OTP-технології (Technology of One-Time Passwords) дозволять зменшити ризики, з якими стикаються IT-фахівці ІОС при використанні довгострокових паролів. Аналізуються способи формування OTP-паролів, основні загрози використання. Розглянуто математичні моделі побудови протоколу багатофакторної аутентифікації на основі гібридних крипто-кодових конструкцій на збиткових кодах (ГККККУК), запропоновані практичні алгоритми їх реалізації

Ключові слова: багатофакторна аутентифікація, гібридні крипто-кодові конструкції на збиткових кодах, одноразові паролі

OTP-технологии (Technology of One-Time Passwords) позволят уменьшить риски, с которыми сталкиваются IT-специалисты ИВС при использовании долгосрочных паролей. Анализируются способы формирования OTP-паролей, основные угрозы использования. Рассмотрены математические модели построения протокола многофакторной аутентификации на основе гибридных крипто-кодовых конструкций на ущербных кодах (ГККККУК), предложены практические алгоритмы их реализации

Ключевые слова: многофакторная аутентификация, гибридные крипто-кодовые конструкции на убыточных кодах, одноразовые пароли

UDC 621.391
DOI: 10.15587/1729-4061.2017.109879

THE DEVELOPMENT OF THE METHOD OF MULTIFACTOR AUTHENTICATION BASED ON HYBRID CRYPTO-CODE CONSTRUCTIONS ON DEFECTIVE CODES

S. Yevseiev
PhD, Associate Professor, Senior Researcher*
E-mail: serhii.yevseiev@m.hneu.edu.ua
H. Kots
PhD, Associate Professor*
E-mail: dekanstei@gmail.com
S. Minukhin
Doctor of Technical Sciences, Professor*
E-mail: minukhin.sv@gmail.com
O. Korol
PhD, Associate Professor*
E-mail: olha.korol@m.hneu.edu.ua
A. Kholodkova
PhD, Associate Professor*
E-mail: anny.kholodkova@gmail.com
*Department of Information Systems
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

1. Introduction

The development of information education networks (IEN) is closely connected with the task of ensuring the security of the network facing IT. The solution is formed of many components, one of them is secure authentication. OTP technologies (Technology of One-Time Passwords) will reduce the risks faced by IT specialists of IEN when using long-term passwords.

The further development of corporate educational systems based on the informatization of services and the use of remote access to network resources puts forward new requirements for ensuring security (integrity, confidentiality, accessibility and authenticity) when receiving educational services. To ensure authenticity, IEN (CES) commonly uses an electronic digital signature, based on multi-factor or enhanced authentication. It is based on the joint use of several factors of authentication (knowledge, means or objects of storage of one of the information components of a legitimate authentication procedure). This approach significantly increases the security of information usage, at least on the part of users connecting to information systems over secure and unprotected communication channels. Among methods of multi-factor authentication, a method based on SMS authentication has become widely used. However, its use carries significant security risks and it is needed to use other, more secure methods, such as Time-based One-Time Password Algorithm (TOTP) with additional cryptographic protection.

2. Literature review and problem statement

Modern universities, as objects of informatization, have a number of features: a diversified nature of activities, the presence of spatial infrastructure (branches, representative offices), the diversity of forms and methods of teaching. Adaptation to the constantly changing conditions of the educational market, electronic interaction with legal organizations, periodic change in the status of teachers and students lead to the need to consider corporate educational systems (CES) as management systems with critical cybernetic infrastructure [1, 2].

Information (corporate) education systems are increasingly using the global Internet (GI) and its main portal –

cellular communication for the provision of educational services, electronic document management and administrative functions. One of the main components of security in the use of various technologies and gadgets is electronic authentication (EA) – a procedure that confirms the authenticity of the source of the message. The main mechanisms for electronic authentication are mechanisms based on symmetric and asymmetric encryption, electronic digital signatures (in the mechanisms of PKI technologies (X.509 standard), IPSec, PGP, S/MIME certificates), MDC and MAC code generation procedures [5–7]. In [8], basic requirements to the architecture and mechanisms of safety in cellular technology of the fourth generation (4G, *Long Term Evolution* (LTE)) are considered, the security basis of which are the mechanisms of protection in the stack of TCP/IP and MAC codes. In the standard [11], derivatives of the SHA-3 (*Keccak*) algorithm for the formation of MAC codes based on SHAKE, KMAC, Tuple Hash and Parallel Hash derived algorithms, each of which is defined for the 128-bit and 256-bit MAC code sequence are proposed.

A special place among the mechanisms of EA is occupied by two-factor authentication methods based on various smart cards, USB keys, OTP passwords [9, 10, 12–14]. Multi-factor authentication methods have become widespread among hi-tech organizations, financial and insurance sectors of the market, large banking institutions, and public sector enterprises. The trends of consumerization in IEN lead to the fact that users need to use different types of devices to access resources of the corporate educational network – a fixed or mobile computer, tablet or smartphone is used [9, 10]. One-time password technology (OTP) can help implement a strong two-factor authentication and will not require significant implementation and support costs [9]. OTP is virtually invulnerable to attacking network packet analysis and additionally requires the user to enter a PIN, which is an additional factor of authentication [9]. Thus, two-factor authentication of the user in the system is formed on the basis of owning something (Authentication by Ownership) or on the basis of knowledge of something (Authentication by Knowledge) [9].

The downside of using OTP passwords is that an attacker can "intercept" the text (SMS) with one part of the token. Attackers can compromise two-factor authentication based on social engineering methods (message forwarding through the provider) [3, 4] by means of the *International Mobile Subscriber Identity* (IMSI), using communication protocol weaknesses [15, 16].

For this reason, the National Institute of Standards and Technology (NIST) in [6] is going to prohibit the use of two-factor authentication codes based on OTP passwords for services that connect to public IT systems. Thus, there is a contradiction between the use of OTP passwords in the protocols of two-factor authentication and provision of security in the transfer of its individual factors.

3. The aim and objectives of the study

The aim is to develop an improved method of strict two-factor authentication with OTP password based on hybrid crypto-code systems on flawed codes that allows the further use of 2 FA based on SMS, and to construct mathematical models and practical algorithms for implementing McEliece and Niederreiter modified asymmetric crypto-code systems on flawed codes.

To achieve the aim, let us consider the following objectives:

– to analyze the main methods of forming OTP passwords, the main threats to use;

– to describe the mathematical models of hybrid crypto-code systems on flawed codes, based on McEliece and Niederreiter modified asymmetric crypto-code systems (MACCS) on elliptic codes;

– to develop practical algorithms for data encryption and decryption in Niederreiter-McEliece hybrid crypto-code systems on flawed codes (HCCSFC).

4. Analysis of the main methods of construction of OTP passwords

Authentication based on electronic (digital) authentication establishes that the subject is actually, what he calls himself. Digital authentication is the process of determining the authenticity of one or more authenticators used to obtain a digital identity. Authentication establishes that a subject attempting to access a digital service monitors the technologies used for authentication. For services that use return visits, successful authentication provides reasonable risk-based guarantees that the entity accessing the service today is the same as the one who previously accessed the service [6, 9, 10].

Two-factor authentication or 2FA is a method of identifying a user in a service where two different types of authentication data are used. The introduction of an additional level of security provides more effective protection of your account from unauthorized access. Using this type of 2FA, the user enters a personal password on the first level of authentication. The next step is to enter the One-time Password Algorithm (*OTP*), usually sent via SMS to the mobile device. OTP will be available only to those who, as expected in theory, have entered an inaccessible password [13, 14]. The following *Authenticator Assurance Levels* (*AALs*) are [6], presented in Fig. 1.

The analysis of requirements [6, 17–21] to the methods of forming OTP passwords showed that:

– *memorable secret authenticator* – commonly called a *password* or, if numeric, *PIN* is a secret value intended for selection and memorization by the user, it must consist of 8 characters, be difficult enough to memorize and kept secret. For the formation of a secret authenticator, it is proposed to use the algorithms for generating MAC codes: HMAC [FIPS 198-1], SHA-3 [FIPS 202], CMAC [SP 800-38B] or Kecacak Message Authentication Code (KMAC), configurable SHAKE (cSHAKE) or ParallelHash [SP 800-185];

– *secret authenticators Look-Up* – is a physical or electronic record that stores a set of secrets shared between the applicant and the CSP (*Center for Security Policy*). To create a list of secrets, a standardized random bit generator [SP 800-90Ar1] is used [21];

– *out-of-band authenticator* – a physical device that is uniquely addressed and can safely communicate with the verifier through a separate communication channel, called a secondary channel. The device is owned and controlled by the applicant and supports private communication on this secondary channel, separately from the primary channel for electronic authentication. For the formation of the secondary channel, public switched networks (*4G LTE*) can be used. The authenticator is transmitted in encrypted form [8];

– *single-factor OTP device* generates an OTP. This category includes hardware devices and OTP software generators installed on mobile gadgets. These devices have a built-in secret that is used as a key for generating OTP and does not require activation through a second factor. Symmetric and asymmetric cryptoalgorithms are used to generate the key. OTP is displayed on the device and entered manually for transfer to the verifier, thereby proving the ownership and management of the device;

– *multi-factor device OTP* generates an OTP for use in authentication after activation with an additional authenticator. The device uses hardware devices and OTP software generators based on symmetric cryptoalgorithms, or hashing functions, installed on mobile gadgets. The second authentication factor can be achieved with the help of some built-in input pad, an integrated biometric reader (for example, a fingerprint) or a direct computer interface (for example, a USB port). OTP is displayed on the device and entered manually for transmission to the verifier;

– *single-factor cryptographic software authenticator* is a cryptographic key stored on a disk or some other "soft" medium. Single-factor cryptographic software authenticators encapsulate a private key that is unique to the authenticator. Authentication is carried out by checking the ownership and control of the key;

– *single-factor cryptographic device* is a hardware device that performs cryptographic operations using a secure cryptographic key and provides an authenticator output through a direct connection to the user endpoint. The device uses built-in symmetric or asymmetric cryptographic keys and does not require activation through a second authentication factor. Authentication is performed by checking the ownership of the device using the authentication protocol;

– *multi-factor cryptographic software authenticator* – a cryptographic key stored on a disk or some other "soft" medium that requires activation through a second authentication factor. Authentication is carried out by checking the ownership and control of the key;

– *multi-factor cryptographic device* – a hardware device that performs cryptographic operations using one or more secure cryptographic keys and requires activation through the second authentication content. Authentication is performed by checking the ownership of the device and control of the key. The authenticator output is provided by direct connection to the user endpoint and strongly depends on the particular cryptographic device and protocol. Multi-factor authenticators of cryptographic devices use equipment protected from unauthorized access to encapsulate a private key.

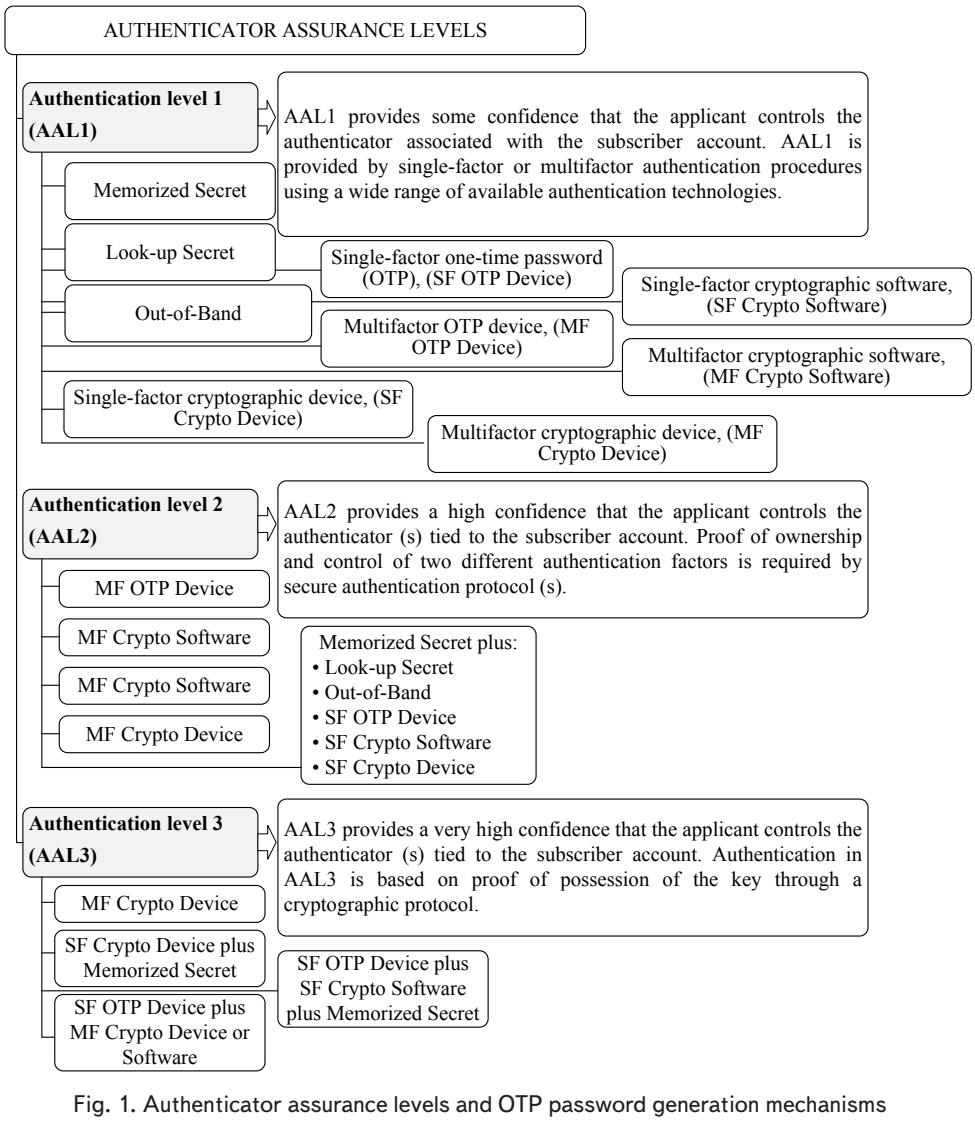


Fig. 1. Authenticator assurance levels and OTP password generation mechanisms

Thus, to ensure strict authentication in the IEN, it is proposed to use integrated mechanisms for providing two-factor authentication based on multi-channel cryptography on persistent cryptoalgorithms that ensure the security of the OTP passwords used.

Biometric methods form a probabilistic verification approach and do not provide key privacy (fingerprint, diaphragm, facial characteristics). Therefore, they can be used as an additional factor of multi-factor authentication with the help of a physical authenticator based on a secure channel between the sensor and the verifier.

Method based on Passwindows allows generating OTP passwords without using cryptographic procedures based on the bar code of the seven-segment element. However, the studies of this method and the proposed monitoring algorithm [12] allow hacking the *Passwindows* system in 3–5 sessions by forming a bar code of the tt card of the user of banking services.

Fig. 2 shows the main threats to authenticators, which can be classified according to the types of authentication factors based on attacks [6].

The conducted threat analysis based on the synergistic approach to threat assessment [14] showed that attackers today use an integrated approach to obtaining personal data and authenticators of users of IES service providers. As a rule, hacking methods are based on combining social engineering techniques with traditional methods of masquerading and infiltration.

In addition, new types of cyber attacks are used to effectively integrate malicious software into mobile communications, which in turn leads to a decrease in the profitability of multi-factor authentication methods based on SMS messages and OTP passwords in IEN.

Thus, it becomes necessary to use additional means to ensure the confidentiality of the transfer of authenticators in open switched mobile systems/4G LTE.

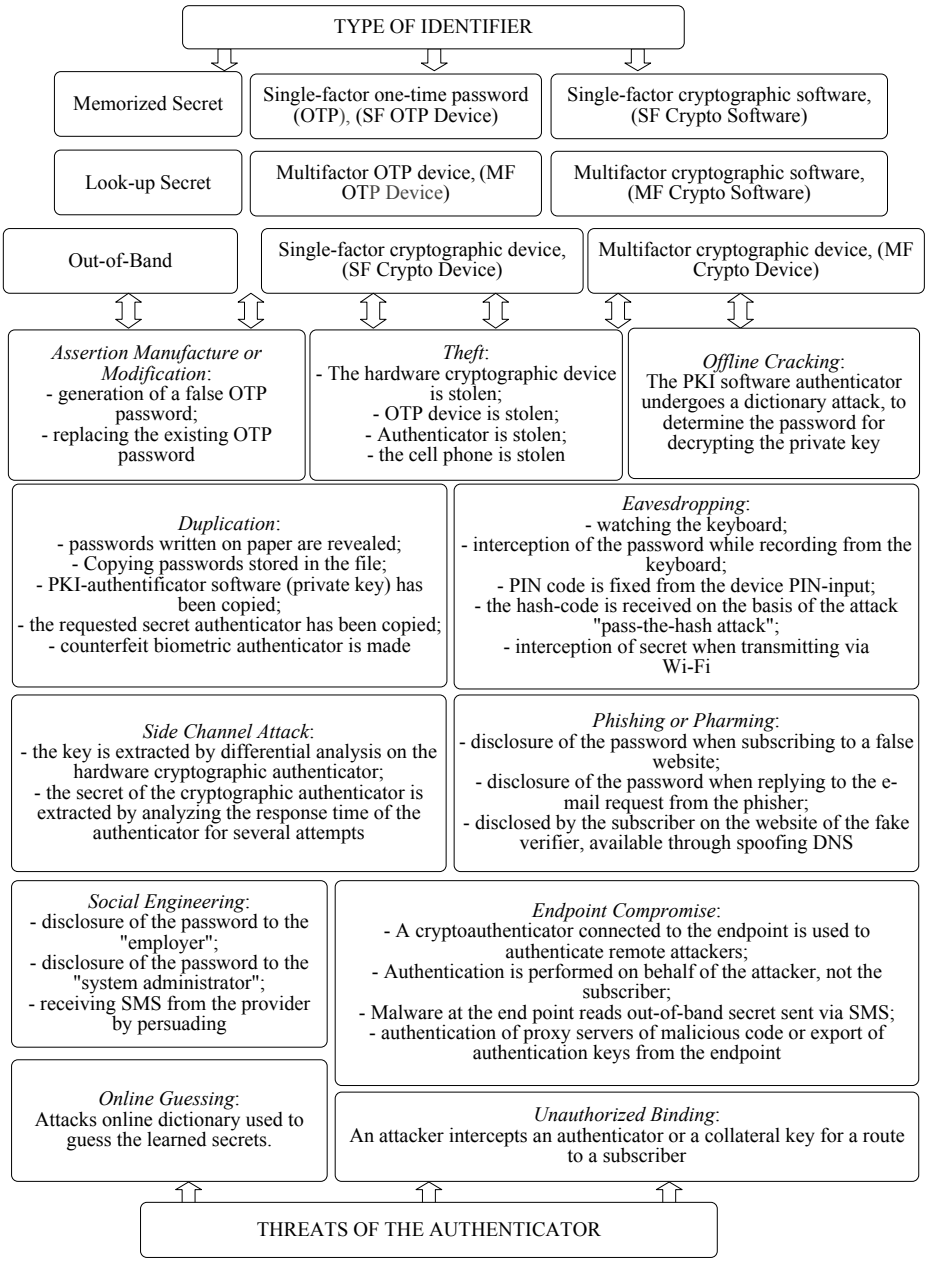


Fig. 2. Classification of threats by the type of the classifier

5. Development of a multi-factor authentication protocol based on hybrid crypto-code systems on flawed codes

The analysis of attacks on authenticators of multi-factor authentication schemes using OTP passwords allows us to formulate the basic requirements for such protocols:

– increasing the number of multi-factor authentication factors;

– increasing the length of secrets, the use of persistent standardized cryptoalgorithms;

– the use of encryption procedures for transmission over open GI channels, mobile open networks;

– increasing the requirements for the level of security in the system and network devices of GI and mobile networks;

– raising the level of information and cyber literacy of users.

To ensure the requirements, the authors propose to use the crypto-code systems considered in [13, 14, 22]. In [1], practical algorithms for constructing hybrid crypto-code systems on flawed codes are considered that allow improving the multi-factor authentication scheme in order to increase the level of cryptographic strength and authenticity of the authenticator generated.

To do this, the bank card (BC) must store the following data elements [13, 14]:

1) Certification Authority Public Key Index –since the terminal can work with several certification authorities, this value specifies which key the terminal must use when working with this card;

2) Issuer Public Key Certificate is signed by the appropriate certification authority;

3) Public Key Certificate of BC – is signed by the issuer and is formed on the basis of McEliece MCCS;

4) Issuer Public Key Modulus and Exponent;

5) Public Key Modulus and Exponent of BC;

6) Private Key of BC.

The terminal supporting the multi-factor authentication scheme must store the public keys of all certification authorities and associated information relating to each of the keys.

The terminal must also be able to select the appropriate keys based on the index (1) and some special identification information.

To support multi-factor authentication, the user's bank card (BC) must have its own key pair (public and private authenticator keys). The public key of the BC is stored on the BC in the public key certificate. Each public key of the BC is certified by the issuer, and the trusted certification authority certifies the public key of the issuer. This means that to verify the card's authenticator, the terminal first needs to check the two certificates in order to recover and authenticate the public key of the BC, which is then used to verify the authenticator of the BC.

The proposed authentication process consists of five steps:

1) Restoration of the certification authority public key by the terminal. The terminal reads the index (1), identifies and retrieves the certification authority public key modulus, the disguise matrix (*X, P, D*); *equation of a curve for an algebraic geometric code (AGC)*, and associated information stored in it, selects appropriate algorithms.

2) Obtaining the initialization vector (secret "places" in the error vector –shortening bits) from the issuer bank. Formation of the OTP code (error vector based on the Niederreiter modified crypto-code system (MCCS)).

3) Formation of the authenticator based on the use of McEliece MCCS. Obtaining the codeword (authenticator) based on the use of the crypto-code system by adding the obtained codeword with the session key.

4) Formation of the flawed text of the authenticator and the damage [23, 24].

5) Authentication. Finding the multiplicity of the error vector and comparing it with the obtained one. The structure of the proposed method of two-factor authentication based on the HCCSFC is shown in Fig. 3.

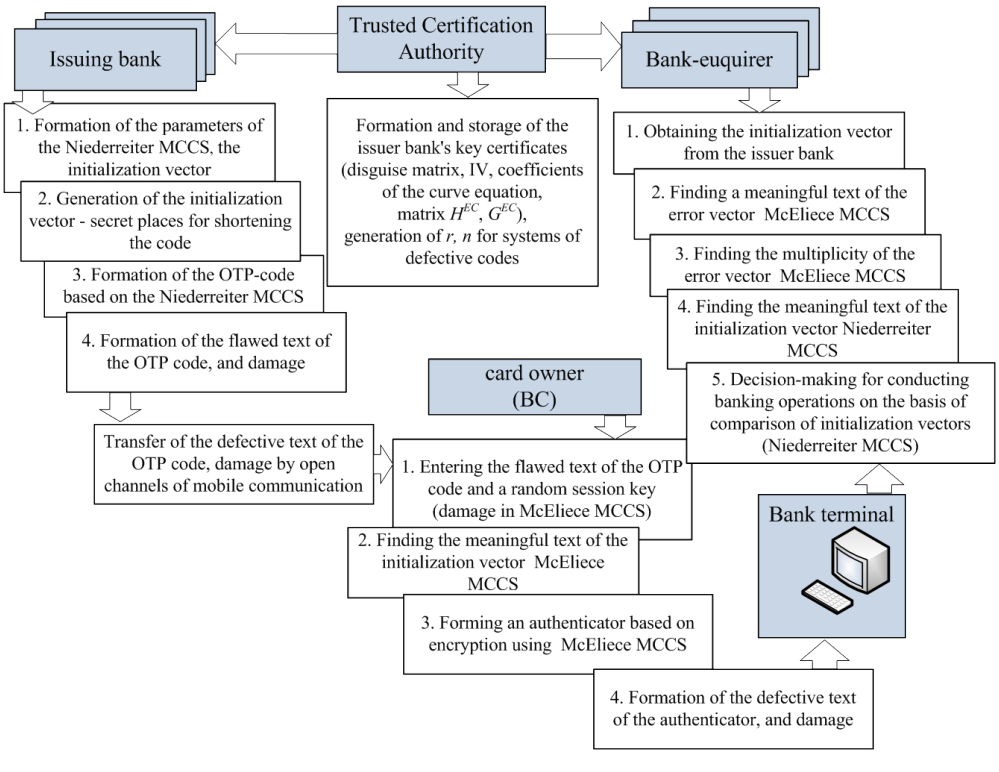


Fig. 3. Block diagram of the protocol of the improved OTP authentication method based on the HCCSFC

In the authors' opinion, an important advantage of this multi-factor authentication scheme is the provision of the required indicators of cryptographic strength and authenticity of transmitted authenticators based on the use of McEliece and Niederreiter modified asymmetric crypto-code systems Methods for transferring multi-channel cryptography systems on flawed codes allows the use of open mobile communication channels for the transmission of authentication tokens. The transfer of the flawed text of the OTP password and damage through open mobile communication channels using the Niederreiter MCCS provides the confidentiality of the OTP password. An additional factor of cryptographic strength is the use of the flawed text of the authenticator and/or damage (session key – error vector).

Thus, the use of hybrid crypto-code systems on flawed codes allows increasing the number of authenticator tokens, using two asymmetric crypto-code systems, two/four channels of transmission of the flawed text of the authenticator and the damage.

Scalability of the software module by changing the parameters of the Niederreiter and/or McEliece MCCS, depending on the requirements for the IES communication channels, provides its software implementation in mobile gadgets and compatibility with the protocols used for data transmission in the Internet and mobile networks.

6. Mathematical models of McEliece and Niederreiter MCCS on flawed codes, practical implementation algorithms

Let us consider a formal description of the McEliece modified crypto-code system on flawed codes used in the two-factor authentication protocol.

To construct a mathematical model, we use the basic provisions in [25] for a formal mathematical definition of a secret system. In [22], a formal description of the mathematical model of McEliece MACCS on modified elliptic codes was considered; in [1], a universal mechanism of damage and methods of transmission in systems on flawed codes were considered.

The mathematical model of McEliece MACCS on the basis of shortening (reduction of information symbols) is formally defined by the following elements [22]:

– a set of plaintexts

$$M=\{M_1,M_2,...,M_{q^k}\},$$

where $M_i=\{I_0,I_{h_1},..\,I_{h_j},I_{k\text{-}1}\}$, $\forall I_j\in GF(q)$, h_j are the information symbols equal to zero, $|h|=\frac{1}{2}k$, that is, I_i=0, $\forall I_i\in h$;

– a set of ciphertexts *(codegrams)*

$$C=\{\mathrm{C}_1,\mathrm{C}_2,...,\mathrm{C}_{\mathrm{q}^k}\},$$

where

$$C_i=(c^*_{X_0},c^*_{h_1},...,c^*_{h_j},c^*_{X_{n-1}}),\ \ \forall c^*_{X_j}\in GF(q);$$

– a set of direct mappings (based on public key usage – generating matrix)

$$\phi=\{\phi_1,\phi_2,...,\phi_s\},$$

where

$$\phi_i: M\to C_{k-h_j},\ \ i=1,2,...,s;$$

– a set of inverse mappings (based on private key usage – disguise matrixes)

$$\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\},$$

where

$$\phi_i^{-1}: C_{k-h_j}\to M,\ \ i=1,2,...,s;$$

– a set of keys, parameterizing direct mappings (public key of the authorized user)

$$K_{a_i}=\{K_{1_{a_i}},K_{2_{a_i}},...,K_{s_{a_i}}\}=\{G_X^{EC_1}{}_{a_i},G_X^{EC_2}{}_{a_i},...,G_X^{ECs}{}_{a_i}\},$$

where $G_X^{ECi}{}_{a_i}$ is the generating $n\times k$ matrix disguised as a random code of the-algebraic geometric block (n, k, d) code with elements from $GF(q)$, i. e.

$$\phi_i: M\xrightarrow{K_{ia_i}}C_{k-h_j};\ \ i=1,2,...,s;$$

a_i is a set of the polynomial curve coefficients $a_1...a_6$, $\forall a_i\in$ $\in GF(q)$, uniquely defining a specific set of points on the curve from the space P^2;

– a set of keys, parameterizing inverse mappings (private key of the authorized user)

$$K^*=\{\mathrm{K}_1^*,\mathrm{K}_2^*,...,\mathrm{K}_s^*\}=\{\{\mathrm{X,P,D}\}_1,\{\mathrm{X,P,D}\}_2,...,\{\mathrm{X,P,D}\}_s\},$$

$$\{\mathrm{X,P,D}\}_\mathrm{i}=\{X^i,P^i,D^i\},$$

where X^i is the disguise nondegenerate randomly equiprobably formed by a source of keys $k\times k$ matrix with elements from $GF(q)$; P^i – permutation randomly equiprobably formed by a source of keys $n\times n$ matrix with elements from $GF(q)$; D^i – diagonal formed by a source of keys $n\times n$ matrix with elements from $GF(q)$, i. e.

$$\phi_i^{-1}: C\xrightarrow{\mathrm{K}_\mathrm{i}^*}M,\ \ i=1,2,...,s,$$

the complexity of the inverse mapping ϕ_i^{-1} without knowing the key $\mathrm{K}_\mathrm{i}^*\in K^*$ is associated with solving theoretical-complexity problems in random code decoding (general position code).

The initial data in the description of the considered asymmetric crypto-code information protection system are:

– algebraic geometric block (n, k, d) code C_{k-h_j} over $GF(q)$, i. e. a set of codewords $C_i\in C_{k-h_j}$ such that the equality is true $C_iH^T=0$, where H is the parity check matrix of the algebraic geometric block code;

– a_i – a set of the curve polynomial coefficients $a_1...a_6$, $\forall a_i\in GF(q)$, uniquely defining a specific set of the curve points from the space P^2 to form the generating matrix;

– h_j – information symbols, equal to zero, $|h|=1/2k$, i. e. I_i=0, $\forall I_i\in h$;

– disguising matrix mappings, given by a set of matrices $\{\mathrm{X, P, D}\}_\mathrm{i}$, where X is the nondegenerate $k\times k$ matrix over $GF(q)$, P is the permutation $n\times n$ matrix over $GF(q)$ with one non-zero element in each row and each column of the matrix, D is the diagonal $n\times n$ matrix over $GF(q)$ with non-zero elements on the main diagonal.

In the McEliece MACCS, the modified (shortened) algebraic geometric (n, k, d) code C_{k-h_j} with fast decoding algorithm is disguised as a random (n, k, d) code C_{k-h_j}* by multiplying the generating matrix G^{EC} of the code C_{k-h_j} by the secret disguise matrices X^u, P^u and D^u [8], providing the formation of the authorized user's public key:

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

$$u \in \{1,2,...,s\},$$

where G^{EC} is the generating $n \times k$ matrix of the algebraic geometric block (n, k, d) code with elements from $GF(q)$, built on the basis of the user-selected curve polynomial coefficients $a_1 ... a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of points on the curve from the space P^2.

The formation of the ciphertext $C_j \in C_{k-h_j}$ on the basis of the entered plaintext $M_i \in M$ and a given public key $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ is carried out by forming a codeword of the disguised code by adding the random vector $e = (e_0, e_1, ..., e_{n-1})$:

$$C_j = \phi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e,$$

where the Hamming weight (number of nonzero elements) of the vector does not exceed the correcting ability of the algebraic block code used:

$$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

$\lfloor x \rfloor$ – the integer part of the real number x.

For each formed ciphertext $C_j \in C_{k-h_j}$, the corresponding vector $e = (e_0, e_1, ..., e_{n-1})$ acts as a one-time session key, i. e. for a particular E_j the vector e is generated randomly equiprobably and independently of the other ciphertexts.

The communication channel receives

$$C_j^* = C_j - C_{k-h_j}.$$

On the receiving side, an authorized user who knows the rules of damage F_n^r, disguise, the number and location of zero information symbols can use a fast algebraic geometric code decoding algorithm (with polynomial complexity) to recover the plaintext [8]:

$$E_{K_{MV2}}^{-1} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j^*,$$

$$M_i = \phi_u^{-1}\left(C_j^*, \{\mathrm{X,P,D}\}_\mathrm{u}\right).$$

To recover the plaintext, an authorized user adds zero information symbols $C_j^* = C_j + C_{k-h_j}$, from the recovered ciphertext C_j, removes the effect of the secret permutation and diagonal matrices P^u and D^u:

$$C = C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \times$$

$$\times \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

decodes the received vector by the Berlekamp-Massey algorithm [15]:

$$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

i. e. gets rid of the second term and the multiplier $(G)^{ECT}$ in the first term on the right side of the equation, and then removes the effect of the disguise matrix X^u. For this, the result of decoding $M_i \cdot \left(X^u\right)^T$ should be multiplied by

$$\left(X^u\right)^{-1} : \left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i.$$

The resulting solution is the plaintext M_i.

For the practical implementation of the HCCSFC, Fig. 4, 5 present the algorithms for specifying the basic characteristics of algebraic geometric codes on elliptic curves. Where: *requiredProbability* is the given probability of the block distortion; *n* is the total number of characters in the code (code length); *k* is the number of information symbols; *d* is the minimum distance of the Hamming code combinations; *g* is the genus of the curve; *degF is* the degree of the generator function; *degCurve* is the degree of the curve, *probability* is the probability of distortion of one symbol; *n* is the total number of characters in the code (code length); *ecc* is the number of errors corrected by the code.

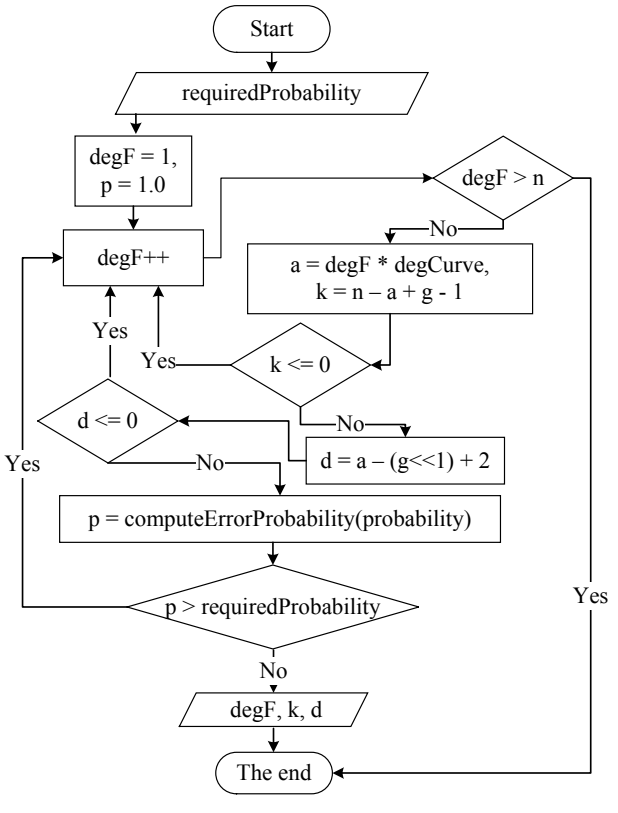


Fig. 4. Block diagram of the calculation function of the code parameters

Pratical algorithms for the formation of the flawed text of one factor of the authenticator and decryption/verification based on the McEliece hybrid crypto-code system on flawed codes are shown in Fig. 6, 7 (formation of the cryptogram), Fig. 8 (decryption of the cryptogram).

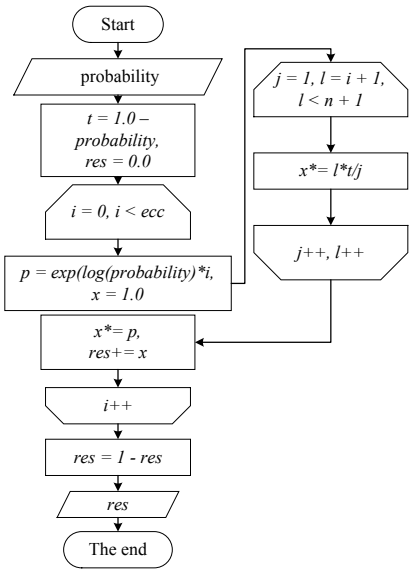


Fig. 5. Error probability calculation function for the specified code parameters

Algorithm for forming the codegram in the McEliece HCCS on flawed codes is given by the sequence of the following steps:

Step 1. We fix a finite field *GF(q)*. We fix an elliptic curve

$$y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$$

and a set of its points $EC(GF(q)):(P_1, P_2,..., P_N)$ over *GF(q)*. We fix a subset of points $h(GF(q))$: $(P_{x1}, P_{x2}, ...,P_{xx})$, $h\subseteq EC(GF(q))$, $|h|=x$ and keep it secret.

Step 2. We form the initialization vector $IV=EC-h_j$, h_j – information symbols equal to zero, $|h|=\frac{1}{2}k$, i. e. $I_i=0, \leftrightarrow I_i\in h$;

Step 3. By entering the information vector *I*, we form the codeword *c*. If (*n*, *k*, *d*) code over *GF(q)* is given by its generating matrix, then $c=I\times G$.

Step 4. We form the random error vector *e* so that $w(e)\leq t$, $t=\lfloor (d-1)/2 \rfloor$. We add the formed vector to the codeword, obtain the codeword: $c^*=c+e$.

Step 5. We form the codegram by removing (shortening) the initialization vector symbols:

$$c_X{}^*=c^*-IV.$$

Step 6. We form the flawed text (the remainder) and the flag (damage)

$$C_j^* = C_j - C_{k-h_j}, E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

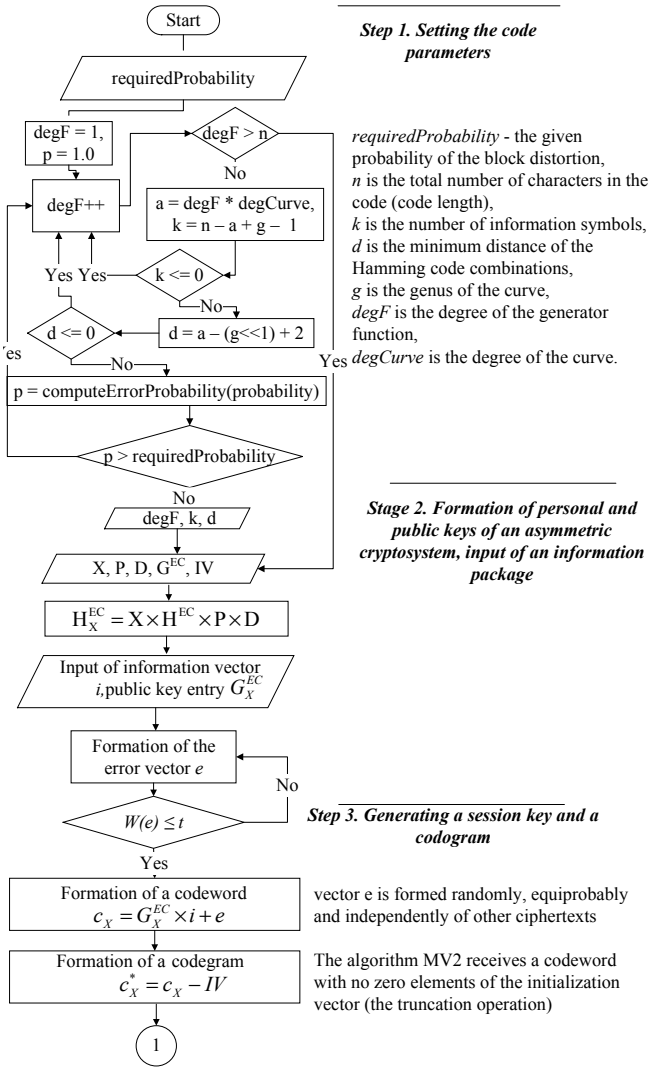
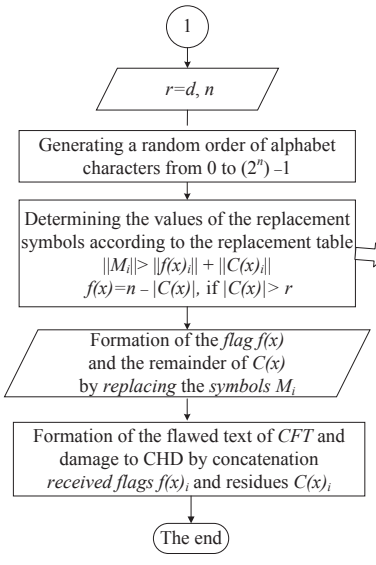


Fig. 6. Algorithm for the formation of a cryptogram in the McEliece hybrid crypto-code system on flawed codes



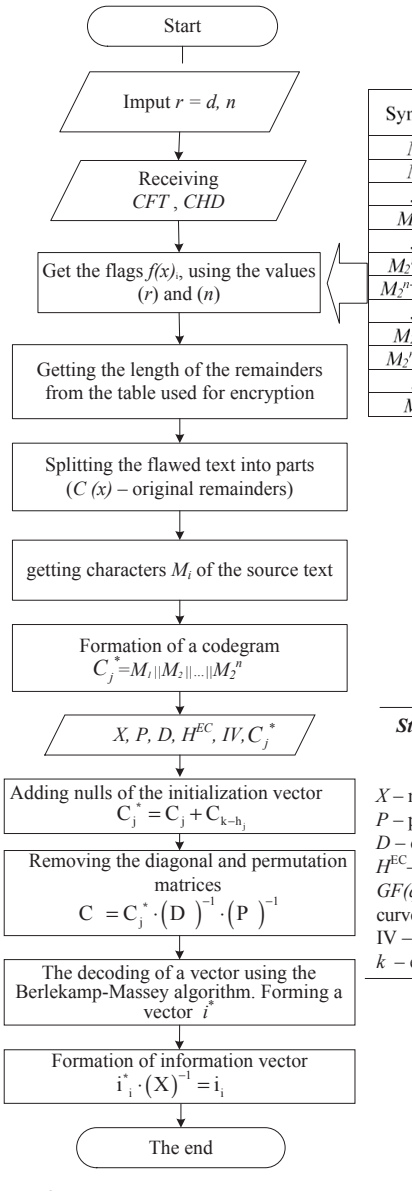
Step 4. Damage

Symbol	Length of the remainder	Balance $C(x)$	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}

n is the total number of characters in the code (code length),
d is the minimum distance of the Hamming code combinations, $f(x)$ is the flag, $C(x)$ is the remainder

The channel / channels of communication receive a flawed text (remainder) and damage (flag)

Fig. 7. Algorithm for the formation of a cryptogram in the McEliece hybrid crypto-code system on flawed codes



Stage 1. The formation of a meaningful code

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}

n is the total number of characters in the code (code length),
d is the minimum distance of the Hamming code combinations,
$f(x)$ is the flag,
$C(x)$ is the remainder

Step 2: Setting the code parameters, enter the private key and the codegram

X – non-degenerate $k \times k$ matrix over $GF(q)$,
P – permutation $n \times n$ matrix over $GF(q)$,
D – diagonal $n \times n$ matrix over $GF(q)$,
H^{EC} – testing $r \times n$ matrix of elliptic code over $GF(q)$, a_i – set of coefficients of the polynomial curve $a_1 \ldots a_6$,
IV – initialization vector, IV= $|h|$ =½
k – elements of reduction

Step 3. Decoding the code

Fig. 8. Decryption of the cryptogram in the McEliece HCCS on flawed codes

Algorithm for decoding codegrams in the McEliece HCCSFC set by the sequence of the following steps.

Step 1. Obtaining a meaningful text of the codegram based on the MV2 algorithm:

$$E^{-1}_{K_{MV2}}: \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j^*.$$

Step 2. Entering the codegram to be decoded. Entering the private key – the generator and/or parity check matrix of the elliptic code.

Step 3. The codegram is the codeword with errors in the elliptic code. The weight of the error vector $w(e) \le t$. We decode the codegram – we find the error vector.

Step 4. We form the required information vector.

Let us consider a formal description of the *mathematical model of Niederreiter hybrid MCCS*, which is specified by the following elements:

–a set of plaintexts

$$M = \left\{ M_1, M_2, ... M_{q^k} \right\},$$

where $M_i = \left\{ e_0, e_{h_1}, ... e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$, $h_{e\,v}$ are the error vector symbols equal to zero, $|h| = \frac{1}{2} e$, i. e. $e_i = 0$, $\forall e_i \in h$;

–a set of ciphertexts

$$S = \left\{ S_0, S_1, ... S_{q^r} \right\},$$

where

$$S_i = \left\{ S^*_{X_0}, S^*_{h_1}, ... S^*_{h_j}, S^*_{X_r} \right\}, \quad \forall S_{X_r} \in GF(q);$$

– a set of direct mappings (based on the use of public key – parity check matrix of the elliptic code (EC):

$$\varphi = \left\{ \varphi_1, \varphi_2, ..., \varphi_r \right\},$$

where $\varphi_i : M \to S_{r-h_e}, i = 1,2,...,e$;

– a set of inverse mappings (based on the use of a private key –disguise matrices)

$$\varphi^{-1} = \left\{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1} \right\},$$

where $\varphi_i^{-1} : S_{r-h_e} \to M, i = 1,2,...,e$;

– a set of keys that parameterize direct mappings (public key of an authorized user):

$$KU_{a_i} = \left\{ KU_{1_{a_i}}, KU_{2_{a_i}}, ..., KU_{r_{a_i}} \right\} = \left\{ H^{EC_1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, ..., H^{ECr}_{X_{a_i}} \right\},$$

where $H^{EC_i}_{X_{a_i}}$ is the parity check $r \times n$ matrix of the algebraic geometric block (n, k, d) code with elements from $GF(q)$, that is,

$$\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*_{r-h_e}, \quad i = 1,2,...,e,$$

a_i is the set of coefficients of the polynomial curve $a_1 ... a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of points of a curve from the space P^2.

– a set of keys that parameterize inverse mappings (private key of an authorized user):

$$KR = \left\{ KR_1, KR_2, ..., KR_r \right\} =$$

$$= \left\{ \{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_r \right\},$$

$$\{X,P,D\}_i = \left\{ X^i, P^i, D^i \right\},$$

where X^i is the disguise nondegenerate randomly equiprobably generated by the source of keys $k \times k$ matrix with elements from $GF(q)$; P^i is the permutation randomly generated by the source of keys $n \times n$ matrix with elements from $GF(q)$; D^i is the diagonal formed by the source of keys $n \times n$ matrix with elements from $GF(q)$, i. e.

$$\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M, \quad i = 1,2,...,s,$$

the complexity of performing a reverse mapping φ_i^{-1} without knowledge of the key $KR_i \in KR$ is associated with the solution of the theoretic-complexity problem of decoding a random code (code of general position).

–a set of flawed texts *CFT*,

$$CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\};$$

–a set of damages *CHD*,

$$CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\};$$

– a set of direct damage (based on the use of the key – K^i_{MV2}, and algorithm MV2)

$$E = \{E^1_{K_{MV2}}, E^2_{K_{MV2}}, ..., \phi^S_{K_{MV2}}\}, \quad i = 1,2,...,s;$$

$f(x)_i$ – flag (damage, *CHD*), $C(x)_i$ – remainder (flawed text, *CFT*); $f(x) = n - |C(x)|$, if $|C(x)| > r$, where r is some parameter $r \in_R Z_{q^m}, 0 \langle r \langle n$;

– a set of mappings *MV2* F^r_n is given by a bijective mapping between the set of permutations $\{S_1, S_2, ..., S_{2^n}\}$ and by the set $\# F^r_n$, $\# F^r_n = \# \left\{ (c, f) \right\} = 2^n !$;

– a set of meaningful text (based on the use of the key – K^i_{MV2}, and algorithm MV2).

The initial data for describing the considered asymmetric crypto-code system of information protection are:

– non-binary equilibrium code over *GF (q)*, that is, the set of sequences of length n and weight $w(\varepsilon_i)$;

– algebraic geometric block *(n, k, d)* code C over *GF(q)*, i. e. the set of codewords $C_i \in C$ such that the equality $C_i H^T = 0$, where H is the parity check matrix of the algebraic geometric block code;

– *IV* – initialization vector, $IV = |h| = ½\ h_v$ – elements of reduction ($h_{e\,v}$ – error vector symbols equal to zero, $|h| = 1/2e$, i. e. $e_i = 0$, $\forall e_i \in h$);

– disguise matrix mappings given by a set of matrices $\{X,P,D\}_i$, where X is the non-degenerate $k \times k$ matrix over *GF(q)*, P is the permutation $n \times n$ matrix over *GF(q)* with one non-zero element in each row and in each column of the matrix, D is the diagonal $n \times n$ matrix over *GF(q)* with non-zero elements on the main diagonal;

– r – some parameter

$$r \in_R Z_{q^m}, Z_{q^m} = \left\{ 0,1,...2^n - 1 \right\},$$

n – some parameter

$$n \in_R Z_{q^n}, Z_{q^n} = \left\{ 1,...2^n \right\};$$

– a set of mappings *MV2* F^r_n.

On the basis of equilibrium coding, a ciphertext is formed by $C_j \in C$ with the entered plaintext $M_i \in M$ and the given key H_X^{ECu}, $u \in \{1,2,...,s\}$ by forming a syndrome (in terms of error-correction coding) sequence S_{X_j}, corresponding to the equilibrium sequence $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$:

$$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \cdot \left(H_X^{ECu}\right)^T,$$

the Hamming weight (the number of non-zero elements) of the vector does not exceed the correcting ability of the algebraic block (n,k,d) code:

$$\forall i: 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

The cardinality of the sets M and C is determined by the admissible spectrum of the weights $w(M_i)$, that is, in the general case (for all admissible values $w(M_i)$) we have:

$$m = \sum_{i=0}^{t} (q-1)^i \cdot C_n^i,$$

where C_n^i is the binomial coefficient,

$$C_n^i = \frac{n!}{i! \cdot (n-1)!}.$$

It is the most appropriate to select the value $w(M_i)$ according to the required data transfer security value.

Then for $w(M_i) = const = w(e)$ we have:

$$m = (q-1)^{w(e)} \cdot C_n^{w(e)},$$

and the sequence

$$M_i = \{e_0, e_1, ..., e_{n-1}\}$$

from the set

$$M = \{M_1, M_2, ..., M_m\}$$

are formed as a result of some mapping ψ, realized by redundant coding by non-binary equilibrium codes of non-redundant information sequences.

The formed ciphertext $C_j \in C$ uniquely corresponds to the vector $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Let's form the initialization vector $IV=EC-h_j$, h_j – information symbols equal to zero, $|h| = \frac{1}{2}k$, that is, $I_i=0$, $\forall I_i \in h$.

Formation of the shortened error vector $e_x = e(A) - IV$.

The public key is formed by multiplying the parity check matrix of the algebraic geometric code by the disguise matrices

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u, \quad u \in \{1,2,...,s\},$$

where H^{EC} is the parity check $n \times (n-k)$ matrix of the algebraic geometric block (n,k,d) code with elements from $GF(q)$.

The MV2 algorithm receives a syndrome sequence

$$S^*_{r-h_e} = (e_n - h_e) \times H_X^{ECT}.$$

The MV2 algorithm receives $S^*_{r-h_e}$,

$$E_{K_{MV2}} : S^*_{r-h_e} \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

In the communication channel $\left\| f(x)_i \right\|$ and $\left\| C(x)_i \right\|$, the transmission can be carried out either by one or two independent channels.

On the receiving side, an authorized user who knows the rule of damage F_n^r, disguise (the set of matrices $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) and the initialization vector (the number and places of the zero-point symbols of the error vector):

$$E^{-1}_{K_{MV2}} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to S^*_{r-h_e},$$

forms a code sequence $c^*_{X_i}$ as one (any) of the possible solutions of the equation

$$S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j},$$

i. e., it finds such the vector $c^*_{X_i}$, which is decomposed into the sum

$$c^*_{X_i} = c_{X_i} + M_i,$$

where c_{X_i} is one (any) of the possible codewords of the disguised (n,k,d) code with the parity check matrix $H^T_{X_j}$, i. e.

$$c_{X_i} \cdot H^T_{X_j} = 0.$$

Next, an authorized user using a set of matrices

$$\{X,P,D\}_u = \{X^u, P^u, D^u\}$$

forms the vector

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

that is, unmasks the code sequence $c^*_{X_i}$.

After substitution, we obtain the equality:

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(c_{X_i} + M_i\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$
$$= c_{X_i} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

An authorized user who generated the vector $\bar{c}^*$, has the ability to apply a fast (polynomial complexity) algorithm for error-correction decoding and thus form the vector

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$$

and the vector

$$M_i^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

To restore the information equilibrium sequence M_i it is enough to multiply the vector M_i^u again by the disguise matrices D^u and P^u, but in a different order:

$$M_i = M_i^u \cdot P^u \cdot D^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u = M_i.$$

Formation of the sought error vector e:

$$M = M_i + IV.$$

To construct the Niederreiter HCCS, we use the main algorithms of encryption/decryption of the system, considered in [14]. Fig. 9, 10 show a block diagram of the Niederreiter MCCS, the main difference from the known construction

methods is the use of the shortening mechanism for the symbols of the error vector obtained in the algorithm of equilibrium coding. The system on flawed codes can reduce the power of the alphabet, which reduces the power of $GF(q)$ used and the computing power capacity of the system as a whole.

An analysis of the practical implementation of encryption/decryption algorithms in the Niederreiter HCCSFC shows that after the error vector is formed on the basis of the initialization vector, its shortening is performed – h_v (error vector symbols equal to zero), $|h|=1/2e$, i. e. $e_i=0$, $\forall e_i \in h$. The initialization vector is formed by the PRSG in accordance with [21] in the trusted center and transmitted through closed channels to technical information protection systems (TIPS) to the issuer and acquirer banks. For transmission to the GI, the initialization vector is transformed by the MV2 algorithm into binary sequences of flawed text (*CFT*) and damage (*CHD*), each of which is transmitted through an independent open channel.

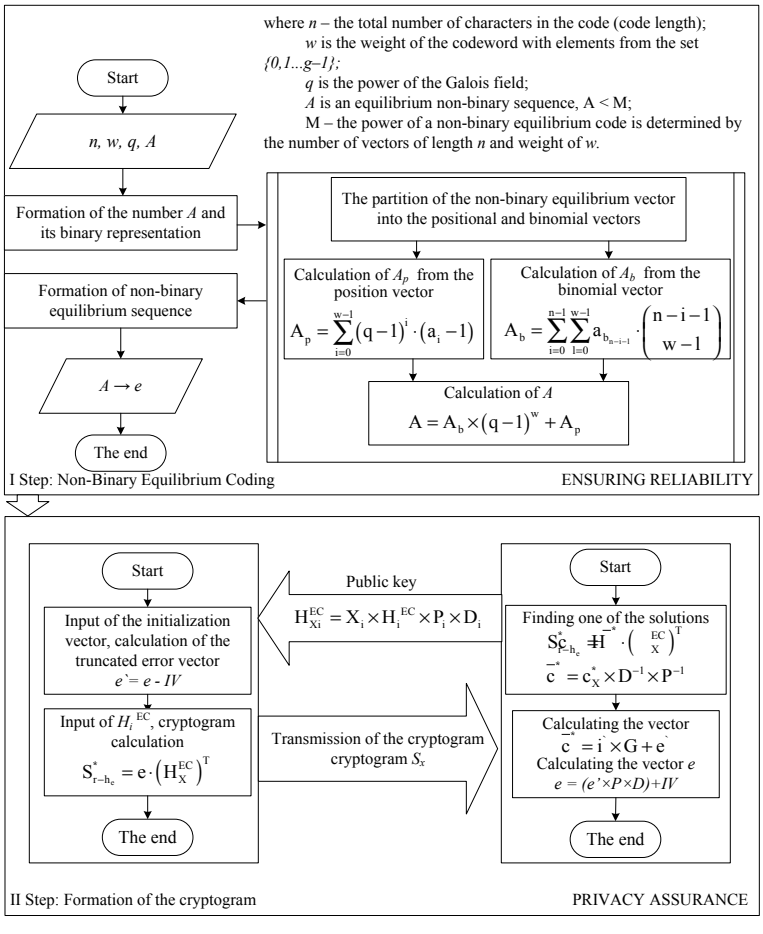


Fig. 9. Schematic block diagram of the hybrid Niederreiter crypto-code system on flawed codes

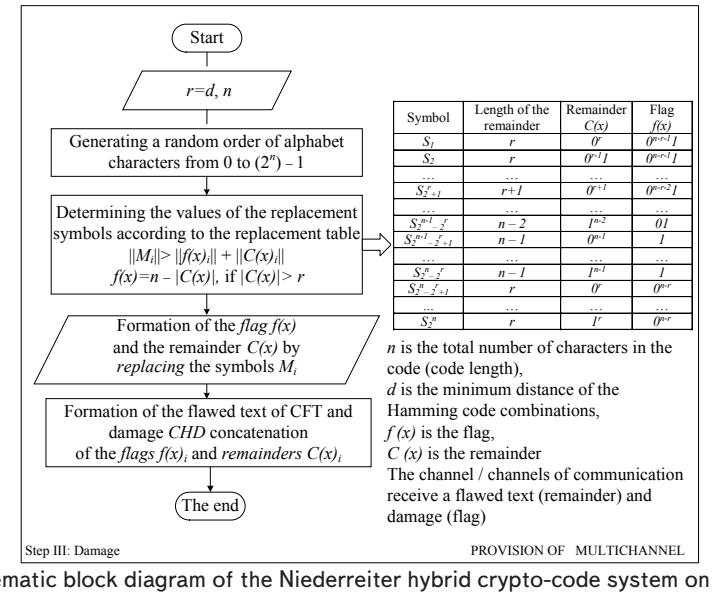


Fig. 10. Schematic block diagram of the Niederreiter hybrid crypto-code system on flawed codes

When decrypting the cryptogram (after receiving the error vector, before using the equilibrium coding algorithm), "zero" shortening symbols are introduced to obtain the information. The encryption and decryption algorithms are shown in Fig. 11, 12 (encryption), Fig. 13, 14 (decryption).

Algorithm for the formation of a cryptogram in the Niederreiter MCCS can be represented as a sequence of the following steps:

Step 1. Entering information to be encoded. Entering the public key H_X^{EC}.

Step 2. Formation of the error vector e, whose weight does not exceed $\leq t$ – the corrective power of the elliptic code based on the non-binary equilibrium coding algorithm [13, 14].

Step 3. Formation of the shortened error vector: e_x= =e(A)–IV.

Step 4. Formation of the codegram

$$S^*_{r-h_e} = (e_n - h_e) \times H_X^{ECT}.$$

Step 5. Formation of the flawed text (the remainder) and the flag (damage)

$$E_{K_{MV2}} : S^*_{r-h_e} \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

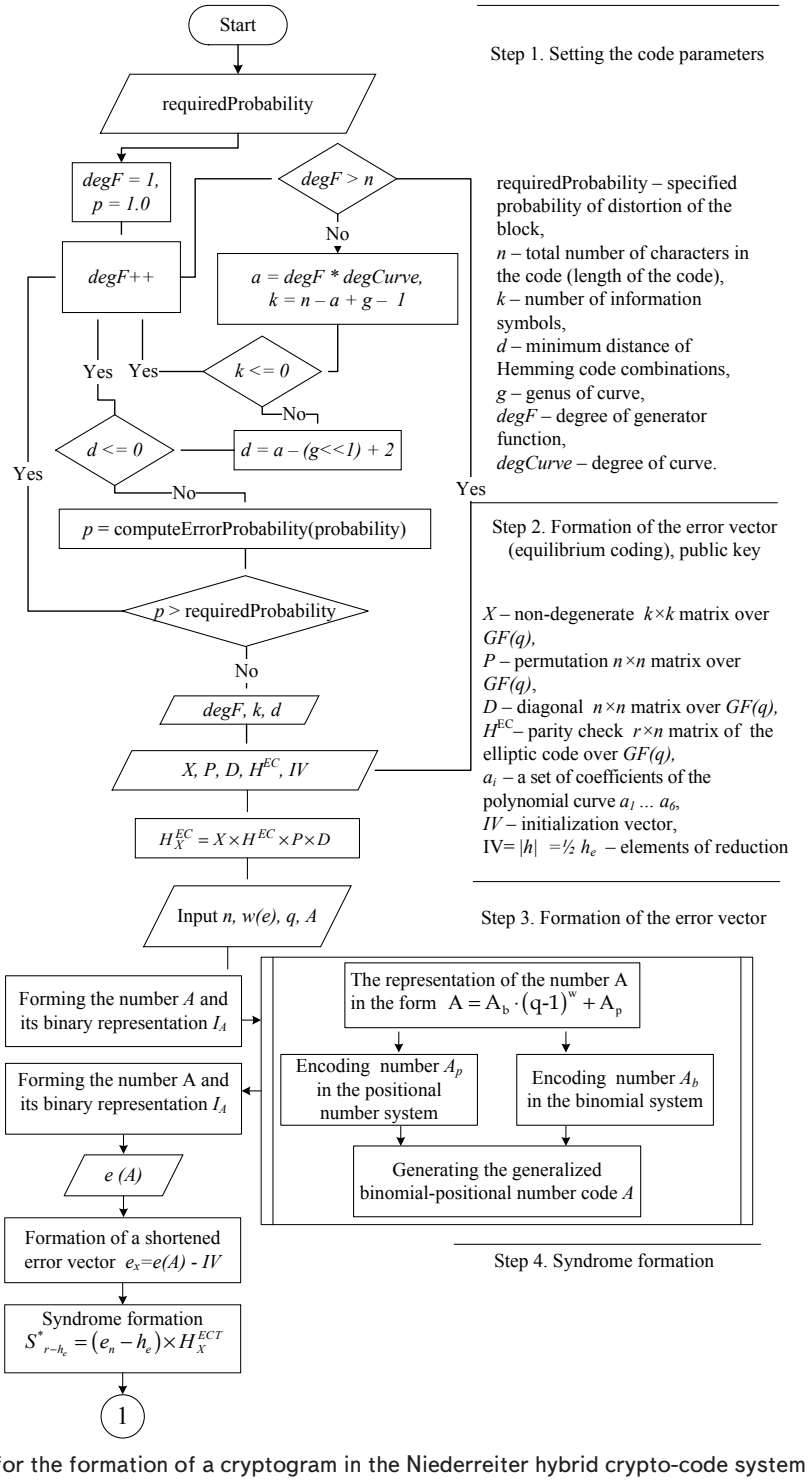
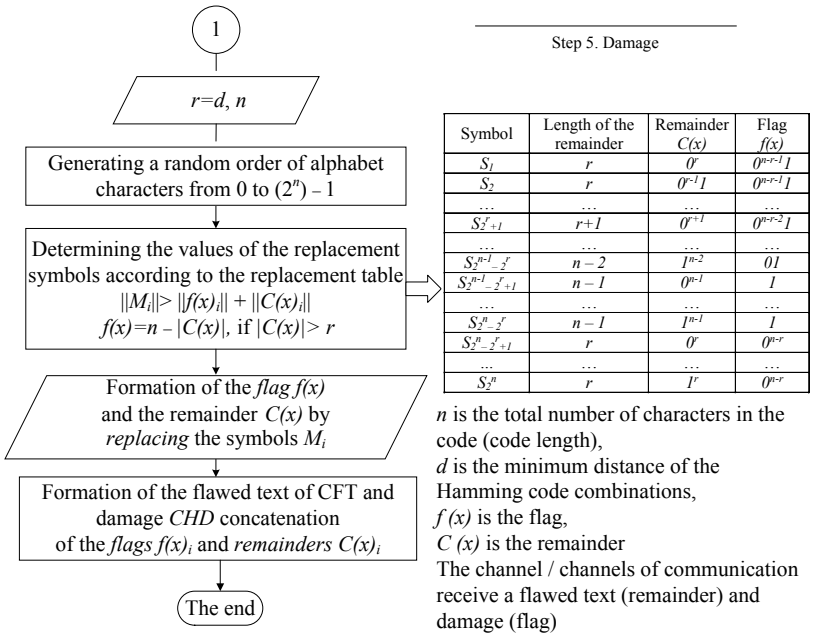


Fig. 11. Algorithm for the formation of a cryptogram in the Niederreiter hybrid crypto-code system on flawed codes



Symbol	Length of the 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. 12. Algorithm for the formation of a cryptogram in the Niederreiter hybrid crypto-code system on flawed codes

Algorithm for decoding the codegram in the Niederreiter MCCS can be represented as a sequence of the following steps:

Step 1. Obtaining a meaningful text of the codegram based on the MV2 algorithm:

$$E^{-1}_{K_{MV2}}: \left\|f(x)_i\right\| + \left\|C(x)_i\right\| \to S^*_{r-h_e}.$$

Step 2. Entering the code S_X to be decoded. Entering the private key – matrices *X, P, D.*

Step 3. Finding one of the possible solutions of the equation:

$$S^*_{r-h_e} = \overline{c}^* \times \left(H^{EC}_X\right)^T.$$

Step 4. Removing the action of the diagonal and permutation matrices:

$$\overline{c}^* = c^*_X \cdot D^{-1} \cdot P^{-1}.$$

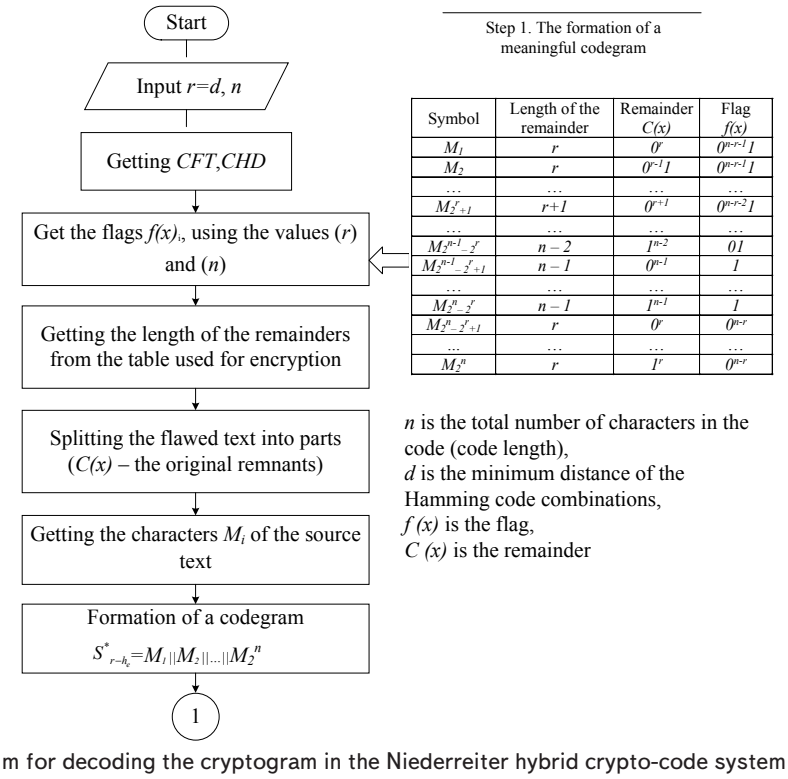
Step 5. Decoding the vector $\overline{c}^*$. Forming the vector e_x'.

Step 6. Transformation of the vector e_x': $e_x=e_x'\times P\times D$.

Step 7. Formation of the sought error vector e:

$$e=e_x+IV.$$

Step 8. Transformation of the vector e based on the use of non-binary equilibrium code in the information sequence.



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. 13. Algorithm for decoding the cryptogram in the Niederreiter hybrid crypto-code system on flawed codes

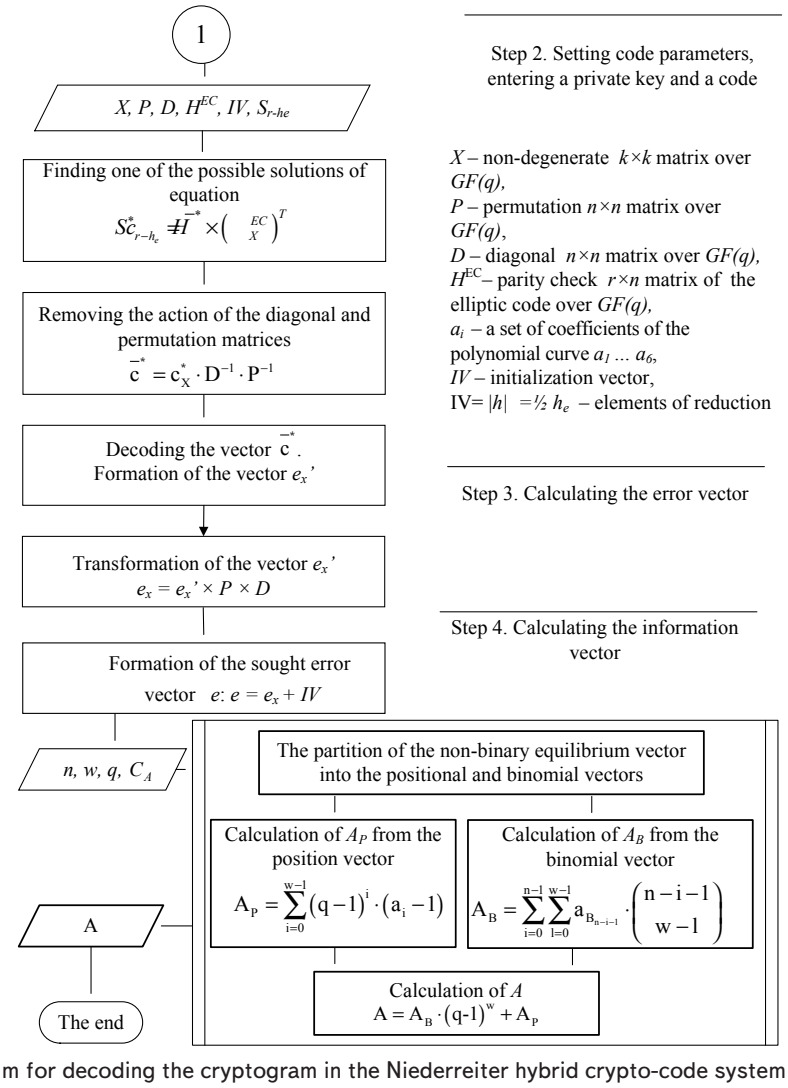


Fig. 14. Algorithm for decoding the cryptogram in the Niederreiter hybrid crypto-code system on flawed codes

Thus, a new approach to using the method of two-factor authentication based on OTP passwords, allowing its further application is proposed.

7. Discussion of the results of using the multi-factor authentication method

The proposed advanced method of strict two-factor authentication with OTP passwords based on McEliece and Niederreiter crypto-code systems allows eliminating the main disadvantage of the protocol 2FA – the transfer of individual authentication tokens via open mobile communication channels. For this purpose, crypto-code systems on flawed codes providing the required safety indices on the basis of encryption using the Niederreiter/McEliece asymmetric crypto-code system, the rate of crypto-transformations at the level of block cryptographic algorithms and the provision of data transmission with direct error correction have been proposed. This approach can be implemented in modern mobile and desktop applications using the protocols of GI and/or mobile networks.

A *schematic block diagram of practical implementation* of the proposed HCCS on flawed codes is shown in Fig. 15.

Assessment of the cryptographic strength of the proposed HCCS on flawed codes

To assess the cryptographic strength, we use the entropy method proposed in [1].

The proposed hybrid cryptosystem is comparable in stability with the second method of damage – damage to the ciphertext considered in [23, 24]. In this case, we have a set of flawed ciphertexts and damages, all individually not corresponding to the original meaningful text. With a complete set of flawed ciphertexts and all damages, the unicity distance increases due to additional keys of damage to the ciphertext. Thus, additional encryption provides an increased unicity distance:

$$U_0 = \frac{\begin{array}{l} H\left(H^{EC}\right)+H\left(X_N^{EC}\right)+H\left(P_N\right)+H\left(D_N\right)+ \\ +H\left(G^{EC}\right)+H\left(X_{Mc}^{EC}\right)+H\left(P_{Mc}\right)+H\left(D_{Mc}\right)+ \\ +\sum_{i=1}^{m}H\left(\left(K_{MV2_N}^i\right)+H\left(K_i\right)\right)+\sum_{i=1}^{m}H\left(\left(K_{MV2_{Mc}}^i\right)+H\left(K_i\right)\right) \end{array}}{B\log|I|}, \quad (1)$$

where U_0 is the unicity distance, H^{EC}, X_N^{EC}, P_N, D_N is the private key in the Niederreiter MCCS, G^{EC}, X_{Mc}^{EC}, P_{Mc}, D_{Mc} is the private key in the McEliece MCCS, $K_{MV2_N}^i$ is the key in the Niederreiter HCCS on flawed codes, $K_{MV2_{Mc}}^i$ is the key in the McEliece HCCS on flawed codes, $|I|$ is the number of meaningful texts, B is the number of texts, m is the number of damages.

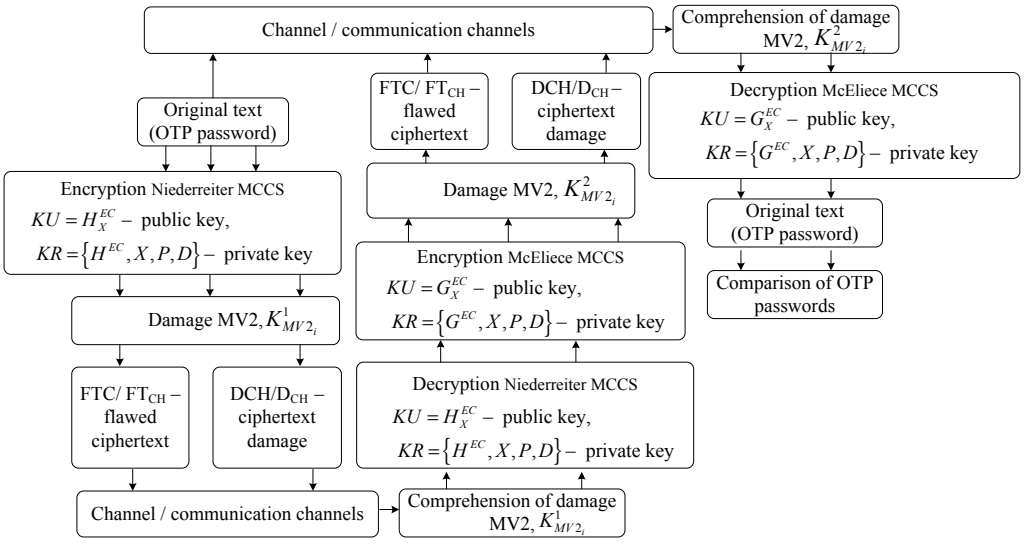


Fig. 15. Schematic block diagram of practical implementation of HCCSFC

Expression (1) makes it possible to evaluate the stability of the proposed McEliece and Niederreiter hybrid crypto-code systems on flawed codes.

8. Conclusions

1. The analysis of multi-factor authentication methods showed that in automated banking systems, 95 % of bank customers use electronic banking based on multi-factor OTP authentication. However, the use of OTP passwords in open data transmission systems in recent months has not met the security requirements. For further use, the NIST experts recommend using additional authentication factors with the mandatory transfer of OTP passwords in encrypted form and/or through closed communication channels, which significantly increases the cost and time of transmission. To solve the problem, a method of improving 2FA based on the use of hybrid crypto-code systems on flawed codes is proposed. These complex cryptosystems provide all the requirements for 2FA and allow expanding the range of use in IEN (CBS).

2. Mathematical models and practical algorithms for encryption/decryption of cryptograms/codegrams in hybrid crypto-code systems based on modified Niederreiter and McEliece crypto-code systems on flawed codes are proposed. They differ from the error vector (initialization vector) symbol shortening, and provide the required cryptographic strength when transmitting data over open mobile communication channels.

3. The developed multi-factor authentication scheme based on the Niederreiter-McEliece HCCSFC allows eliminating a significant drawback of 2FA on the basis of SMS – providing confidentiality in the transmission of the OTP password via mobile communication channels. The conducted research confirms that the application of the proposed procedures ensures the high speed of crypto-transformations comparable with the BSE, the provable cryptographic strength based on the complexity-theoretic problem of decoding a random code (10^{30}–10^{35} group operations are provided), and reliability based on the use of a shortened algebraic geometric code (P_{er} 10^{-9}–10^{-12} is provided). To further reduce the power of the alphabet – the Galois field to GF (2^4–2^6), it is proposed to use systems on flawed codes that allow simultaneously forming multi-channel cryptosystems.

References

1. Yevseiev, S. Construction of hybrid security systems based on the crypto-code structures and flawed codes [Text] / S. Yevseiev, O. Korol, H. Kots // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 4, Issue 9 (88). – P. 4–21. doi: 10.15587/1729-4061.2017.108461
2. Litvinov, V. A. Informacionnaya bezopasnost' vysshego uchebnogo zavedeniya v ramkah sovremennoy globalizacii [Electronic resource] / V. A. Litvinov, E. V. Lypko, A. A. Yakovleva // Available at: http://conference.osu.ru/assets/files/conf_reports/conf13/132.doc
3. Rose, S. Domain name systems-based electronic mail security [Text] / S. Rose, W. C. Barker, S. Jha, C. Irrechukwu, K. Waltermire. – U. S. Department of Commerce Penny Pritzker, Secretary, 2016. – 240 p. – Available at: https://nccoe.nist.gov/sites/default/files/library/sp1800/dns-secure-email-sp1800-6-draft.pdf
4. Dang, Q. Recommendation for Applications Using Approved Hash Algorithms [Text] / Q. Dang. – U. S. Department of Commerce, 2012. – 25 p. – Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
5. Shnayder, B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Text] / B. Shnayder. – Moscow: Triumf, 2012. – 815 p.
6. Grassi, P. A. Digital identity guidelines: authentication and lifecycle management [Text] / P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr et. al. – NIST, 2017. doi: 10.6028/nist.sp.800-63b
7. Barrett, M. The Cybersecurity Framework [Text] / M. Barrett, J. Marron, V. Y. Pillitteri, J. Boyens, G. Witte, L. Feldman. – NIST, 2017. – 41 p. – Available at: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

8. Cichonski, J. Guide to LTE Security [Text] / J. Cichonski, J. M. Franklin, M. Bartock. – NIST, 2016. – 48 p. – Available at: http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
9. Shapiro, L. Autentifikaciya na osnove odnorazovyh paroley. Teoreticheskie osnovy. Chast' 1 [Text] / L. Shapiro // Sistemnyy administrator. – 2012. – Issue 9. – P. 88–91.
10. Shapiro, L. Autentifikaciya i odnorazovye paroli. Chast' 2. Vnedrenie OTP dlya autentifikacii v AD [Text] / L. Shapiro // Sistemnyy administrator. – 2012. – Issue 10.
11. Kelsey, J. SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash [Text] / J. Kelsey, S. Change, R. Perlner. – NIST, 2016. doi: 10.6028/nist.sp.800-185
12. Yevseiev, S. P. Monitoring algorithm of two-factor authentication method based on passwindow system [Text] / S. P. Yevseiev, V. G. Abdullaev // Eastern-European Journal of Enterprise Technologies. – 2015. – Vol. 2, Issue 2 (74). – P. 9–16. doi: 10.15587/1729-4061.2015.38779
13. Yevseiev, S. P. Usovershenstvovanie metoda dvuhfaktornoy autentifikacii na osnove ispol'zovaniya modificirovannyh kripto-kodovyh skhem [Text] / S. P. Yevseiev, V. G. Abdullaev, Zh. F. Agazade, V. S. Abbasova // Systemy obrobky informatsyi. – 2016. – Issue 9 (146). – P. 132–144.
14. Yevseiev, S. Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system [Text] / S. Yevseiev, K. Hryhoryi, Y. Liekariev // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 6, Issue 4 (84). – P. 11–23. doi: 10.15587/1729-4061.2016.86175
15. Meyer, D. Time is running out for this popular online security technique [Electronic resource] / D. Meyer // FORTUNE. – 2016. – Available at: http://fortune.com/2016/07/26/nist-sms-two-factor/
16. Hackett, R. You're implementing this basic security feature all wrong [Electronic resource] / R. Hackett // FORTUNE. – 2016. – Available at: http://fortune.com/2016/06/27/two-factor-authentication-sms-text/
17. Bartock, M. Guide for cybersecurity event recovery [Text] / M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte, K. Scarfone. – NIST, 2016. doi: 10.6028/nist.sp.800-184
18. Security requirements for cryptographic modules [Text] // Change Notices. – 2001. doi: 10.6028/nist.fips.140-2
19. Annex A: Approved Security Functions for FIPS PUB 140-2 [Text]. – U. S. Department of Commerce, 2017. – Available at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf
20. Annex B: Approved Protection Profiles for FIPS PUB 140-2 [Text]. – U. S. Department of Commerce, 2016. – Available at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf
21. Annex C: Approved Random Number Generators for FIPS PUB 140-2 [Text]. – U. S. Department of Commerce, 2016. – Available at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf
22. 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
23. Mishchenko, V. A. Ushcherbnye teksty i mnogokanal'naya kriptografiya [Text] / V. A. Mishchenko, Yu. V. Vilanskiy. – Minsk: Enciklopediks, 2007. – 292 p.
24. Mishchenko, V. A. Kriptograficheskiy algoritm MV 2 [Text] / V. A. Mishchenko, Yu. V. Vilanskiy, V. V. Lepin. – Minsk, 2006. – 177 p.
25. Shennon, K. E. Teoriya svyazi v sekretnyh sistemah [Text] / K. E. Shennon // Raboty po teorii informacii i kibernetike. – Moscow: Il, 1963. – P. 333–402.