UDC 621.391
DOI: 10.15587/1729-4061.2017.108461

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

Розглядаються принципи побудови крипто-кодових конструкцій на алгеброгеометрічних (еліптичних) кодах, багатоканальних криптосистем на основі збиткових кодів. Пропонуються гібридні крипто-кодові конструкції на збиткових кодах, алгоритми формування та розшифрування криптограми в гібридних криптосистемах на основі крипто-кодових конструкцій з збитковими кодами. Обґрунтовується ефективність та стійкість запропонованих гібридних конструкцій на основі оцінки енергозатрат й запропонованої методики оцінки стійкості

Ключові слова: гібридні криптосистеми, несиметрична крипто-кодова конструкція, алгеброгеометричні коди, збиткові коди

Рассматриваются принципы построения крипто-кодовых конструкций на алгеброгеометрических (эллиптических) кодах, многоканальных криптосистем на основе ущербных кодов. Предлагаются гибридные крипто-кодовые конструкции на ущербных кодах, алгоритмы формирования и расшифрования криптограммы в гибридных криптосистемах на основе крипто-кодовых систем Мак-Элиса с ущербными кодами. Обосновывается эффективность и стойкость предложенных гибридных конструкций на основе оценки энергозатрат и предложенной методики оценки стойкости

Ключевые слова: гибридные криптосистемы, несимметричная крипто-кодовая конструкция, алгеброгеометрические коды, ущербные коды

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 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 structure of 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.

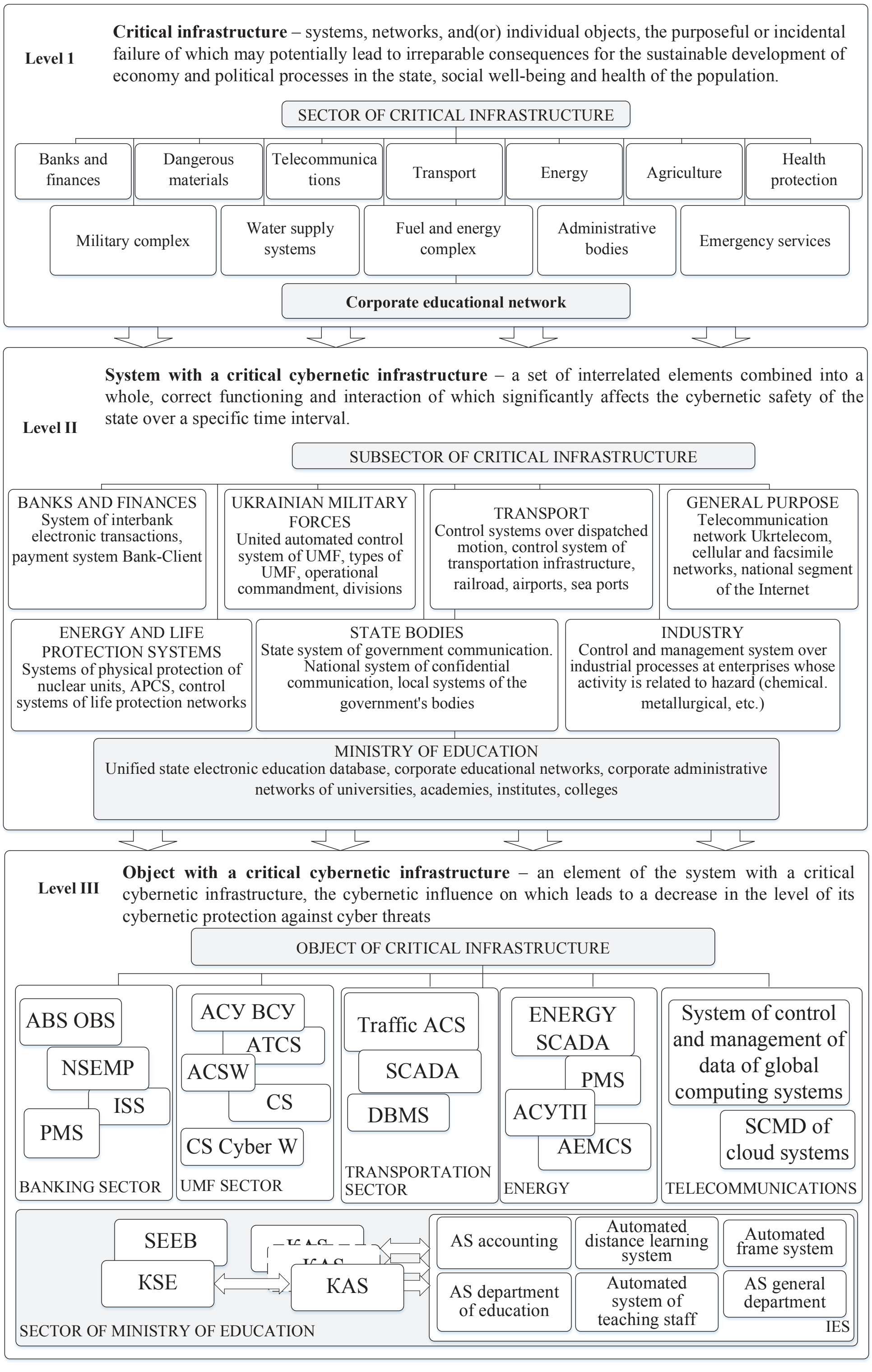

Level 1
Critical infrastructure – systems, networks, and(or) individual objects, the purposeful or incidental failure of which may potentially lead to irreparable consequences for the sustainable development of economy and political processes in the state, social well-being and health of the population.
SECTOR OF CRITICAL INFRASTRUCTURE
Banks and finances
Dangerous materials
Telecommunica tions
Transport
Energy
Agriculture
Health protection
Military complex
Water supply systems
Fuel and energy complex
Administrative bodies
Emergency services
Corporate educational network
Level II
System with a critical cybernetic infrastructure – 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.
SUBSECTOR OF CRITICAL INFRASTRUCTURE
BANKS AND FINANCES System of interbank electronic transactions, payment system Bank-Client
UKRAINIAN MILITARY FORCES United automated control system of UMF, types of UMF, operational commandment, divisions
TRANSPORT Control systems over dispatched motion, control system of transportation infrastructure, railroad, airports, sea ports
GENERAL PURPOSE Telecommunication network Ukrtelecom, cellular and facsimile networks, national segment of the Internet
ENERGY AND LIFE PROTECTION SYSTEMS Systems of physical protection of nuclear units, APCS, control systems of life protection networks
STATE BODIES State system of government communication. National system of confidential communication, local systems of the government's bodies
INDUSTRY Control and management system over industrial processes at enterprises whose activity is related to hazard (chemical. metallurgical, etc.)
MINISTRY OF EDUCATION Unified state electronic education database, corporate educational networks, corporate administrative networks of universities, academies, institutes, colleges
Level III
Object with a critical cybernetic infrastructure – an element of the system with a critical cybernetic infrastructure, the cybernetic influence on which leads to a decrease in the level of its cybernetic protection against cyber threats
OBJECT OF CRITICAL INFRASTRUCTURE
ABS OBS
NSEMP
ISS
PMS
BANKING SECTOR
АСУ ВСУ
ATCS
ACSW
CS
CS Cyber W
UMF SECTOR
Traffic ACS
SCADA
DBMS
TRANSPORTATION SECTOR
ENERGY SCADA
PMS
АСУТП
AEMCS
ENERGY
System of control and management of data of global computing systems
SCMD of cloud systems
TELECOMMUNICATIONS
SEEB
KSE
KAS
KAS
KAS
AS accounting
Automated distance learning system
Automated frame system
AS department of education
Automated system of teaching staff
AS general department
IES
SECTOR OF MINISTRY OF EDUCATION

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 $GF(q)$, vector space $GF^n(q)$ as a set of n-sequences of elements from $GF(q)$ with a component by component addition and multiplication by a scalar. *Linear (n, k, d) code C* is the subspace in $GF^n(q)$, that is, a non-empty set of n-sequences (*codewords*) over $GF(q)$, *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 of length r, $r=n-k$) 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-Hocquingham (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 $O(t^2)$, where 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].

Asymptotic complexity of decoding the Reed-Solomon codes in this case does not exceed the magnitude $O(n\log^2 n)$, and it is very close to the magnitude $O(n\log n)$.

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 $GF(q)$, 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.

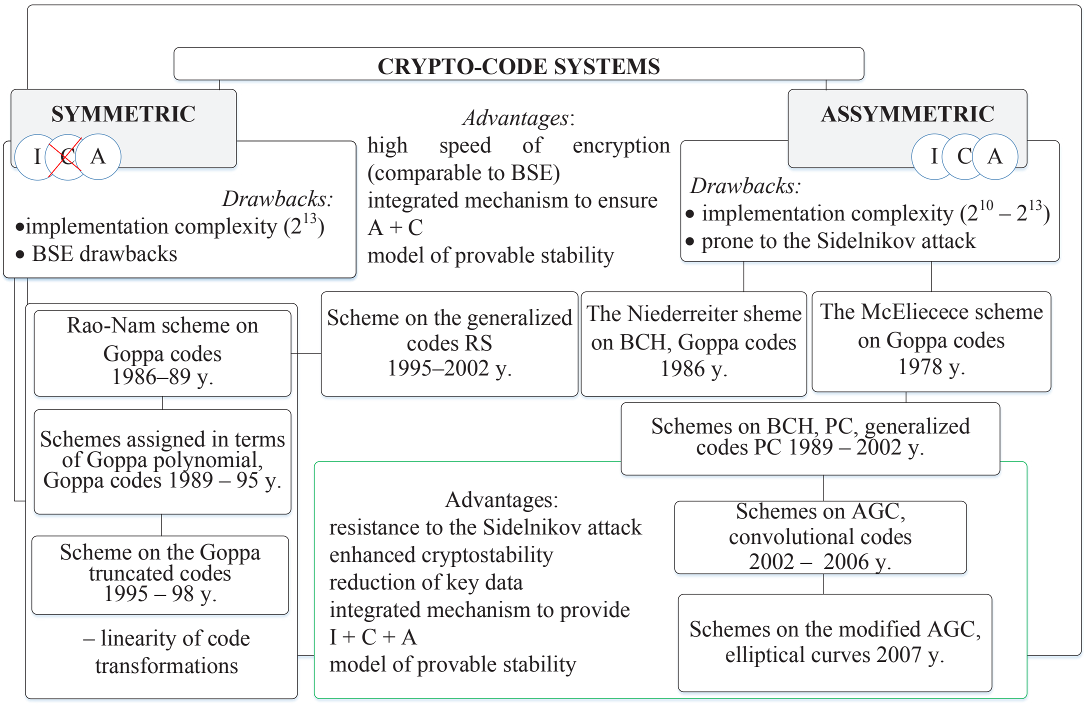

CRYPTO-CODE SYSTEMS
SYMMETRIC
I C A
Drawbacks:
•implementation complexity (2^{13})
• BSE drawbacks
Advantages:
high speed of encryption (comparable to BSE)
integrated mechanism to ensure A + C
model of provable stability
ASSYMMETRIC
I C A
Drawbacks:
• implementation complexity (2^{10} – 2^{13})
• prone to the Sidelnikov attack
Rao-Nam scheme on Goppa codes 1986–89 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
Scheme on the generalized codes RS 1995–2002 y.
The Niederreiter sheme on BCH, Goppa codes 1986 y.
The McEliecece scheme on Goppa codes 1978 y.
Schemes on BCH, PC, generalized codes PC 1989 – 2002 y.
Advantages:
resistance to the Sidelnikov attack
enhanced cryptostability
reduction of key data
integrated mechanism to provide I + C + A
model of provable stability
Schemes on AGC, convolutional codes 2002 – 2006 y.
Schemes on the modified AGC, elliptical curves 2007 y.

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

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 $GF(q)$, $g=g(X)$ 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 $\alpha>g-1$. Then C determines mapping φ: $X\to P^{k-1}$, where $k\geq\alpha-g+1$. Set $y_i=\varphi(x_i)$ assigns the code. The number of points in the intersection $\varphi(X)$ with a hyperplane equals α, that is, $n-d\leq\alpha$. This construction allows us to build codes with parameters $k+d\geq n-g+1$, whose length n is less than or equal to the number of points on the X curve. At $2g<\alpha\leq n$, algebraic geometric code has parameters $(n, \alpha-g+1, d)$, $d\geq n-\alpha$. Its dual code is also algebraic geometric, and has parameters $(n, n-\alpha+g-1, d^{\perp})$, $d^{\perp}\geq\alpha-2g+2$. Structural characteristics of the elliptic codes, constructed through representation of the form φ: $EC\to P^{k-1}$ over $GF(q)$, $q=2^m$, $m=\overline{2,6}$, are given in Table 1.

Table 1

Structural code characteristics of the elliptic codes, constructed through representation j: EC→pk^{-1} over GF(q), q=2m, $m=\overline{2,6}$

deg$F$	α	(n, k, d)				
		$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
1	3	9, 3, 6	14, 3, 11	25, 3, 22	44, 3, 41	81, 3, 78
2	6	9, 6, 3	14, 6, 8	25, 6, 19	44, 6, 38	81, 6, 75
3	9	–	14, 9, 5	25, 9, 16	44, 9, 35	81, 9, 72
4	12	–	14, 12, 2	25, 12, 13	44, 12, 32	81, 12, 69
5	15	–	–	25, 15, 10	44, 15, 29	81, 15, 66
6	18	–	–	25, 18, 7	44, 18, 26	81, 18, 63
7	21	–	–	25, 21, 4	44, 21, 23	81, 21, 60
8	24	–	–	–	44, 24, 20	81, 24, 57
9	27	–	–	–	44, 27, 17	81, 27, 54
10	30	–	–	–	44, 30, 14	81, 30, 51
11	33	–	–	–	44, 33, 11	81, 33, 48
12	36	–	–	–	44, 36, 8	81, 36, 45
13	39	–	–	–	44, 39, 5	81, 39, 42
14	42	–	–	–	44, 42, 2	81, 42, 39
15	45	–	–	–	–	81, 45, 36
16	48	–	–	–	–	81, 48, 33
17	51	–	–	–	–	81, 51, 30
18	54	–	–	–	–	81, 54, 27
19	57	–	–	–	–	81, 57, 24
20	60	–	–	–	–	81, 60, 21
21	63	–	–	–	–	81, 63, 18
22	66	–	–	–	–	81, 66, 15
23	69	–	–	–	–	81, 69, 12
24	72	–	–	–	–	81, 72, 9
25	75	–	–	–	–	81, 75, 6
26	78	–	–	–	–	81, 78, 3

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 deg$F$. Let $I(i_1, i_2,..., i_n)$ be the informational sequence. *Algebraic geometric code along the X curve* over *GF(q)* is a linear code of length $n\leq N$, whose codewords $C(c_1, c_2, ..., c_n)$ are assigned by equality

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i,$$

where $P_i(X_i, Y_i, Z_i)$ 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, $i=\overline{1,n}$; $F_j(P_i)$ are the values of generator functions in the points of the curve.

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

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

where G is the generating matrix of dimension $k\times n$, $k=\alpha-g+1$, $\alpha=\deg X\times\deg F$.

$$G=\begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j\left(P_i\right) \right\|_{n,k}.$$

Definition 2 [17]. *An elliptic curve (EC)* in the affine space 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 *(n, k, d)* code along an elliptic curve (elliptical code) over *GF(q)*, constructed through representation of the form φ: $EC\to P^{k-1}$, is bound by characteristics $k+d\geq n$; in this case

$$n\leq 2\sqrt{q}+q+1,\ k\geq\alpha,\ d\geq n-\alpha,\ \alpha=3\times\deg F.$$

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 deg$F$. *Algebraic geometric code along the X curve* over *GF(q)* is a linear code, consisting of all words $(c_1, c_2, ..., c_n)$ of length $n\leq N$, for which equality $d+g-1$ of equations holds

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0,$$

where $c_i\in GF(q)$, $d\geq\alpha-2g+2$, $\alpha=\deg X\times\deg F$.

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

$$H\,(c_0, c_1, ..., c_{n-1})^{\mathrm{T}} = 0,$$

where H is the test code matrix of dimension $r\times n$, $r=$ $=n-k=d+g-2$

$$H=\begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

Assertion 2 [17]. Elliptical (n, k, d) code over $GF(q)$, constructed through representation of the form $\varphi\colon EC\to P^{r-1}$ is bound by characteristics $k+d\geq n$; in this case: $n\leq 2\sqrt{q}+q+1$, $k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times\deg F$.

Definitions 1, 2 and the result of assertion 1 make it possible to set the McElice theoretical-code scheme on the basis of the elliptic codes in the following way. Let G^{EC} be a generating matrix of elliptical (n, k, d) code over $GF(q)$ of the form

$$G^{EC}=\begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}.$$

and a dimension of $k\times n$, $k=\alpha$, $\alpha=3\times\deg F$.

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

$$G_X^{EC}=X\cdot G^{EC}\cdot P\cdot D,$$

– secret (closed) key – matrices *X, P, and D.*

Closed information (a codogram) is a vector of length n and is calculated by rule

$$c_X^*=i\cdot G_X^{EC}+e,$$

where vector $c_X=i\cdot G_X^{EC}$ belongs to elliptical (n, k, d) code with generative matrix G_X^{EC}, i is the k-digit information vector, vector e is the secret weight error vector $\leq t$.

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^n, that is, a totality of the solutions of a homogeneous unreduced algebraic equation of degree degX 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 $(c_1, c_2, \dots, c_n)$ of length $n\leq N$, for which equality $d+g-1$ of the equations holds

$$\sum_{i=0}^{n-1} c_i F_j(P_i)=0,$$

where $c_i\in GF(q)$, $d\geq\alpha-2g+2$, $\alpha=\deg X\times\deg F$.

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

$$H\,(c_0, c_1, \dots, c_{n-1})^{\mathrm{T}}=0,$$

where H is the test code matrix of dimension $r\times n$, $r=$ $=n-k=d+g-2$

$$H=\begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

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

$$H^{EC}=\begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}$$

and a dimension of $r\times n$, $r=\alpha$, $\alpha=3\times\deg F$.

Let X be a nondegenerate $k\times k$-matrix over $GF(q)$, D is the diagonal matrix with nonzero diagonal elements, P is the permutation matrix of dimension $n\times n$. We shall determine the asymmetric *Niederreiter scheme with elliptical code* [23]:

– public key – matrix $H_X^{EC}\ =\ X\ \cdot H^{EC}\cdot P\cdot D,$

– secret (closed) key – matrices *X, P* and *D.*

Closed information (a codogram) is a vector of length n and it is calculated by rule

$$S_X=e\cdot\left(H_X^{EC}\right)^{\mathrm{T}},$$

where vector e is the vector of length n and weight ≤t, which carries confidential information (informational message subject to be closed).

Proven assertions 1, 2 and the proposed theoretical-code scheme with elliptic codes allow us to create codograms by a nonsymmetrical algorithm, that is, to use a public key for the exchange of closed information.

Nevertheless, an analysis conducted in [17, 21] of the software implementation of an asymmetric crypto-code system on the theoretical-code scheme (TCS) by McEliece and Niederreiter revealed considerable complexities in the software implementation, which significantly complicates the application of ACCS in the GIN open systems protocols. Dependence of group operations of the ACCS implementation on field power is given in Table 2.

Table 2

Dependence of software implementation on field power

McEliece ACCS	2^5	2^6	2^7	2^8	2^9	2^{10}
EC	10018042	18048068	32847145	47489784	63215578	82467897
truncated EC	10007947	17787431	28595014	44079433	61974253	79554764
extended EC	11156138	18561228	33210708	48297112	65171690	84051337

In order to reduce energy consumption for the crypto-transformations into the McEliece ACCS, authors ofn paper [17] propose to use the modified ACCS (MCCS) on the modified ASC on EC.

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 $I=(I_1, I_2, ..., I_k)$ be the information vector (n, k, d) of a block code. Choose subset h of informational symbols, $|h|=x$, $x\leq 1/2k$. Put zeroes into information vector I in the subset h, that is, $I_i=0$, $\forall I_i \in h$. 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, $X\cup h=EC(GF(q))$, $|h|=x$. Then the *truncated* elliptical (n, k, d) code over $GF(q)$, constructed through representation of the form $\varphi: X\to P^{k-1}$, is bound by characteristics $k+d\geq n$; in this case:

$$n=2\sqrt{q}+q+1-x,$$

$k\geq\alpha-x$, $d\geq n-\alpha$, $\alpha=3\times\deg F$.

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

$$n=2\sqrt{q}+q+1-x,$$

$k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times\deg F$.

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 $\varphi: X\to P^{k-1}$ and $\varphi: X\to P^{r-1}$. The following assertions are true.

Assertion 5. Truncated elliptical (n, k, d) code over $GF(2^m)$, constructed through representation of the form $\varphi: X\to P^{k-1}$, determines a modified theoretical-code scheme with the following parameters:

$$l_{K_+}=x\left\lceil\log_2\left(2\sqrt{q}+q+1\right)\right\rceil;$$

$l_I=(\alpha-x)\cdot m$;

$$R=(\alpha-x)/\left(2\sqrt{q}+q+1-x\right).$$

Assertion 6. Truncated elliptical (n, k, d) code over $GF(2^m)$, constructed through representation of the form $\varphi: X\to P^{r-1}$, determines a modified theoretical-code scheme with the following parameters:

– dimensionality of the secret key is given by expression

$$l_{K_+}=x\left\lceil\log_2\left(2\sqrt{q}+q+1\right)\right\rceil;$$

– dimensionality of the informational vector (in bits):

$$l_I=\left(2\sqrt{q}+q+1-\alpha\right)\times m;$$

– dimensionality of the codogram is determined by expression

$$l_S=\left(2\sqrt{q}+q+1-x\right)\times m;$$

– relative transmission rate:

$$R=\left(2\sqrt{q}+q+1-\alpha\right)/\left(2\sqrt{q}+q+1-x\right).$$

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 $I=(I_1, I_2,..., I_k)$ be the informational vector (n, k, d) of a block code. Choose subset h of informational symbols, $|h|=x$, $x\leq 1/2k$ and *generate an initialization vector.* Put in informational vector I in the subset h zeros, that is, $I_i=0$, $\forall I_i\in h$. 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 $h_1\subseteq h$, $|h_1|=x_1$. Let the elliptical (n, k, d) code over $GF(q)$ be assigned, constructed through representation of the form $\varphi: X\to P^{k-1}$. Then parameters of the elliptic code, *extended* by x_1 symbols from $GF(q)$, constructed through representation of the form $\varphi: (X\cup h_1)\to P^{k-1}$, $n=2\sqrt{q}+q+1-x+x_1$ will be bound by relations: $k\geq\alpha-x+x_1$, $d\geq n-\alpha$, $\alpha=3\times\deg F$.

Proof. If $x_1<x$, then extending the code by x_1 is equivalent to the truncation of source code by $x-x_1$. Substituting these parameters in expression $n=2\sqrt{q}+q+1-x+x_1$, we shall obtain the result of corollary 7.

Corollary 1. If one knows the shape of elliptical curve (set $a_1...a_6$, $\forall a_i\in GF(q)$), then subsets h and h_1 completely determine the modified elliptical (n, k, d) codes over $GF(q)$, constructed through representation of the form: $\varphi: X\to P^{k-1}$ and $\varphi:(X\cup h_1)\to P^{k-1}$.

Proof. Set of coefficients $a_1...a_6$, $\forall a_i\in GF(q)$ unambiguously assigns the shape of elliptic curve and, consequently, the set of its points $EC(GF(q))$. Employing representation of the form $\varphi: EC\to P^M$ 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 $h_1\subseteq h$, $|h_1|=x_1$. Assume that the elliptical (n, k, d) code over $GF(q)$ is assigned, constructed through representation of the form $\varphi: X\to P^{r-1}$. Then parameters of the elliptic code, extended by x_1 symbols from $GF(q)$, constructed through representation of the form $\varphi: (X\cup h_1)\to P^{r-1}$, will be bound by relations: $n=2\sqrt{q}+q+1-x+x_1$, $k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times\deg F$.

Corollary 2. If one knows the shape of an elliptic curve (set $a_1...a_6$, $\forall a_i\in GF(q)$), then subsets h and h_1 completely determine the modified elliptical (n, k, d) codes over $GF(q)$, constructed through representation of the form: φ: $X \to P^{r-1}$ and φ: $(X \cup h_1) \to P^{r-1}$.

Proof. Set of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ unambiguously assigns the shape of elliptic curve and, consequently, the set of its points $EC(GF(q))$. Applying representation of the form φ: $EC \to P^M$ 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 8, these are the symbols of sets *h* and h_1, which completely determine the modified elliptical *(n, k, d)* code over *GF(q)*.

Results of assertions 7, 8 and their corollaries allow us to construct modified (extended within $n \le 2\sqrt{q} + q + 1$) elliptical *(n, k, d)* codes over GF(q).

Thus, the proposed crypto-code constructions make it possible to build asymmetric cryptosystems (of provable stability) that comprehensively (applying one mechanism) provide the speed of crypto/code-transformations at the BSE level and the required confidence level (P_{err} 10^{-9}–10^{-12}).

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

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

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_A 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:

$$m \rangle \frac{\log n - B_A}{\log \eta},$$

where *n* is the representation power of the original text character; B_A is the language redundancy; η 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:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i) p_i, \ \sum_{i=1}^{s} p_i = 1, \ \ s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right],$$

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:

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

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

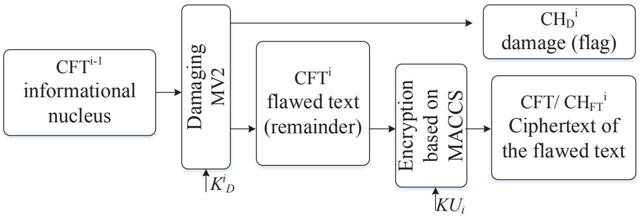


Fig. 3. Block diagram of one step of the universal mechanism for causing damage

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]:

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

$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$

$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

where

$$CFT / CH_{FT} = CFT / CH_{FT}^i, \ldots, CFT / CH_{FT}^m,$$

$$KU^{EC} = \varphi(K_D^i, \ldots, K_D^m, KU_1^{EC}, \ldots, KU_m^{EC},$$

$$CHD / CH_D = CHD / CH_D^i, \ldots, CHD / CH_D^m.$$

Thus, we have two ciphertexts (damage (damage (CH_D) and the flawed text (*FTC*)), each of which makes no sense neither in the alphabet of the original text, nor in the ciphertext alphabet. Actually, a ciphertext of the original message (*M*) is represented as a totality of two flawed ciphertexts, each of which cannot recover the original text separately.

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.

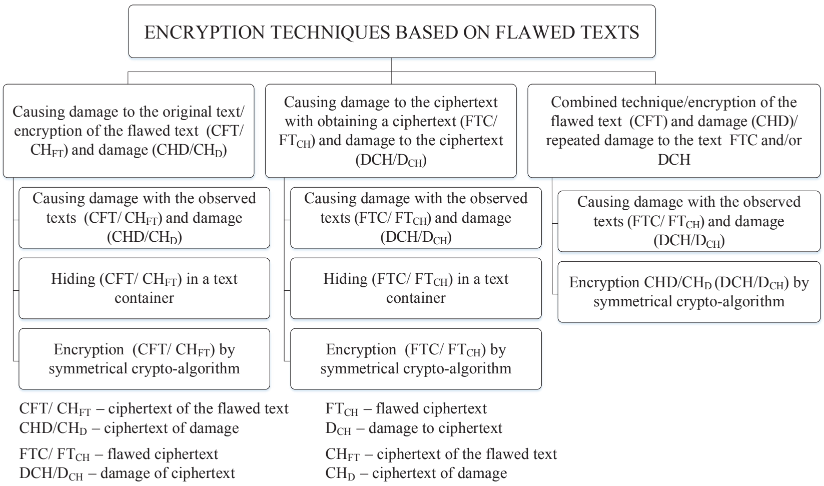

ENCRYPTION TECHNIQUES BASED ON FLAWED TEXTS
Causing damage to the original text/ encryption of the flawed text (CFT/ CH_{FT}) and damage (CHD/CH_D)
Causing damage to the ciphertext with obtaining a ciphertext (FTC/ FT_{CH}) and damage to the ciphertext (DCH/D_{CH})
Combined technique/encryption of the flawed text (CFT) and damage (CHD)/ repeated damage to the text FTC and/or DCH
Causing damage with the observed texts (CFT/ CH_{FT}) and damage (CHD/CH_D)
Hiding (CFT/ CH_{FT}) in a text container
Encryption (CFT/ CH_{FT}) by symmetrical crypto-algorithm
Causing damage with the observed texts (FTC/ FT_{CH}) and damage (DCH/D_{CH})
Hiding (FTC/ FT_{CH}) in a text container
Encryption (FTC/ FT_{CH}) by symmetrical crypto-algorithm
Causing damage with the observed texts (FTC/ FT_{CH}) and damage (DCH/D_{CH})
Encryption CHD/CH_D (DCH/D_{CH}) by symmetrical crypto-algorithm
CFT/ CH_{FT} – ciphertext of the flawed text
CHD/CH_D – ciphertext of damage
FTC/ FT_{CH} – flawed ciphertext
DCH/D_{CH} – damage of ciphertext
FT_{CH} – flawed ciphertext
D_{CH} – damage to ciphertext
CH_{FT} – ciphertext of the flawed text
CH_D – ciphertext of damage

Fig. 4. Basic techniques to cause damage

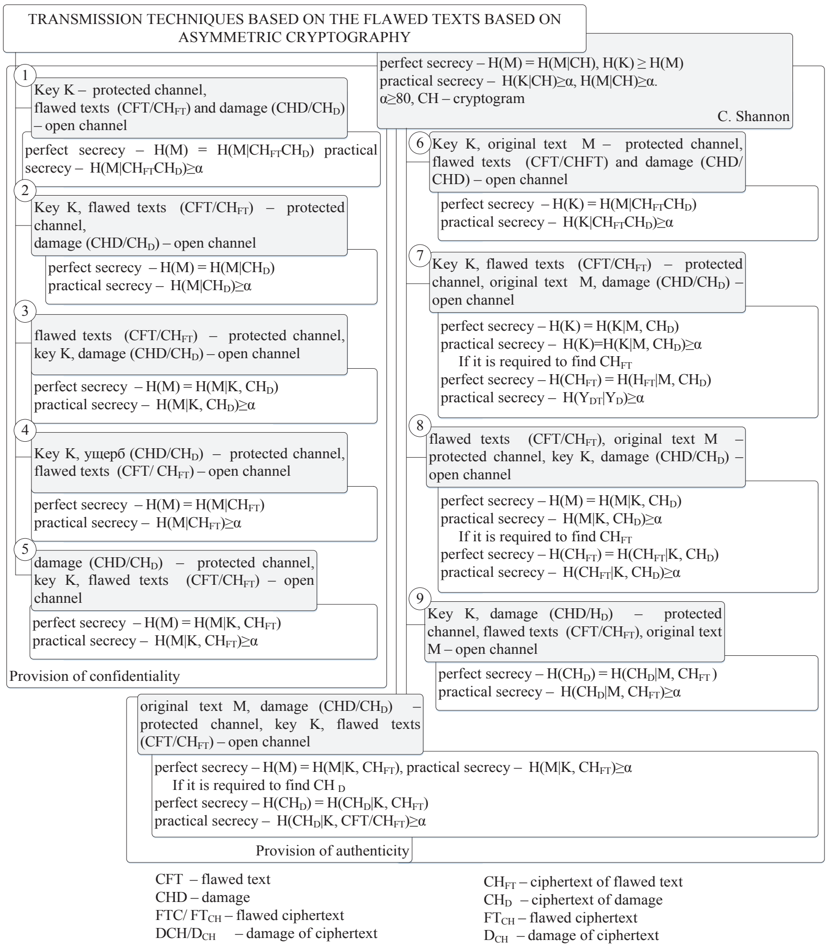

TRANSMISSION TECHNIQUES BASED ON THE FLAWED TEXTS BASED ON ASYMMETRIC CRYPTOGRAPHY
perfect secrecy – H(M) = H(M|CH), H(K) ≥ H(M)
practical secrecy – H(K|CH)≥α, H(M|CH)≥α.
α≥80, CH – cryptogram
C. Shannon
1
Key K – protected channel, flawed texts (CFT/CH_{FT}) and damage (CHD/CH_D) – open channel
perfect secrecy – H(M) = H(M|$CH_{FT}CH_D$) practical secrecy – H(M|$CH_{FT}CH_D$)≥α
2
Key K, flawed texts (CFT/CH_{FT}) – protected channel, damage (CHD/CH_D) – open channel
perfect secrecy – H(M) = H(M|CH_D)
practical secrecy – H(M|CH_D)≥α
3
flawed texts (CFT/CH_{FT}) – protected channel, key K, damage (CHD/CH_D) – open channel
perfect secrecy – H(M) = H(M|K, CH_D)
practical secrecy – H(M|K, CH_D)≥α
4
Key K, ущерб (CHD/CH_D) – protected channel, flawed texts (CFT/ CH_{FT}) – open channel
perfect secrecy – H(M) = H(M|CH_{FT})
practical secrecy – H(M|CH_{FT})≥α
5
damage (CHD/CH_D) – protected channel, key K, flawed texts (CFT/CH_{FT}) – open channel
perfect secrecy – H(M) = H(M|K, CH_{FT})
practical secrecy – H(M|K, CH_{FT})≥α
Provision of confidentiality
6
Key K, original text M – protected channel, flawed texts (CFT/CHFT) and damage (CHD/CHD) – open channel
perfect secrecy – H(K) = H(M|$CH_{FT}CH_D$)
practical secrecy – H(K|$CH_{FT}CH_D$)≥α
7
Key K, flawed texts (CFT/CH_{FT}) – protected channel, original text M, damage (CHD/CH_D) – open channel
perfect secrecy – H(K) = H(K|M, CH_D)
practical secrecy – H(K)=H(K|M, CH_D)≥α
If it is required to find CH_{FT}
perfect secrecy – H(CH_{FT}) = H(H_{FT}|M, CH_D)
practical secrecy – H(Y_{DT}|Y_D)≥α
8
flawed texts (CFT/CH_{FT}), original text M – protected channel, key K, damage (CHD/CH_D) – open channel
perfect secrecy – H(M) = H(M|K, CH_D)
practical secrecy – H(M|K, CH_D)≥α
If it is required to find CH_{FT}
perfect secrecy – H(CH_{FT}) = H(CH_{FT}|K, CH_D)
practical secrecy – H(CH_{FT}|K, CH_D)≥α
9
Key K, damage (CHD/H_D) – protected channel, flawed texts (CFT/CH_{FT}), original text M – open channel
perfect secrecy – H(CH_D) = H(CH_D|M, CH_{FT})
practical secrecy – H(CH_D|M, CH_{FT})≥α
original text M, damage (CHD/CH_D) – protected channel, key K, flawed texts (CFT/CH_{FT}) – open channel
perfect secrecy – H(M) = H(M|K, CH_{FT}), practical secrecy – H(M|K, CH_{FT})≥α
If it is required to find CH $_D$
perfect secrecy – H(CH_D) = H(CH_D|K, CH_{FT})
practical secrecy – H(CH_D|K, CFT/CH_{FT})≥α
Provision of authenticity
CFT – flawed text
CHD – damage
FTC/ FT_{CH} – flawed ciphertext
DCH/D_{CH} – damage of ciphertext
CH_{FT} – ciphertext of flawed text
CH_D – ciphertext of damage
FT_{CH} – flawed ciphertext
D_{CH} – damage of ciphertext

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

$$N_S = H(K)\frac{2^{HL}}{|I|^L} = 1;$$

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B\log|I|}, \qquad (1)$$

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*|>2, 2^{HL} 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 $x_i \in \{0,1\}^n$ with probabilities p_i and $T = (c, f) \in F_n^r$ is the arbitrary fixed transformation *MV*2. Then for any $y \in U_{r\,n-1}$ (a certain binary line from a set of variable-length strings) and for any $1 \le i \le |y|$, the following holds:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} =$$
$$= \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}.$$

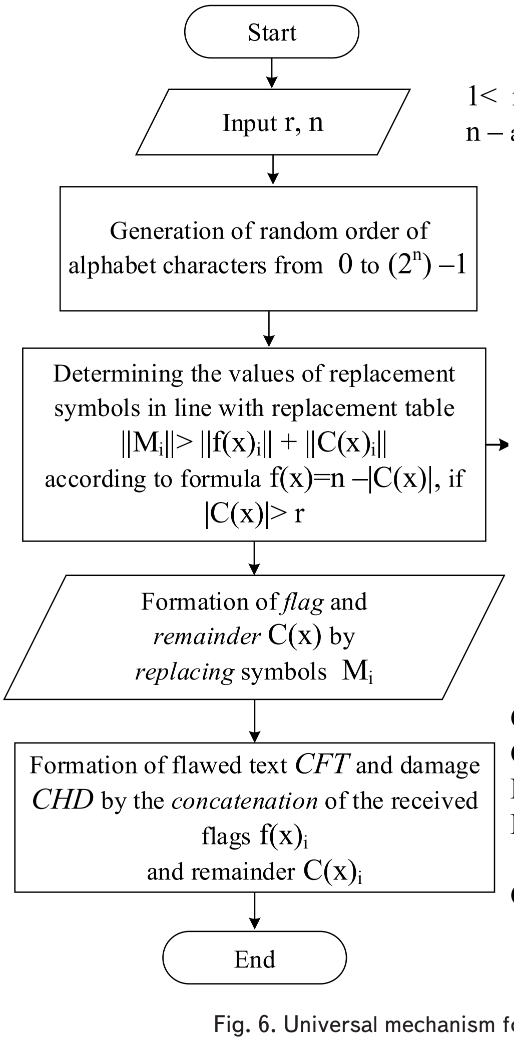
Then, regardless of the probability distribution of random element *X*, for the entropies of random elements *FTC/ FT_{CH}* (flawed ciphertext) and *CHD* (damage), the following equalities hold:

$$H(FTC / FT_{CH}) \le \log(2^n - 2^r),$$

$$H(CHD) \le \log(n - r + 1).$$

Thus, under uniform distribution of inputs (flags) of the algorithm *MV*2, a uniform distribution of the output (remainder) forms:

$$P(c_k = 0 \,|\, 0 \le k \le |FTC / FT_{CH}|) = \frac{1}{2}.$$


Start
Input r, n
Generation of random order of alphabet characters from 0 to (2^n) –1
Determining the values of replacement symbols in line with replacement table ||M_i||> ||f(x)_i|| + ||C(x)_i|| according to formula f(x)=n –|C(x)|, if |C(x)|> r
Formation of *flag* and *remainder* C(x) by *replacing* symbols M_i
Formation of flawed text *CFT* and damage *CHD* by the *concatenation* of the received flags f(x)_i and remainder C(x)_i
End

1< r < n – positive integer
n – alphabet power

Symbol	Length of remainder	Remainder C(x)	Flag f(x)
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	r+1	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	n – 2	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	n – 1	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	n – 1	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

CFT/ CH_{FT} – ciphertext of flawed text
CHD/CH_D – ciphertext of damage
FTC/ FT_{CH} – damaged ciphertext
DCH/D_{CH} – damage to ciphertext
f(x) – flag (damage)
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:

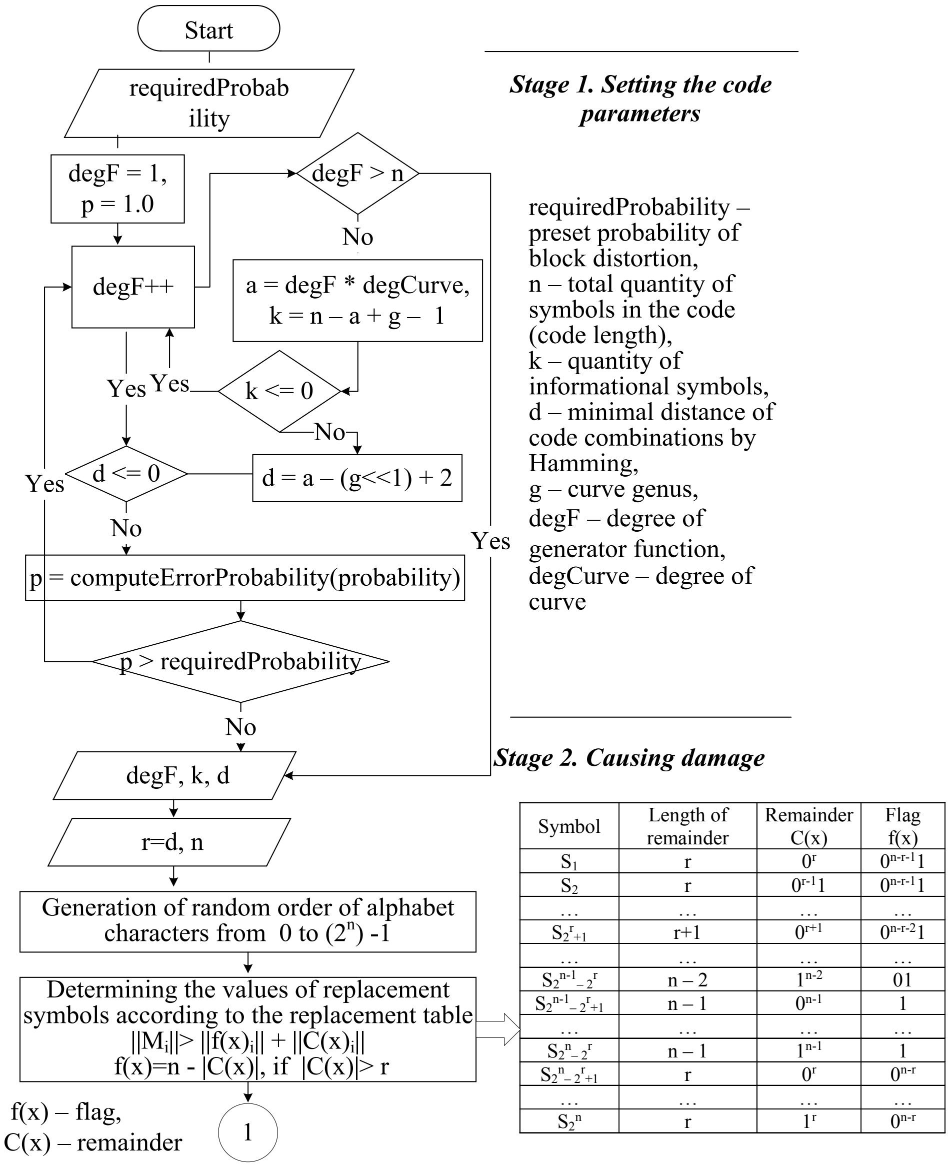
$$U_0 = \frac{\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H(KU_i^{EC})}{B\log|I|}. \qquad (2)$$

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.


Start
requiredProbability
degF = 1,
p = 1.0
degF > n
degF++
No
a = degF * degCurve,
k = n – a + g – 1
Yes
Yes
k <= 0
No
Yes
d <= 0
d = a – (g<<1) + 2
No
Yes
p = computeErrorProbability(probability)
p > requiredProbability
No
degF, k, d
r=d, n
Generation of random order of alphabet characters from 0 to (2^n) -1
Determining the values of replacement symbols according to the replacement table
||M_i||> ||f(x)_i|| + ||C(x)_i||
f(x)=n - |C(x)|, if |C(x)|> r
f(x) – flag,
C(x) – remainder
1
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

Symbol	Length of remainder	Remainder C(x)	Flag f(x)
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	r+1	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	n – 2	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	n – 1	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	n – 1	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

Fig. 7. Stages 1, 2 of the formation of a cryptogram in a hybrid cryptosystem based on the McEliece MACCS with flawed codes

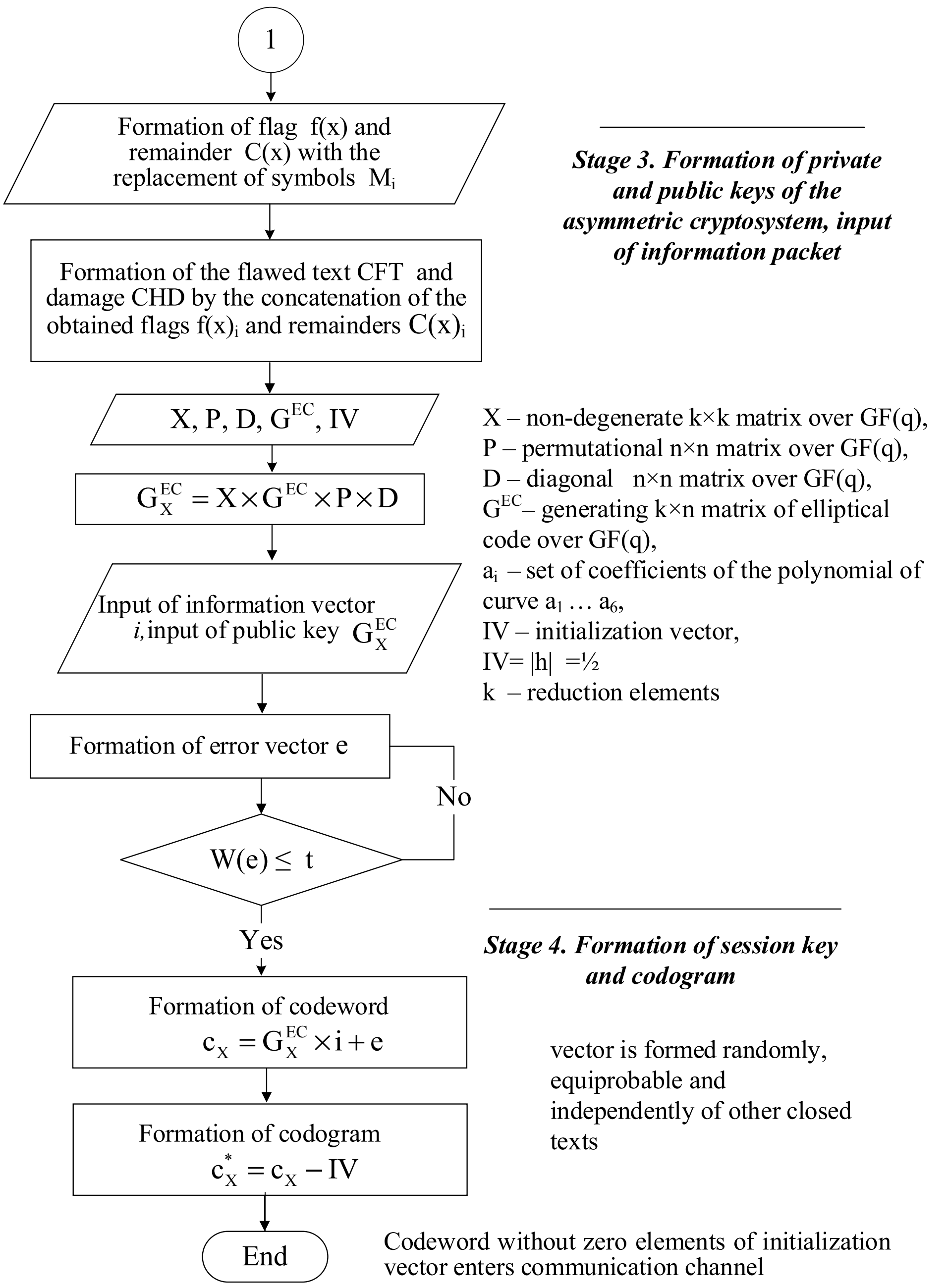

1
Formation of flag f(x) and remainder C(x) with the replacement of symbols M_i
Stage 3. Formation of private and public keys of the asymmetric cryptosystem, input of information packet
Formation of the flawed text CFT and damage CHD by the concatenation of the obtained flags $f(x)_i$ and remainders $C(x)_i$
X, P, D, G^{EC}, IV
$G_X^{EC}=X\times G^{EC}\times P\times D$
X – non-degenerate k×k matrix over GF(q),
P – permutational n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
G^{EC}– generating k×n matrix of elliptical code over GF(q),
a_i – set of coefficients of the polynomial of curve $a_1 \dots a_6$,
IV – initialization vector,
IV= |h| =½
k – reduction elements
Input of information vector *i*, input of public key G_X^{EC}
Formation of error vector e
No
$W(e)\le t$
Yes
Stage 4. Formation of session key and codogram
Formation of codeword $c_X=G_X^{EC}\times i+e$
vector is formed randomly, equiprobable and independently of other closed texts
Formation of codogram $c_X^*=c_X-IV$
End
Codeword without zero elements of initialization vector enters communication channel

Fig. 8. Stages 3, 4 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.

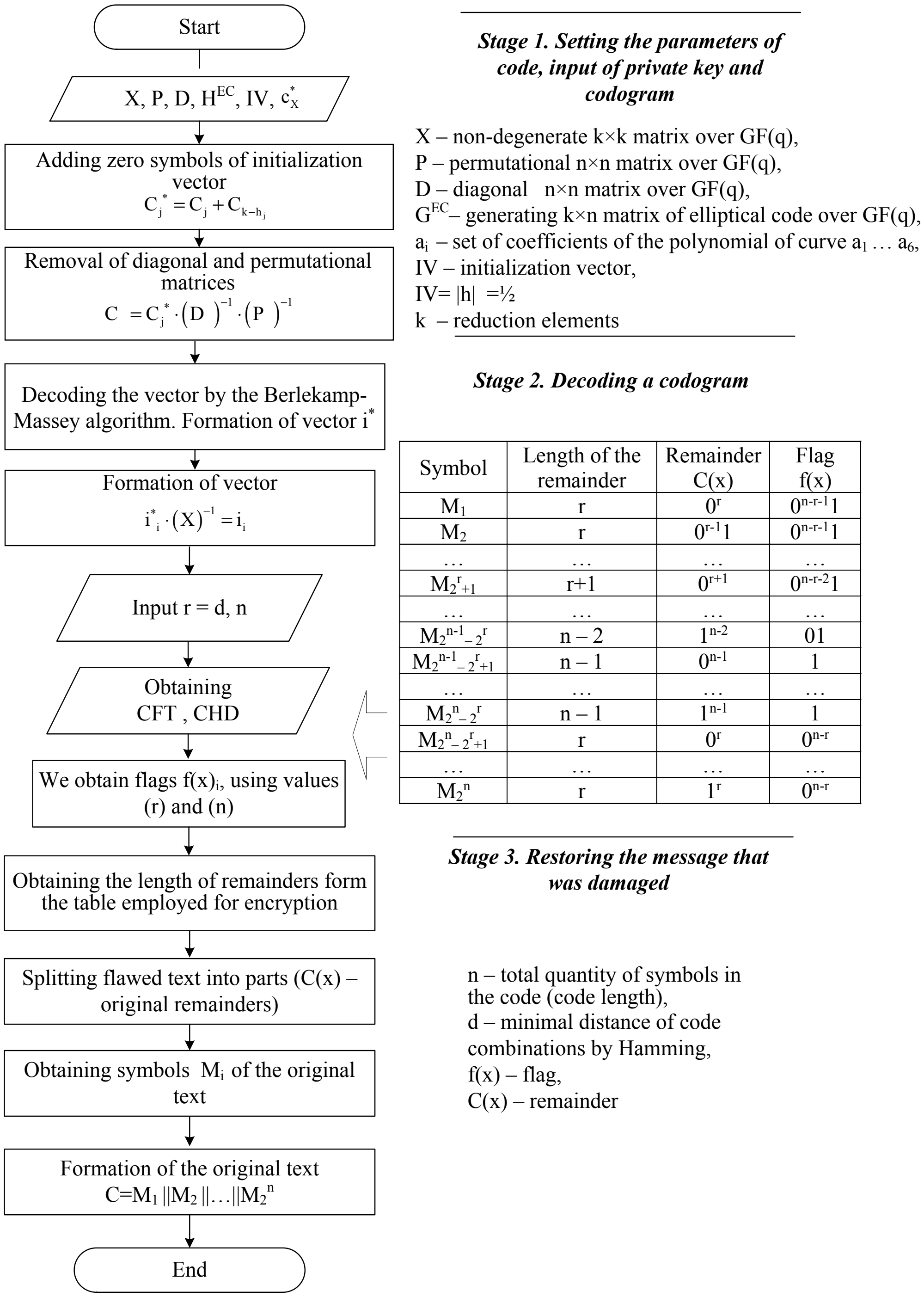
The algorithms proposed for the hybrid cryptosystem make it possible, when hiding the flawed ciphertext *CFT/* CH_{FT}, to improve entropy of the public key:

$$U_0=\frac{H(CFT/CH_{FT})+\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right)+H(KU_i^{EC})}{B\log|I|},\qquad(3)$$

In the case of additional hiding of the last ciphertext of damage CHD/CH_D due to its smallness and proportionality with the flawed text ciphertext CFT/CH_{FT}, the distance of singularity can be further extended:

$$U_0=\frac{H(CHD/CH_D)+H(CFT/CH_{FT})+\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right)+H(KU_i^{EC})}{B\log|I|}.\qquad(4)$$

Thus, a multichannel cryptography based on flawed codes makes it possible to integrate cryptographic systems, combining within the framework of one concept the crypto-code 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.


Start
X, P, D, H^EC, IV, c*_X
Adding zero symbols of initialization vector
$C_j^* = C_j + C_{k-h_j}$
Removal of diagonal and permutational matrices
$C = C_j^* \cdot (D)^{-1} \cdot (P)^{-1}$
Decoding the vector by the Berlekamp-Massey algorithm. Formation of vector i*
Formation of vector
$i^*_i \cdot (X)^{-1} = i_i$
Input r = d, n
Obtaining CFT , CHD
We obtain flags f(x)_i, using values (r) and (n)
Obtaining the length of remainders form the table employed for encryption
Splitting flawed text into parts (C(x) – original remainders)
Obtaining symbols M_i of the original text
Formation of the original text C=M_1 ||M_2 ||…||M_2^n
End
Stage 1. Setting the parameters of code, input of private key and codogram
X – non-degenerate k×k matrix over GF(q),
P – permutational n×n matrix over GF(q),
D – diagonal n×n matrix over GF(q),
G^EC– generating k×n matrix of elliptical code over GF(q),
a_i – set of coefficients of the polynomial of curve a_1 … a_6,
IV – initialization vector,
IV= |h| =½
k – reduction elements
Stage 2. Decoding a codogram
Stage 3. Restoring the message that was damaged
n – total quantity of symbols in the code (code length),
d – minimal distance of code combinations by Hamming,
f(x) – flag,
C(x) – remainder

Symbol	Length of the remainder	Remainder C(x)	Flag f(x)
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
M_{2^r+1}	r+1	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_{2^{n-1}-2^r}$	n – 2	1^{n-2}	01
$M_{2^{n-1}-2^r+1}$	n – 1	0^{n-1}	1
…	…	…	…
$M_{2^n-2^r}$	n – 1	1^{n-1}	1
$M_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
M_{2^n}	r	1^r	0^{n-r}

Fig. 9. Decryption in a hybrid cryptosystem based on the McEliece MACCS

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 *MV*2 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 *MV*2 improves crypto resistance of the system, it makes it possible to "reduce" the alphabet power (dimensionality 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

$$Per = Utl * CPU\_clock / Rate,$$

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

Code sequence length		McEliece on truncated codes			McEliece		
		10	100	1000	10	100	1000
Number of calls for functions that implement basic operations	Symbol readout	10 294 397	28 750 457	76 759 874	11 018 042	30 800 328	80 859 933
	String comparison	3 406 921	9 246 748	25 478 498	3 663 356	10 199 898	26 364 634
	String concatenation	1 705 544	5 045 748	12 379 422	1 834 983	5 125 564	13 415 329
Total		15 406 862	43 042 953	114 617 794	16 516 381	46 125 790	120 639 896
Duration of function* realization in processor cycles	Symbol readout	295374	810478	2 001 167	297 487	831 609	2 183 218
	String comparison	178 814	531 379	1 248 684	197 821	550 794	1 423 690
	String concatenation	544 990	1 328 114	3 586 486	544 990	1 522 293	3 984 353
Total		1 006 781	2 749 548	7 247 488	1 040 298	2 904 696	7 591 261
Implementation duration**, msec		0.52	1.37	3.4	0.55	1.53	4

*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

Code sequence length		*MV2*		
		10	100	1000
Number of calls for functions that implement basic operations	Summing	3942	28673	275499
	Difference	1794	3810	23881
	Division	3274	4804	20104
	Multiplication	19	109	1009
	Comparison	8939	60963	578784
Total		17968	98359	899277
Duration of function* realization in milliseconds	Summing	19.53	93.58	2297.36
	Difference	8.89	12.43	199.14
	Division	16.22	15.68	167.65
	Multiplication	0.09	0.36	8.41
	Comparison	44.28	198.96	4826.43
Total		89	321	7499
Duration of implementation** in milliseconds		89	321	7499

*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 5

Research results of the estimation of temporal and speed parameters of the procedures to form and decode information

Parameters	Code sequence length	Algorithm throughput, Rate (byte/sec)	Processor core utilization (%)	Algorithm complexity, per (cpb)
Number of calls for functions that implement basic operations	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0

Table 6 gives research results of the estimation of temporal and speed parameters of the procedures to cause and eliminate damage.

Table 6

Research results of the estimation of temporal and speed parameters of the procedures to cause and eliminate damage

Parameters	Code sequence length	Work-time (sec)	Algorithm throughput, Rate (byte/sec)	Processor core utilization (cycles)	Algorithm complexity, per (cpb)
Number of calls for functions that implement basic operations	10	0.089	112.3596	90	0.801
	100	0.321	311.5265	322	1.034
	1000	7.499	133.3511	7500	66.166

An analysis we conducted based on Tables 3–6 allows us to draw a conclusion about significant energy costs when implementing the asymmetric crypto-code systems in the protocols of communication systems and technologies, which makes their use extremely problematic. In order to eliminate the shortcoming, it is proposed to use MCCS that reduces energy costs and volumes of key data from the users. The formation of hybrid cryptosystems based on the McEliece MACCS on flawed codes makes it possible to reduce the alphabet power (*GF* (2^6–2^8) without compromising the level of crypto resistance through the use of multichannel cryptography systems on flawed codes. Procedures that employ the algorithm of causing damage *MV*2 practically do not affect encryption speed in the McEliece MACCS. Thus, the proposed hybrid cryptosystem makes it possible to encrypt large quantities of data utilized in IES without bringing down performance, while ensuring the required level of quality service for the CES users.

Estimation of crypto resistance of the proposed hybrid cryptosystem.

In order to compute quantity of information, in article [32], authors suggested using a probability function of entropy (the amount of information as a confidence measure of the transmitted signal is measured in bits), borrowed from statistical thermodynamics. A function is used for this purpose that is reminiscent of the entropy function introduced to physics by Ludwig Boltzmann. Various techniques for assessing the quantity of information have been developed until now. In computing engineering, the approach proposed in paper [32] has been employed in the vast majority of cases.

Assume that we have a source of messages M, which can be in one of the states m_i (i=1÷n) with a probability p_i. The sum of probabilities is (p_1+p_2+ ...+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]:

$$H(p_1, p_2, ..., p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i. \quad (5)$$

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

$$H = \log_2 n, \quad (6)$$

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:

$$\{M_i\} \to \{C_i\}. \quad (7)$$

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: p_i=n_i/N. Next, by calculating the sum:

$$H_M(p_1, p_2, ..., p_m) = -\sum_{i=1}^{m} p_i \log_2 p_i, \quad (8)$$

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 unities). It is clear that the entropy of such ciphertext should be maximal.

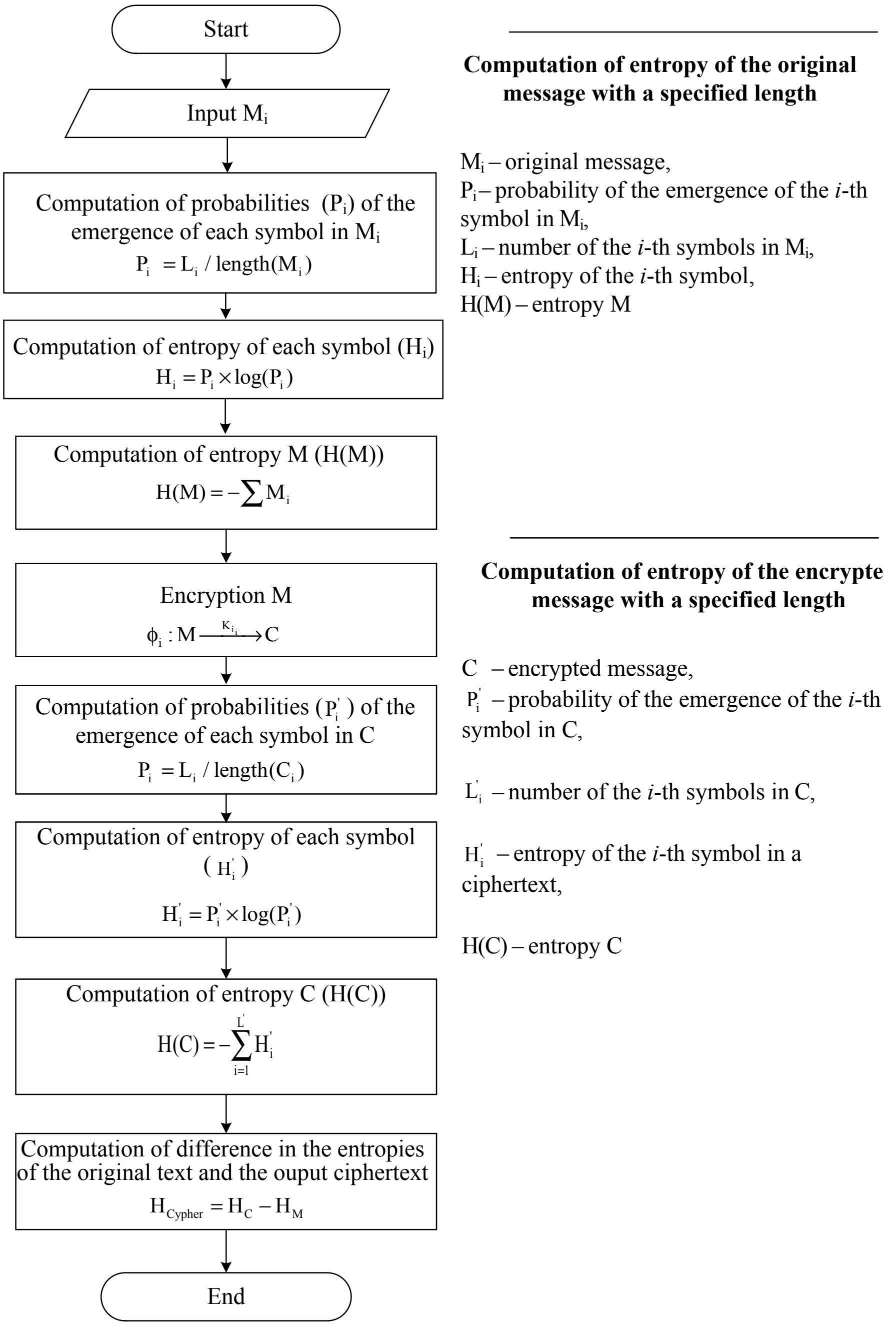

Start
Input M_i
Computation of probabilities (P_i) of the emergence of each symbol in M_i
$P_i = L_i / \text{length}(M_i)$
Computation of entropy of each symbol (H_i)
$H_i = P_i \times \log(P_i)$
Computation of entropy M (H(M))
$H(M) = -\sum M_i$
Encryption M
$\phi_i : M \xrightarrow{K_{i_i}} C$
Computation of probabilities ($P_i^{'}$) of the emergence of each symbol in C
$P_i = L_i / \text{length}(C_i)$
Computation of entropy of each symbol ($H_i^{'}$)
$H_i^{'} = P_i^{'} \times \log(P_i^{'})$
Computation of entropy C (H(C))
$H(C) = -\sum_{i=1}^{L^{'}} H_i^{'}$
Computation of difference in the entropies of the original text and the ouput ciphertext
$H_{Cypher} = H_C - H_M$
End
Computation of entropy of the original message with a specified length
M_i – original message,
P_i – probability of the emergence of the *i*-th symbol in M_i,
L_i – number of the *i*-th symbols in M_i,
H_i – entropy of the *i*-th symbol,
H(M) – entropy M
Computation of entropy of the encrypted message with a specified length
C – encrypted message,
$P_i^{'}$ – probability of the emergence of the *i*-th symbol in C,
$L_i^{'}$ – number of the *i*-th symbols in C,
$H_i^{'}$ – entropy of the *i*-th symbol in a ciphertext,
H(C) – entropy C

Fig. 10. Algorithm for testing a hybrid cryptosystem in terms of resistance based on the entropy randomness assessment method

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:

$$H_C(p_1, p_2, ..., p_m) = -\sum_{i=1}^{m} p_i \log_2 p_i. \qquad (9)$$

6. Difference

$$H_C - H_M = H_{Cypher}. \qquad (10)$$

For the systems on flawed codes:

$$d = H(CFT / CH_{FT}) - H(M_i). \qquad (11)$$

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*-trasformation:

$$H_{Cypher} = H_K + H_{S-box} + H_{MV2}. \qquad (12)$$

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:

$$H_C - \log_2 n, \qquad (13)$$

the less resistant is the examined crypto algorithm.

Thus, the basic steps in the procedure for the estimation of crypto stability based on the 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 $GF(2^{13})$. 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 $MV2$ 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 $GF(2^6–2^8)$ 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

1. Uskov, A. V. Tekhnologyi obespecheniya informatsionnoy bezopasnosti korporativnyh obrazovatel'nyh setey [Text] / A. V. Uskov, A. D. Ivannikov, V. L. Uskov // Educational Technology & Society. – 2008. – Issue 11 (1). – P. 472–479.
2. Gruzdeva, L. M. Povyshenie proizvoditel'nosti korporativnoy seti v usloviyah vozdeystviya ugroz informatsionnoy bezopasnosti [Text] / L. M. Gruzdeva, M. Yu. Monahov // Izvestiya vysshih uchebnyh zavedeniy. Priborostroenie. – 2012. – Vol. 55, Issue 8. – P. 53–56.
3. Anikin, I. V. Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnyh informatsionnyh setyah [Text] / I. V. Anikin, L. Yu. Emaletdinova, A. P. Kirpichnikov // Vestnik tekhnologicheskogo universiteta. – 2015. – Vol. 18, Issue 6. – P. 195–197.
4. Nadezhdin, E. N. Problemnye voprosy upravleniya riskami informatsionnoy bezopasnosti v sfere obrazovaniya [Text] / E. N. Nadezhdin // Nauchnyy poisk. – 2012. – Issue 2.6. – P. 50–56.
5. Kondratova, E. G. Sotsial'nye seti kak kanal utechki korporativnoy informatsyi [Text] / E. G. Kondratova // Bezopasnost' informatsionnyh tekhnologiy. – 2013. – Issue 1. – P. 107–108.
6. Litvinov, V. A. Informatsionnaya bezopasnost' vysshego uchebnogo zavedeniya v ramkah sovremennoy globalizatsyi [Electronic resource] / V. A. Litvinov, E. V. Lypko, A. A. Yakovleva // Kontent-platforma Pandia. – Available at: http://pandia.ru/text/80/257/33657.php
7. Vahonin, S. Udalennyy dostup i utechka dannyh [Text] / S. Vahonin // Informatsionnaya bezopasnost'. – 2014. – Issue 5. – Available at: http://www.itsec.ru/articles2/Inf_security/udalennyy-dostup-i-utechka-dannyh/
8. Zamaraeva, O. A. Razrabotka politiki informatsionnoy bezopasnosti dlya ekonomicheskogo vuza: opredelenie informatsyi, podlezhashchey zashchite, i postroenie modeli zloumyshlennika [Text] / O. A. Zamaraeva, V. A. Titov, D. O. Kuzin // Sovremennye problemy nauki i obrazovaniya. – 2014. – Issue 3. – Available at: https://www.science-education.ru/ru/article/view?id=13106
9. Evseev, S. P. Modelirovanie protsessov upravleniya v informatsionnoy ekonomike [Text] / S. P. Evseev. – Berdyansk, 2017. – 420 p.

10. Hryshchuk, R. V. Teoretychni osnovy modeliuvannia protsesiv napadu na informatsyiu metodamy teoryi dyferentsialnykh ihor ta dyferentsialnykh peretvoren [Text]: monohrafiya / R. V. Hryshchuk. – Zhytomyr: Ruta, 2010. – 280 p.
11. Hryshchuk, R. V. Osnovy kibernetychnoi bezpeky [Text]: monohrafiya / R. V. Hryshchuk, Yu. H. Danyk; Yu. H. Dannyk (Ed.). – Zhytomyr: ZhNAEU, 2016. – 636 p.
12. Ojha, D. B. Transmission of Picturesque content with Code Base Cryptosystem [Text] / D. B. Ojha, A. Sharma, A. Dwivedi, B. Kumar, A. Kumar // International Journal of Computer Technology and Applications. – 2011. – Vol. 02, Issue 01. – P. 127–131.
13. Salman, A. G. Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Text] / A. G. Salman // Journal of Computer Science. – 2014. – Vol. 10, Issue 7. – P. 1249–1252. doi: 10.3844/jcssp.2014.1249.1252
14. Ojha, D. B. Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Text] / D. B. Ojha, A. Sharma, A. D. N. Pandey, A. Kumar // International Journal of Engineering Science and Technology. – 2010. – Vol. 2, Issue 12. – P. 7112–7117.
15. Ojha, D. B. An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Text] / D. B. Ojha, A. Sharma // International Journal of Advanced Networking and Applications. – 2011. – Vol. 2, Issue 5. – P. 841–845.
16. Jeeva, Y. C. A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management [Text] / Y. C. Jeeva // Journal of Computer Science. – 2013. – Vol. 9, Issue 11. – P. 1556–1565. doi: 10.3844/jcssp.2013.1556.1565
17. Yevseiev, S. Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes [Text] / S. Yevseiev, K. Rzayev, O. Korol, Z. Imanova // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 4, Issue 9 (82). – P. 18–26. doi: 10.15587/1729-4061.2016.75250
18. Hamdi, O. On the Usage of Chained Codes in Cryptography [Text] / O. Hamdi // International Journal of Computer Science and Security. – 2010. – Vol. 3, Issue 6. – P. 482–490.
19. Evseev, S. P. Usovershenstvovanie metoda dvuhfaktornoy autentifikatsyi na osnove ispol'zovaniya modifitsirovannyh kripto-kodovyh skhem [Text] / S. P. Evseev, V. G. Abdullaev, Zh. F. Agazade, V. S. Abbasova // Systemy obrobky informatsyi. – 2016. – Issue 9 (146). – P. 132–144.
20. Yevseiev, S. Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system [Text] / S. Yevseiev, K. Hryhorii, Y. Liekariev // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 6, Issue 4 (84). – P. 11–23. doi: 10.15587/1729-4061.2016.86175
21. Rzaev, H. N. Matematicheskie modeli kripto-kodovyh sredstv zashchity informatsii na osnove TKS [Text] / H. N. Rzaev, G. G. Iskenderzade, F. G. Samedov, Z. B. Imanova, Zh. S. Dzhamalova // Zashchita informatsyi. – 2016. – Issue 23. – P. 24–26.
22. McEliece, R. J. A Public-Key Criptosystem Based on Algebraic Theory [Text] / R. J. McEliece // DGN Progres Report 42-44. – Pasadena, C.A., 1978. – P. 114–116.
23. Niederreiter, H. Knapsack-Type Cryptosystems and Algebraic Coding Theory [Text] / H. Niederreiter // Problems of Control and Information Theory. – 1986. – Vol. 15, Issue 2. – P. 159–166.
24. Bleyhut, R. Teoriya i praktika kodov, kontroliruyushchih oshibki [Text] / R. Bleyhut. – Moscow: Mir, 1986. – 576 p.
25. Klark, Dzh.-ml. Kodirovanie s ispravleniem oshibok v sistemah tsifrovoy svyazi [Text] / Dzh.-ml. Klark; B. S. Tsybakov (Ed.). – Moscow: Radio i svyaz', 1987. – 392 p.
26. Mak-Vil'yams, F. Dzh. Teoriya kodov, ispravlyayushchih oshibki [Text] / F. Dzh. Mak-Vil'yams, N. Dzh. A. Sloen. – Moscow: Svyaz', 1979. – 744 p.
27. Muter, V. M. Osnovy pomekhoustoychivoy teleperedachi informatsyi [Text] / V. M. Muter. – Leningrad: Energoatomizdat, 1990. – 288 p.
28. Kasami, T. Teoriya kodirovaniya [Text] / T. Kasami, N. Tokura, E. Ivadari, Ya. Inagaki; B. S. Tsybakov, S. I. Gel'fand (Eds.). – Moscow: Mir, 1978. – 576 p.
29. Sidel'nikov, V. M. Kriptografiya i teoriya kodirovaniya [Text]: konferentsiya / V. M. Sidel'nikov // Moskovskiy universitet i razvitie kriptografii v Rossyi. – Moscow, 2002. – 22 p.
30. Mishchenko, V. A. Ushcherbnye teksty i mnogokanal'naya kriptografiya [Text] / V. A. Mishchenko, Yu. V. Vilanskiy. – Minsk: Entsiklopediks, 2007. – 292 p.
31. Mishchenko, V. A. Kriptograficheskiy algoritm MV 2 [Text] / V. A. Mishchenko, Yu. V. Vilanskiy, V. V. Lepin. – Minsk, 2006. – 177 p.
32. Shennon, K. Teoriya svyazi v sekretnyh sistemah [Text] / K. Shennon // Raboty po teoryi informatsyi i kibernetike. – Moscow, 1963. – P. 333–369.