (cropped) elliptic codes that make it possible to provide integrated reliability indicators required for information secrecy and efficiency when transmitting data in communication systems.

In article [18], new approaches are considered to breaking the McEliece cryptosystem based on randomized concatenated codes. Development of hybrid cryptosystems based on the modified asymmetric crypto-code constructions of McEliece on flawed codes is a promising direction in solving the given scientific and technical task.

3. The aim and objectives of the study

The goal of present work is to develop a hierarchical structure of the control systems with a critical cybernetic infrastructure, to analyze principles of the construction of crypto-code structures, systems of multichannel cryptography on flawed codes, to design hybrid cryptosystems based on the modified asymmetric crypto-code constructions by McEliece on flawed codes, to devise a procedure for the estimation of stability of the proposed hybrid cryptosystems based on an entropy method.

To accomplish the goal, the following tasks should be considered:

- to perform an analysis of control systems with a critical cybernetic infrastructure and to develop a hierarchical structure of the critical infrastructure of a state metasystem on example of Ukraine;
- to analyze the principles of formation of the McEliece modified asymmetric crypto-code systems (MACCS) on algebraic geometric codes, as well as multichannel systems on flawed codes, the principles of their construction;
- to design a hybrid cryptosystem based on the McEliece MACCS on flawed codes (HCCSFC) and basic algorithms for the crypto-transformations in HCCSFC;
- to analyze the cost of software implementation of the hybrid cryptosystem on the crypto-code construction with flawed codes;
- to devise a procedure for the estimation of stability of the proposed cryptosystem based on an entropy method.

4. Analysis of systems with a critical cybernetic structure

An analysis of the main provisions of the systems with a critical cybernetic structure, conducted in articles [10, 11], allows us to use the basic concepts, proposed by the authors, related to the formation of a hierarchical structure of the critical infrastructure of a state metasystem:

Critical infrastructure (CI) of the system, network, and/or individual objects, the purposeful or incidental failure of which may potentially lead to irreparable consequences for
the sustainable development of economy and political processes in the state, social well-being, and health of the population.

*System with a critical cybernetic infrastructure (SCCI)* is a set of interrelated elements combined into a whole, correct functioning and interaction of which significantly affects the cybernetic safety of the state over a specific time interval.

*Object with a critical cybernetic infrastructure (OCCI)* is an element of SCCI, the cybernetic influence on which leads to a decrease in the level of its cybernetic protection against cyber threats.

On the basis of the attributive approach proposed in paper [11], we propose a hierarchical approach to the critical infrastructure of a state metasystem on example of Ukraine is shown in Fig. 1. A distinctive feature of the proposed approach is the inclusion in OCCI of the elements of e-education system (IES, CES). Such an approach allows timely development of mechanisms to ensure security of the information utilized by IES (CES). As well as provide the required level of service quality to the users of IES (CES) in the course of further informatization of the system's elements.

**Fig. 1. Hierarchical structure of critical infrastructure of the state metasystem**
In this case, a metasystem of the critical infrastructure of a state (MCIS) refers to a system of strategic scale, representing a large number of diverse elements, combined within a framework of a unified critical cybernetic architecture into a united system. MCIS possesses synergy and has a common emergent property (purpose, function), different from the properties of individual elements of the entire totality [11].

Thus, based on the conducted analysis [1–4, 11] and the proposed hierarchical critical infrastructure metasystem on example of Ukraine, further development of the services and functions of IES (CES) on the basis of informatization of education services and further implementation of the functions of remote access, it is suggested that IES be considered a system with the SCCI objects.

5. Basic principles for building the crypto-code constructions

We shall examine a general structure of the crypto-code systems. We shall define a finite field \( \mathbb{GF}(q) \), vector space \( \mathbb{GP}(q) \) as a set of \( n \)-sequences of elements from \( \mathbb{GF}(q) \) with a component by component addition and multiplication by a scalar. Linear \((n, \ h, \ d)\) code \( C \) is the subspace in \( \mathbb{GP}(q) \), that is, a non-empty set of \( n \)-sequences (codewords) over \( \mathbb{GF}(q) \), \( k \) is the dimensionality of linear subspaces, \( d \) is the minimal code distance (minimal weight of a non-zero codeword).

The main objective of encoding an information is to control (detect and correct) the errors that appeared when sending a message along a channel with noise. In order to control the errors, an encoder contributes redundancy (verification part and matching it against the transmitted part of length \( r = n - k \)) to the transmitted data.

On the receiving side, by examining the properties of the verification part and matching it against the transmitted data, the decoder reduces the impact of errors that occur during transmission [17–21, 24–28].

The problem of decoding can be efficiently solved (with a polynomial complexity) to a narrow class of codes, for example, noise-resistant codes of Bose-Chowdhury-Hocquengham (BCH) and the Reed-Solomon codes. One of the most efficient algorithms for algebraic decoding of the BCH codes is the Berlekamp-Massey algorithm and its modifications (improvements). The Berlekamp-Massey algorithm contains the number of implementation of multiplications of the order of \( t^2 \) or, formally, the complexity of algorithm \( O(t^2) \), \( t \) the correcting ability of the code, \( t = \lfloor(d-1)/2 \rfloor \). For a large \( t \), there is the accelerated Berlekamp-Massey algorithm used, which makes it possible to reduce computational complexity of the algorithm. Even more effective, in terms of computational complexity, is the recurrent Berlekamp-Massey algorithm [24–28].

Decoding an arbitrary linear code (code of general position) is a very complicated computational task with the difficulty of solving it growing exponentially. Thus, for the correlation decoding of an arbitrary \((n, k, d)\) code over \( \mathbb{GF}(q) \), it is required, in a general case, to compare the accepted sequence with all \( q^k \) codewords and to choose the nearest (in the Hamming metric). Even for small \( n, k, d, \) and \( q \), a problem of correlation decoding is rather labor-consuming. This position underlies all cryptosystems on the algebraic block codes. Masking a code with a fast decoding algorithm (polynomial complexity) for an arbitrary (random) linear code, it is possible to represent a problem of decoding for an outsider observer (possible attacker) as a computationally complex task (of exponential complexity). For the authorized user of the cryptosystem (the one possessing the secret key), decoding is the polynomially solvable task. However, in article [29], authors report algorithms for hacking the McEliece and Niederreiter ACCS by finding elements of the generating (check) matrix.

General classification of the crypto-code systems (ACCS) and the security services, provided by them, is shown in Fig. 2.

---

**Fig. 2. General classification of the crypto-code systems**

**CRYPTO-CODE SYSTEMS**

**SYMmetric**

\( I \times A \)

- implementation complexity \( 2^h \)
- BSE drawbacks

- Rao-Nam scheme on Goppa codes 1986–199 y.
- Schemes assigned in terms of Goppa polynomial, Goppa codes 1989 – 95 y.
- Scheme on the Goppa truncated codes 1995 – 98 y.
- linearity of code transformations

**Advantages:**
- high speed of encryption (comparable to BSE) integrated mechanism to ensure A + C model of provable stability

**ASSYmmetric**

\( I + C + A \)

- implementation complexity \( 2^h \)
- prone to the Sidelnikov attack

- The Niederreiter scheme on BCH, Goppa codes 1986 y.
- The McEliece scheme on Goppa codes 1978 y.
- Schemes on the modified AGC, elliptical curves 2007 y.
One of the promising directions in the development of algebraic theory of codes are the algebraic geometric methods of encoding. Nonbinary algebraic block codes built on the algebraic curves (algebraic geometric codes) possess good asymptotic properties. It is proved that at great length these codes lie above the Varshamov-Gilbert boundary [24–28].

Fix a finite field \( GF(q) \). Let \( X \) be a smooth projective algebraic curve in projective space \( P^n \) over \( GF(q) \), \( g \geq g(X) \) is the genus of the curve, \( X(GF(q)) \) is the set of its points over a finite field, \( N = X(GF(q)) \) is their number. Let \( C \) be the class of divisors on \( X \) degree \( \alpha \geq g - 1 \). Then \( C \) determines mapping \( \varphi: X \to \mathbb{P}^{\alpha-1} \), where \( k2\alpha - g + 1 \). Set \( y_i = \varphi(x_i) \) assigns the code. The number of points in the intersection \( \varphi(X) \) with a hyperplane equals \( \alpha \), that is, \( n - d\alpha \). This construction allows us to build codes with parameters \( k + d2\alpha - g + 1 \), whose length \( n \) is less than or equal to the number of points on the \( X \) curve. At \( 2g < \alpha \), algebraic geometric code has parameters \( (n, \alpha - g + 1, d, d2\alpha - 2g + 2) \). Structural characteristics of the elliptic codes, constructed through representation of the form \( \varphi: EC \to \mathbb{P}^{\alpha-1} \) over \( GF(q) \), \( q \geq n \), \( m = 2, 6 \), are given in Table 1.

### Table 1

<table>
<thead>
<tr>
<th>( degF )</th>
<th>( \alpha )</th>
<th>( (n, k, d) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>9, 3, 6</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>9, 6, 3</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>14, 9, 5</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>14, 12, 2</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>15, 15, 10</td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td>15, 18, 12</td>
</tr>
<tr>
<td>7</td>
<td>21</td>
<td>21, 21, 4</td>
</tr>
<tr>
<td>8</td>
<td>24</td>
<td>24, 24, 20</td>
</tr>
<tr>
<td>9</td>
<td>27</td>
<td>27, 27, 17</td>
</tr>
<tr>
<td>10</td>
<td>30</td>
<td>30, 30, 14</td>
</tr>
<tr>
<td>11</td>
<td>33</td>
<td>33, 33, 11</td>
</tr>
<tr>
<td>12</td>
<td>36</td>
<td>36, 36, 8</td>
</tr>
<tr>
<td>13</td>
<td>39</td>
<td>39, 39, 5</td>
</tr>
<tr>
<td>14</td>
<td>42</td>
<td>42, 42, 2</td>
</tr>
<tr>
<td>15</td>
<td>45</td>
<td>45, 45, 36</td>
</tr>
<tr>
<td>16</td>
<td>48</td>
<td>48, 48, 33</td>
</tr>
<tr>
<td>17</td>
<td>51</td>
<td>51, 51, 30</td>
</tr>
<tr>
<td>18</td>
<td>54</td>
<td>54, 54, 27</td>
</tr>
<tr>
<td>19</td>
<td>57</td>
<td>57, 57, 24</td>
</tr>
<tr>
<td>20</td>
<td>60</td>
<td>60, 60, 2</td>
</tr>
<tr>
<td>21</td>
<td>63</td>
<td>63, 63, 18</td>
</tr>
<tr>
<td>22</td>
<td>66</td>
<td>66, 66, 15</td>
</tr>
<tr>
<td>23</td>
<td>69</td>
<td>69, 69, 12</td>
</tr>
<tr>
<td>24</td>
<td>72</td>
<td>72, 72, 9</td>
</tr>
<tr>
<td>25</td>
<td>75</td>
<td>75, 75, 6</td>
</tr>
<tr>
<td>26</td>
<td>78</td>
<td>78, 78, 3</td>
</tr>
</tbody>
</table>

We shall give the following definition to an algebraic geometric code:

**Definition 1** [17]. Let \( X \) be a smooth projective algebraic curve in projective space \( P^n \), that is, a totality of solutions to the homogeneous unreduced algebraic equation of degree \( degX \) with coefficients from \( GF(q) \). Consider the manifolds corresponding to projective hyperplanes assigned in \( P^n \) by equations \( F = 0 \), where \( F \) are the homogeneous monomials of degree \( degF \). Let \( I(i_1, i_2, ..., i_\alpha) \) be the informational sequence. Algebraic geometric code along the \( X \) curve over \( GF(q) \) is a linear code of length \( n \), whose codewords \( C(c_1, c_2, ..., c_\alpha) \) are assigned by equality

\[
\sum_{j=1}^{\alpha} F_j(P) = c_j,
\]

where \( P(X_i, Y_i, Z_i) \) are the projective points of curve \( X \), that is, \( (X_i, Y_i, Z_i) \) are the solutions to a homogeneous algebraic equation, which assign curve \( X_i = \Gamma_i \). \( F_j(P) \) are the values of generator functions in the points of the curve.

This definition is equivalent to the matrix representation of algebraic geometric code:

\[
G = \left( \begin{array}{cccc}
F_1(P) & F_2(P) & ... & F_{\alpha}(P) \\
F_1(P) & F_2(P) & ... & F_{\alpha}(P) \\
... & ... & ... & ... \\
F_1(P) & F_2(P) & ... & F_{\alpha}(P) \\
\end{array} \right)_{\alpha \times \alpha},
\]

**Definition 2** [17]. An elliptic curve (EC) in the affine space \( \mathbb{A}^{2} \) over field \( GF(q) \) is a smooth curve given by equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,
\]

or in \( P^2 \) given by homogeneous equation

\[
y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,
\]

\( a_i \in GF(q) \), the genus of the curve \( g = 1 \).

**Assertion 1** [17]. Algebraic geometric \((\alpha, k, d)\) code along an elliptic curve (elliptical code) over \( GF(q) \), constructed through representation of the form \( \varphi: EC \to \mathbb{P}^{\alpha-1} \), is bound by characteristics \( k + d2\alpha \), in this case

\[
n \leq 2\sqrt{q} + q + 1, k2\alpha, d2\alpha - \alpha = 3degF.
\]

**Definition 3** [17]. Let \( X \) be a smooth projective algebraic curve in \( P^n \), that is, a totality of the solutions to a homogeneous unreduced algebraic equation of degree \( degX \) with coefficients from \( GF(q) \). \( F \) are the homogeneous monomials of degree \( degF \). Algebraic geometric code along the \( X \) curve over \( GF(q) \) is a linear code, consisting of all words \((c_1, c_2, ..., c_\alpha)\) of length \( n \), for which equality \( d + g - 1 \) of equations holds

\[
\sum_{j=1}^{\alpha} c_jF_j(P) = 0,
\]

where \( c_i \in GF(q) \), \( d2\alpha - 2g + 2, \alpha = degX \).

This definition is equivalent to the matrix representation of algebraic geometric code:

\[
H = \begin{pmatrix} c_1 & c_2 & \cdots & c_\alpha \end{pmatrix}^T = 0,
\]
where \( H \) is the test code matrix of dimension \( r \times n, r = n - k = d + g - 2 \)
\[
H = \begin{pmatrix}
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
\vdots & \vdots & \ddots & \vdots \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast})
\end{pmatrix} = \left[ F_1(P) \right]_{n \times r}.
\]

Definition 4 [20]. Let \( X \) be a smooth projective algebraic curve in \( P^r \), that is, a totality of the solutions of a homogeneous unreduced algebraic equation of degree \( \deg X \) with coefficients from \( GF(q) \). \( F \) are the homogeneous monomials of degree \( \deg F \). Algebraic geometric code along the \( X \) curve over \( GF(q) \) is a linear code, consisting of all words \((c_1, c_2, \ldots, c_n)\) of length \( n \leq N \), for which equality \( d + g - 1 \) of the equations holds
\[
\sum_{i=1}^{n} c_i F_i(P) = 0,
\]
where \( c_i \in GF(q) \), \( d \alpha - 2g + 2, \alpha = \deg X s \deg F \).

This definition is equivalent to a rearrangement of algebraic geometric code:
\[
H (c_1, c_2, \ldots, c_n)^T = 0,
\]
where \( H \) is the test code matrix of dimension \( r \times n, r = n - k = d + g - 2 \)
\[
H = \begin{pmatrix}
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
\vdots & \vdots & \ddots & \vdots \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast})
\end{pmatrix} = \left[ F_1(P) \right]_{n \times r}.
\]

Definition 4 and result of assertion 2 allow us to determine the theoretical-code Niederreiter scheme on the basis of elliptic codes in the following way. Let \( H^{EC} \) be a test matrix of elliptic \((n, k, d)\) code over \( GF(q) \) of the form
\[
H^{EC} = \begin{pmatrix}
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast}) \\
\vdots & \vdots & \ddots & \vdots \\
F_1(P) & F_2(P) & \cdots & F_{r}(P_{\ast})
\end{pmatrix} = \left[ F_1(P) \right]_{n \times r},
\]
and a dimension of \( r \times n, r = n - k = d + g - 2 \).

Let \( X \) be a nondegenerate \( k \times k \)-matrix over \( GF(q) \), \( D \) is the diagonal matrix with elements that are non-zero along the diagonal, \( P \) is the permutation matrix of dimension \( n \times n \). We shall determine the asymmetric McEliece crypto-code system with an elliptical code [22]:

- public key – matrix
  \[
  G^{EC} = X \cdot G^{EC} \cdot P \cdot D,
  \]
- secret (closed) key – matrices \( X, P, \) and \( D \).

Closed information (a codogram) is a vector of length \( n \) and is calculated by rule
\[
c^e = i \cdot G^{EC} + e,
\]
where vector \( c^e = i \cdot G^{EC} \) belongs to elliptical \((n, k, d)\) code with generative matrix \( G^{EC} \), \( i \) is the \( k \)-digit information vector, \( c^e \) is the secret weight error vector \( e \).

In order to assign the asymmetric Niederreiter scheme on elliptic codes, we shall refer to a different definition of the algebraic geometric code.

Definition 4 [20]. Let \( X \) be a smooth projective algebraic curve in \( P^r \), that is, a totality of the solutions of a homogeneous unreduced algebraic equation of degree \( \deg X \) with coefficients from \( GF(q) \). \( F \) are the homogeneous monomials of degree \( \deg F \). Algebraic geometric code along the \( X \) curve over \( GF(q) \) is a linear code, consisting of all words \((c_1, c_2, \ldots, c_n)\) of length \( n \leq N \), for which equality \( d + g - 1 \) of the equations holds
\[
\sum_{i=1}^{n} c_i F_i(P) = 0,
\]
where \( c_i \in GF(q) \), \( d \alpha - 2g + 2, \alpha = \deg X s \deg F \).

This definition is equivalent to a rearrangement of algebraic geometric code:
\[
H (c_1, c_2, \ldots, c_n)^T = 0,
\]
The easiest and most convenient way of modifying a linear block code, not reducing the minimal code distance, is to shorten its length by reducing informational symbols. Let \( I = (i_1, i_2, ..., i_n) \) be the information vector \((n, k, d)\) of a block code. Choose subset \( h \) of informational symbols, \( |h| = x \), \( x \leq \frac{1}{2}k \). Put zeros into information vector \( I \) in the subset \( h \), that is, \( I_j = 0, \forall j \in h \). We shall place informational symbols on the remaining positions in vector \( I \). When encoding an information vector, the symbols of set \( h \) are not involved (they are zero) and can be discarded, while the resulting codeword will be shorter by \( x \) code symbols. To modify (truncate) elliptic codes, we shall use a reduced set of points of the curve.

The following assertion is true.

**Assertion 3.** Let \( EC \) be an elliptic curve over \( GF(q) \), \( g = g(EC) \) is the curve genus, \( EC(GF(q)) \) is the set of its points over a finite field, \( N = EC(GF(q)) \) is their number. Let \( X \) and \( h \) be the disjoint subsets of points, \( X \setminus h = EC(GF(q)) \), \( |h| = x \). Then the truncated elliptical \((n, k, d)\) code over \( GF(q) \), constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \), is bound by characteristics \( k + d2n \); in this case:

\[
\begin{align*}
\alpha & = \sqrt{7} + q + 1 - x, \\
\alpha & = 2\sqrt{q} + q + 1 - x \\
\alpha & = 3 \times \text{deg} F.
\end{align*}
\]

**Assertion 4.** Truncated elliptical \((n, k, d)\) code over \( GF(q) \), constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \), is bound by characteristics \( k + d2n \); in this case:

\[
\alpha = \sqrt{7} + q + 1 - x, \\
\alpha = 2\sqrt{q} + q + 1 - x \\
\alpha = 3 \times \text{deg} F.
\]

Using the result of assertions 3, 4, we shall assign a theoretical-code scheme on the modified elliptical codes, constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \) and \( \phi : X \rightarrow P^{k-1} \). The following assertions are true.

**Assertion 5.** Truncated elliptical \((n, k, d)\) code over \( GF(p^m) \), constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \), determines a modified theoretical-code scheme with the following parameters:

\[
\begin{align*}
I_1 &= x \log \left( 2\sqrt{q} + q + 1 \right), \\
I_2 &= (\alpha - x) m, \\
R &= (\alpha - x) / (2\sqrt{q} + q + 1 - x).
\end{align*}
\]

**Assertion 6.** Truncated elliptical \((n, k, d)\) code over \( GF(p^m) \), constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \), determines a modified theoretical-code scheme with the following parameters:

- Dimensionality of the secret key is given by expression

\[
\begin{align*}
l_1 &= x \log \left( 2\sqrt{q} + q + 1 \right), \\
l_2 &= (\alpha - x) m, \\
l_3 &= (2\sqrt{q} + q + 1 - x) m.
\end{align*}
\]

- Relative transmission rate:

\[
R = \frac{2\sqrt{q} + q + 1 - x}{2\sqrt{q} + q + 1 - x}.
\]

Article [17] gave a formal description of the modified asymmetric crypto-code information protection system based on the use of methods of modification and practical algorithms for the formation of codograms and their decoding in the McEliece MACCS.

To further reduce the cost of software implementation, authors of the paper propose employing flawed codes in the McEliece MACCS.

The second technique for the modification of a linear block code that maintains minimal code distance and increases the amount of transmitted data implies extending its length after the formation of an initialization vector, by reducing the informational symbols. Let \( I = (i_1, i_2, ..., i_n) \) be the informational vector \((n, k, d)\) of a block code. Choose subset \( h \) of informational symbols, \( |h| = x \), \( x \leq \frac{1}{2}k \) and *generate an initialization vector*. Put in informational vector \( I \) in the subset \( h \), zeros, that is, \( I_j = 0, \forall j \in h \). We shall put informational symbols in the remaining positions of vector \( I \). Next, we add informational symbols to the positions of initialization vector. For the modification (extending) of elliptic codes, we shall use a reduced set of points of the curve. The following assertion is true.

**Assertion 7.** Let \( EC \) be an elliptic curve over \( GF(q) \), \( g = g(EC) \) is the curve genus, \( EC(GF(q)) \) is the set of its points over a finite field, \( N = EC(GF(q)) \) is their number. Fix a subset \( h \subseteq GF(q) \), \( |h| = x \). Let the elliptical \((n, k, d)\) code over \( GF(q) \) be assigned, constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \). Then parameters of the elliptic code, extended by \( x \) symbols from \( GF(q) \), constructed through representation of the form \( \phi : (X \setminus h) \rightarrow P^{k-1} \), \( n = 2\sqrt{q} + q + 1 - x + 1 \), will be bound by relations:

\[
\begin{align*}
l_1 &= x \log \left( 2\sqrt{q} + q + 1 \right), \\
l_2 &= (\alpha - x) m, \\
l_3 &= (2\sqrt{q} + q + 1 - x) m.
\end{align*}
\]

**Proof.** If \( x < 1 \), then extending the code by \( x \) is equivalent to the truncation of source code by \( x - 1 \). Substituting these parameters in expression \( n = 2\sqrt{q} + q + 1 - x + x \), we shall obtain the result of corollary 7.

**Corollary 1.** If one knows the shape of elliptical curve (set \( a_1, a_6, \forall a \in GF(q) \)), then subsets \( h \) and \( h_1 \) completely determine the modified elliptical \((n, k, d)\) code over \( GF(q) \), constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \) and \( \phi : (X \setminus h) \rightarrow P^{k-1} \). Set of coefficients \( a_1, a_6, \forall a \in GF(q) \) unambiguously assigns the shape of elliptical curve and, consequently, the set of its points \( EC(GF(q)) \). Employing representation of the form \( \phi : EC \rightarrow P^{k-1} \) and results of assertions 1, 2, we shall construct elliptical \((n, k, d)\) code over \( GF(q) \). If one knows the symbols of extension, then we shall construct extended codes.

According to assertion 7, these are the symbols of set \( h_1 \), which completely determine the modified elliptical \((n, k, d)\) code over \( GF(q) \).

**Assertion 8.** Fix a subset \( h \subseteq GF(q) \), \( |h| = x \). Assume that the elliptical \((n, k, d)\) code over \( GF(q) \) is assigned, constructed through representation of the form \( \phi : X \rightarrow P^{k-1} \). Then parameters of the elliptic code, extended by \( x \) symbols from \( GF(q) \), constructed through representation of the form \( \phi : (X \setminus h) \rightarrow P^{k-1} \), will be bound by relations:

\[
\begin{align*}
l_1 &= x \log \left( 2\sqrt{q} + q + 1 \right), \\
l_2 &= (\alpha - x) m, \\
l_3 &= (2\sqrt{q} + q + 1 - x) m.
\end{align*}
\]

**Proof.** Set of coefficients \( a_1, a_6, \forall a \in GF(q) \) unambiguously assigns the shape of elliptical curve and, consequently, the set of its points \( EC(GF(q)) \). Employing representation of the form \( \phi : EC \rightarrow P^{k-1} \) and results of assertions 1, 2, we shall construct elliptical \((n, k, d)\) code over \( GF(q) \). If one knows the symbols of extension, then we shall construct extended codes.
6. Basic principles for the construction of cryptosystems on flawed codes

In articles [30, 31], authors considered theoretical and practical fundamentals for the construction of flawed codes. A flawed text is understood to be a text obtained by further deformation of the non-redundant letter codes.

Thus, the necessary and sufficient condition for the flawed text with its meaning lost is a reduction in the lengths of text character codes outside of their redundancy. Consequently, a flawed text is of length that is less than the length of the original text, and it has no meaning of the original text [30].

Theoretical basis for constructing flawed texts is the removal of the orderliness of the original text characters and, consequently, a reduction in the redundancy of language symbols in the flawed text.

In this case, amount of information indicating this orderliness will be equal to a reduction in entropy of the text as compared to the maximally possible magnitude of entropy, that is, equiprobable appearance of any letter after any previous letter. Methods for computing the information, proposed in paper [32], make it possible to identify a ratio of predictable (that is, generated according to certain rules) information and the quantity of the unexpected information that cannot be predicted in advance.

Text redundancy will be calculated from formula

$$B(M) = B_4L_0 = \left( \log N - \frac{H(M)}{L_0} \right) \times L_0,$$

where $M$ is the original text; $B$ is the language redundancy ($B = R - r$), $R$ is the absolute entropy of a language ($R = \log N$, $N$ is the alphabet power), $r$ is the entropy of language per one character, $r = H(M)/L$, $L$ is the length of message $M$ in language characters; $H(M)$ is the entropy (uncertainty) of the message; $L_0$ is the length of message $M$ in language characters with a meaning; $B_4$ is the language redundancy.

In order to obtain a flawed text (FTC) and a damage (DCH), a “perfect” compression method is used after performing $m$ cycles of damaging mechanism $C_m$ [30, 31].

The number of cycles required to minimize the length of the original text is equal to:

$$m = \frac{1}{\log n} \frac{B_4L_0}{\log \eta},$$

where $n$ is the representation power of the original text character; $B_4$ is the language redundancy; $\eta$ is the number of times the length of the original text in MV2 is reduced in each step (a certain constant coefficient).

A quantitative measure of the effectiveness of damage is the degree of destruction of the meaning, equal to the difference in entropies of the flawed text and the original text in different intervals of length of the flawed text:

$$d = H(FTC) - \sum_{i=1}^{M} H(M_i)p_i,$$

where $M_i$ is part of the original text, corresponding to the $i$-th interval, $p_i$ is its probability. $L_0$ is the length $M_i$ equal to length of $L_{FTC}$ of the flawed text, $s$ is the number of intervals.

For an ergodic source of characters for the original text:

$$d_{\min} = \log L_{FTC} - H(M_i).$$

Fig. 3 shows a block diagram of one step of the universal damaging mechanism.

---

**Fig. 3. Block diagram of one step of the universal mechanism for causing damage**

An informational nucleus of some text is understood to be a flawed text $CFT$, obtained by cyclic transformation of the universal mechanism for causing damage $C_m$.

A universal mechanism for causing damage $C_m$ can be described [30, 31]:

$$CFT / CH_{\delta} = E_1(M,KU^{EC}),$$

$$CHD / CH_B = E_1(M,KU^{EC}),$$

$$M = E_1^{-1}(CFT / CH_{\delta}, CHD / CH_B, KU^{EC}),$$

where

$$CFT / CH_{\delta} = CFT / CH_{\delta}, ..., CFT / CH_{\delta},$$

$$KU^{EC} = \varphi(K_{D1}, K_{D2}, K_{D3}, K_{U1}^{EC}, ..., K_{Uw}^{EC}),$$

$$CHD / CH_B = CHD / CH_{\delta}, ..., CHD / CH_{\delta}.$$
To restore the original sequence, it is not required to know the intermediate flawed sequences. One only needs to know the latest flawed sequence (the resulting flawed text after performing all cycles) and all damages with the rules that caused them.

The main techniques for causing damage are shown in Fig. 4. Fig. 5 exhibits main protocols for providing security services based on the use of flawed codes.

Cryptographic flawed texts are the texts obtained by the following ways [30]:

- causing damage to the original text with subsequent encryption of the flawed text and/or its damages;
- causing damage to a ciphertext;
- causing damage to the ciphertext of a flawed text and/or to the ciphertext of damages.

The main advantage in the proposed techniques and protocols for providing security services based on the use of flawed codes is not the application of BSE but the McEliece and Niederreiter MACCS to ensure the crypto resistance of the damage and/or flawed text.

**Fig. 4. Basic techniques to cause damage**

**Fig. 5. Basic protocols for the provision of security services based on the use of flawed codes**
Distance of singularity for the model of a random cipher, for which there is a probability of obtaining a meaningful text at random and equiprobable selection of key \( K \) and while attempting to decrypt the ciphertext at

\[
N_S = H(K)\frac{p_{HL}}{|I|} = 1;
\]

\[
L = U_p = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B \log|I|},
\]

(1)

where \( B \) is the redundancy of the original text; \( H \) is the entropy per a letter of meaningful text in the input alphabet \( I \); \( |I| \geq 2 \), \( 2^{H(I)} \) is the approximated value of the number of meaningful texts.

In articles [30, 31], a cyclic algorithm for obtaining the flawed texts refers to the universal mechanism of causing damage \( C_m \), where \( m \) is the number of cycles), which implies a random replacement of the bit representation of each character of the original text with a tuple of a smaller or equal number of bits with their subsequent concatenation. Fig. 6 shows a universal mechanism of causing damage (algorithm \( MV_2 \) (formation of a flawed text)).

Domain of transformation determination in the \( MV_2 \) algorithm – the set \( \{0, 1\}^n \) is considered to be the alphabet power of certain family of original texts, which are associated with a certain probability distribution of the letters of the given alphabet, while the characters of the original text are the value of a discrete random element [24].

Let \( X \) be a random discrete element that takes values \( x \in \{0,1\}^n \) with probabilities \( p \) and \( T = \{c, f\} \in F^n \) is the arbitrary fixed transformation \( MV_2 \). Then for any \( y \in U_{r+1} \) (a certain binary line from a set of variable-length strings) and for any \( 1 \leq i \leq |y| \), the following holds:

\[
\# \{x \in \{0,1\}^n : c(x) = y\} = \# \{x \in \{0,1\}^n : c(x) = y^{(i)}\}.
\]

Then, regardless of the probability distribution of random element \( X \), for the entropies of random elements \( FTC/FTCH \) (flawed ciphertext) and \( CHD \) (damage), the following equalities hold:

\[
H(FTC / FTCH) \leq \log(2^n - 3).
\]

\[
H(CHD) \leq \log(n - r + 1).
\]

Thus, under uniform distribution of inputs (flags) of the algorithm \( MV_2 \), a uniform distribution of the output (remainder) forms:

\[
P(c_i = 0 | 0 \leq k \leq |FTC / FTCH|) = \frac{1}{2}.
\]

### Algorithm \( MV_2 \)

1. \( r < n \) – positive integer
2. \( n \) – alphabet power
3. \( C_{FT}, CH \) – ciphertext of flawed text
4. \( CHD/CH_0 \) – ciphertext of damage
5. \( FTC/FT_{CH} \) – damaged ciphertext
6. \( DCH/DCH \) – damage to ciphertext
7. \( f(x) \) – flag (damage)
8. \( C(x) \) – remainder (flawed code)

---

**Fig. 6. Universal mechanism for causing damage (algorithm \( MV_2 \))**
An analysis that we performed on the techniques of causing damage revealed that in order to use in IES, the most appropriate one is the first technique – causing damage with subsequent crypto-transformation, which makes it possible to reduce the alphabet power in the formation of a cryptogram in the McEliece MCCS. The distance of singularity for the given method (expression 1) will be transformed to:

\[ U'_b = \sum_{i=1}^{x} (H(CHD^{CI})) + H(KU^{EI}) \cdot \frac{\log p}{B}. \]  

(2)

Such a system is based on the permanent distortion of damage and ensuring stability due to the subsequent use of the encryption based on MCCS. This leads to the impossibility to learn the ciphertext of the flawed text.

Thus, the analysis we performed of the basic principles for the construction of the McEliece MCCS and the multichannel cryptography systems on flawed codes allows us to design hybrid cryptosystems based on the modified asymmetric McEliece crypto-code systems and multichannel cryptography systems on flawed codes. A distinctive difference from the "classical" approach to the formation of a hybrid cryptosystem is the exploitation of asymmetric crypto-code constructions (that relate to secret models with provable stability) with fast crypto-transformations (a rate of transformation is comparable to the crypto-transformations in block-symmetric cipher (BSC) as a key mechanism for ensuring stability (safety) of information with subsequent application of the algorithm MV2 (a system on flawed codes) in order to reduce energy consumption (alphabet power of the McEliece MACCS) with the subsequent transmission along one or several channels. We shall consider practical algorithms for the formation of a cryptogram and decryption in the proposed hybrid cryptosystem.

7. Practical algorithms for the formation and decryption of a cryptogram in hybrid cryptosystems

Fig. 7, 8 show the algorithm for the formation of a cryptogram/codogram in a hybrid cryptosystem.

---

### Stage 1. Setting the code parameters

- **requiredProbability** – preset probability of block distortion, 
- **n** – total quantity of symbols in the code (code length), 
- **k** – quantity of informational symbols, 
- **d** – minimal distance of code combinations by Hamming, 
- **g** – curve genus, 
- **degF** – degree of generator function, 
- **degCurve** – degree of curve

### Stage 2. Causing damage

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Length of remainder</th>
<th>Remainder C(x)</th>
<th>Flag f(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S₀</td>
<td>r</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>S₁</td>
<td>r</td>
<td>0^0</td>
<td>0</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Sₖ₋₁</td>
<td>r+1</td>
<td>0^r+1</td>
<td>0</td>
</tr>
<tr>
<td>Sₖ</td>
<td>n-2</td>
<td>1^r</td>
<td>0¹</td>
</tr>
<tr>
<td>Sₖ₋₁</td>
<td>n-1</td>
<td>0^r</td>
<td>1</td>
</tr>
<tr>
<td>Sₖ</td>
<td>n-1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Sₖ₋₁</td>
<td>n-2</td>
<td>1^r</td>
<td>0¹</td>
</tr>
<tr>
<td>Sₖ</td>
<td>n-2</td>
<td>0^r</td>
<td>1</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Sₖ</td>
<td>r</td>
<td>1^r</td>
<td>0</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

Fig. 7. Stages 1, 2 of the formation of a cryptogram in a hybrid cryptosystem based on the McEliece MACCS with flawed codes.
If the original text had a certain meaning, then, for such a system, flawed texts when using a brute force method over the entire field of encryption keys and key of damage have the only meaningful text equivalent to the original, provided that the length of the ciphertext exceeds the distance of singularity \[30]. Fig. 9 shows the decryption/decoding algorithm of a cryptogram in the proposed hybrid cryptosystem.

The algorithms proposed for the hybrid cryptosystem make it possible, when hiding the flawed ciphertext \( CFT/CHF \), to improve entropy of the public key:

\[
H(CFT/CHF) + \sum_{i=1}^{n} H(\text{CHD}^{(i)}) + H(KU^{EC}) \]

\[ U_b = \frac{H(CHD/CH) + H(CFT/CHF) + \sum_{i=1}^{n} [H(CHD^{(i)})] + H(KU^{EC})}{B \log |P|}, \tag{3} \]

In the case of additional hiding of the last ciphertext of damage \( CHD/CH \) due to its smallness and proportionality with the flawed text ciphertext \( CFT/CHF \), the distance of singularity can be further extended:

\[
H(CHD/CH) + H(CFT/CHF) + \sum_{i=1}^{n} [H(CHD^{(i)})] + H(KU^{EC}) \]

\[ U_b = \frac{H(CHD/CH) + H(CFT/CHF) + \sum_{i=1}^{n} [H(CHD^{(i)})] + H(KU^{EC})}{B \log |P|}, \tag{4} \]

Thus, a multichannel cryptography based on flawed codes makes it possible to integrate cryptographic systems, combining within the framework of one concept the cryptographic constructions (the McEliece MACCS) and the systems on flawed codes, which, by complementing each other, will ensure the required safety and reliability parameters, as well as enrich the resulting system with their properties.
8. Discussion of the research results

The hybrid crypto-code constructions on flawed codes, proposed in the present work, make it possible to obtain maximum quantity of the emergent properties at minimal resource cost, aimed at triggering in the system a synergistic effect of security provision. The main difference between the proposed HCCSFC and the "classical" hybrid cryptosystem is not the application of BSC (a temporary stable model) as the basic mechanism for encryption, but rather the asymmetric cryptosystem (a model of provable stability) based on the McEliece MACCS.

Thus, it is possible to ensure a provable resistance at the encryption rate comparable to the crypto-transformations in BSC, with integrated reliability enabled through the use of interference-resistant codes on elliptic curves. To reduce energy consumption, the algorithm \( MV2 \) is employed, which provides for an increase in the entropy of a ciphertext and makes it possible to transmit a message along one channel (a damage vector can be used in the McEliece MCCS as an error vector \( e \)), or along two independent channels. Therefore, the application of the algorithm \( MV2 \) improves crypto resistance of the system, it makes it possible to “reduce” the alphabet power (di-
mensionality of field $GF(2^m)$ for the construction of the McEliece MCCS without compromising crypto stability of the system as a whole.

We shall estimate energy cost and stability of the proposed HCCSFC.

**Estimation of energy cost for the software implementation of the proposed hybrid cryptosystem.**

In order to evaluate temporal and speed indicators, a $cpb$ unit of measurement is typically applied, where $cpb$ (cycles per byte) is the number of cycles of the processor required to spend to process 1 byte of incoming information.

The algorithm complexity will be to computed from expression

$$\text{Per} = \frac{Utl \times \text{clock}}{\text{Rate}},$$

where $Utl$ is the processor’s core utilization (%); $Rate$ is the algorithm throughput (byte/sec).

Table 3 gives results of examining a dependence of the length of code sequence of the algebraic geometric code in the McEliece MACCS on the number of processor cycles to perform elementary operations in the software implementation of crypto-code systems.

Table 4 gives results of the study into dependence of length of the input sequence on the algorithm $MV2$ on the number of processor cycles to perform elementary operations in the software implementation.

Table 5 gives research results of the estimation of temporal and speed parameters of the procedures to form and decode information in the asymmetric crypto-code systems based on the McEliece TCS.

### Table 3

**Results of examining a dependence of the length of code sequence of code in the McEliece ACCS and the modified ACCS on the number of processor cycles**

<table>
<thead>
<tr>
<th>Code sequence length</th>
<th>McEliece on truncated codes</th>
<th>McEliece</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>Number of calls for functions that implement basic operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol readout</td>
<td>10 294 397</td>
<td>28 750 457</td>
</tr>
<tr>
<td>String comparison</td>
<td>3 406 921</td>
<td>9 246 748</td>
</tr>
<tr>
<td>String concatenation</td>
<td>1 705 544</td>
<td>5 045 748</td>
</tr>
<tr>
<td>Total</td>
<td>15 406 862</td>
<td>43 042 953</td>
</tr>
<tr>
<td>Duration of function* realization in processor cycles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbol readout</td>
<td>293 354</td>
<td>810 478</td>
</tr>
<tr>
<td>String comparison</td>
<td>178 814</td>
<td>531 379</td>
</tr>
<tr>
<td>String concatenation</td>
<td>544 990</td>
<td>1 328 114</td>
</tr>
<tr>
<td>Total</td>
<td>1 006 781</td>
<td>2 749 548</td>
</tr>
<tr>
<td>Implementation duration**, msec</td>
<td>0.52</td>
<td>1.37</td>
</tr>
</tbody>
</table>

Notes: * – duration of 1000 operations in processor cycles: symbol readout – 27 cycles, string comparison – 54 cycles, string concatenation – 297 cycles; ** – in the calculation we used processor with a clock frequency of 2 GHz, taking into account loading the operating system by 5 %

### Table 4

**Results of the study into dependence of length of the input sequence on the algorithm $MV2$ on the number of processor cycles**

<table>
<thead>
<tr>
<th>Code sequence length</th>
<th>$MV2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Number of calls for functions that implement basic operations</td>
<td></td>
</tr>
<tr>
<td>Summing</td>
<td>3942</td>
</tr>
<tr>
<td>Difference</td>
<td>1794</td>
</tr>
<tr>
<td>Division</td>
<td>3274</td>
</tr>
<tr>
<td>Multiplication</td>
<td>19</td>
</tr>
<tr>
<td>Comparison</td>
<td>8939</td>
</tr>
<tr>
<td>Total</td>
<td>17968</td>
</tr>
<tr>
<td>Duration of function* realization in milliseconds</td>
<td></td>
</tr>
<tr>
<td>Summing</td>
<td>19.53</td>
</tr>
<tr>
<td>Difference</td>
<td>8.89</td>
</tr>
<tr>
<td>Division</td>
<td>16.22</td>
</tr>
<tr>
<td>Multiplication</td>
<td>0.09</td>
</tr>
<tr>
<td>Comparison</td>
<td>44.28</td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
</tr>
<tr>
<td>Duration of implementation**, msec</td>
<td>89</td>
</tr>
</tbody>
</table>

Notes: * – duration of 1000 operations in processor cycles: symbol readout – 27 cycles, string comparison – 54 cycles, string concatenation – 297 cycles; ** – in the calculation we used processor with a clock frequency of 2 GHz, taking into account loading the operating system by 5 %
sum of probabilities is \((p_1+p_2+\ldots+p_n-1)\), because the source is always in one of its states. If any of the probabilities \(p_i\) does not equal 1, then it is impossible to unambiguously identify the state of the system, in other words, the system possesses uncertainty.

When determining the quantity of information, the only function that measures such types of uncertainty is the following [26]:

\[
H(p_1,p_2,\ldots,p_n) = - \sum_{i=1}^{n} p_i \log_2 p_i. \tag{5}
\]

This function is called the entropy by analogy with physical entropy. If all events in the system are equiprobable, that is,

\[
p_i = \frac{1}{n},
\]

then

\[
H = \log_2 n. \tag{6}
\]

where \(n\) is the number of equiprobable events.

Equation (6) is a particular case of the Shannon formula (5) and it is called the Hartley formula.

Now we shall consider in terms of information theory the transformations that the encryption systems introduce to the original text.

Let us imagine an arbitrary cryptographic transformation in the form of a “black box”, which assigns a cryptogram to the incoming message, that is, it converts a set of incoming messages to a set of cryptograms:

\[
\{M_i\} \rightarrow \{C_i\}. \tag{7}
\]

Transformation of type (7) will change the entropy of an incoming message. Consider such a transformation and calculate the entropy, which is added by an encryption mechanism, the algorithm is shown in Fig. 10.

1. We shall calculate the entropy of an incoming message.

Assume that we have an open message of length \(N\). By counting the number of occurrences of each character in message \(n_i\), we shall compute the mean probability of that the given symbol is found in this message:

\[
H_n(\{p_1, p_2, \ldots, p_N\}) = - \sum_{i=1}^{N} p_i \log_2 p_i. \tag{8}
\]

we shall obtain entropy of the incoming message.

2. We shall send the incoming message to the encryption system input, which mandatory significantly increases the entropy of the message.

3. As a result of processing, the incoming message is converted into a ciphertext. In the case of an ideal cipher, at the output, in line with (7), we should receive a random number. Because for the random number, on average, the emergence of each character should be equiprobable, the entropy of such a ciphertext should be described by the Hartley formula (8). This means, for example, that in the case of a binary alphabet \((0,1)\), on average, a cryptogram should contain half of zeros (half of units). It is clear that the entropy of such ciphertext should be maximal.
4. Actual ciphers differ from the ideal in that the entropy of the cryptogram created by them will not be maximal. However, it is clear that in the course of processing the incoming message entropy will increase.

5. We shall compute the cryptogram entropy in the way similar to the incoming message:

\[ H_c(p_1, p_2, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i. \]  \hspace{1cm} (9)

6. Difference

\[ H_c - H_M = H_{cypher}. \]  \hspace{1cm} (10)

For the systems on flawed codes:

\[ d = H(CFT / CH_{pv}) - H(M). \]  \hspace{1cm} (11)

Magnitude \( d \) characterizes the degree of disorderliness of the flawed text characters compared to the orderliness of the original text [24].

This contribution may consist of various components – the entropy of key, the entropy of replacement blocks and entropy of the MV2-transformation:

\[ H_{cypher} = H_K + H_{J-box} + H_{MV2}. \]  \hspace{1cm} (12)

By changing encryption keys, replacement blocks, number of cycles, etc., it is possible to investigate their influence on the resulting ciphertext entropy and thus establish its optimal structure and components.

The best cipher (in terms of entropy) will be considered the one whose entropy \( H_{cypher} \) is maximal. This is consistent with the notion of a cipher as the ideal oracle, which should match...
each open message to a random number. The closer the resulting encrypted cryptogram to the random number (a maximum of entropy, which in this case is determined by the Hartley formula), the higher resistance of the crypto algorithm.

7. The measure of difference between the examined cipher and the ideal can also be expressed using the entropy. The bigger the difference:

\[ H_e = -\log_2 n, \]  
(13)

the less resistant is the examined crypto algorithm.

Thus, the basic steps in the procedure for the estimation of crypto stability based on entropy randomness evaluation method are:

**Stage 1.** Calculation of entropy of the input information vector (expression 8).

**Stage 2.** Calculation of entropy of the cryptogram (expression 10).

**Stage 3.** Calculation of the extent of disorderliness in the flawed text characters compared to the orderliness of the original text (expressions 11, 12).

**Stage 4.** Estimation of stability of the cryptosystem (expression 13).

The given approach to the estimation of resistance is the most applicable to the developed hybrid cryptosystem on the McEliece MACCS on flawed codes.

9. Conclusions

1. We performed an analysis of the development of services and functionality of IES (CES), which revealed that such systems should regarded as OCCI that form part of MCIS. With the growth of informatization and further development of remote access to sociosystems and CES, a relevant issue is to provide security and reliability in order to ensure the required level of quality service for the IES users.

2. We analyzed a general structure for building the asymmetric crypto-code constructions based on the McEliece TCS, which comprehensively (employing one mechanism) provide the required indicators of reliability, efficiency, and security of data. A major shortcoming of ACCS is a large amount of key data that narrows the scope of their application in various areas of communications systems. In order to ensure the required parameters of stability, it is required to use the alphabet power over \( GF(2^8) \). Application of the modified (truncated/extended) elliptical codes makes it possible to reduce the volume of key data, while maintaining the requirements to the ACCS crypto resistance. The data conversion performance efficiency estimation is comparable to the rate of crypto-transformations in modern BSE; in this case, crypto resistance is provided at the level of the NP-problem – decoding a random code.

3. The employment of the algorithm M\( \sqrt{2} \) of the systems on flawed codes improves crypto stability of the proposed hybrid system, and makes it possible to “reduce” the alphabet power (dimensionality of field \( GF(2^6-2^3) \) for the construction of the McEliece MCCS) without compromising reliability of the system as a whole.

The given approach allows constructing hybrid cryptosystems whose main feature is a new approach to their formation – the asymmetric cryptosystems based on MACCS are used for encryption, while in order to improve resistance, the multichannel systems on flawed codes are employed. To assess their stability, we propose in the present work to use a technique based on the entropy assessment method that makes it possible to estimate total resistance of a hybrid cryptosystem.

4. Transmission of confidential data and key sequences of standard encryption algorithms in IES on the basis of the proposed hybrid cryptosystem allows the use of open channels of GIN and CES. For the IES users, the required parameters of safety, reliability, and efficiency over the entire cycle of information processing are provided.

**References**


