В роботі проводиться аналіз переваг і недоліків методів багатофакторної автентифікації, які використовуються в банківському секторі, розглядаються основні ризики їх використання, пропонується вдосконалений метод багатофакторної SMS-автентифікації на основі модифікованих (укорочених) крипто-кодових систем Нідеррайтера-Мак-Еліса. Розглядаються математичні моделі та основні протоколи шифрування/розшифрування в запропонованих модифікованих крипто-кодових системах

Ключові слова: багатофакторна автентифікація, модифіковані крипто-кодові системи, одноразові паролі OTP

В работе проводится анализ преимуществ и недостатков методов многофакторной аутентификации, рассматриваются основные риски их использования, предлагается усовершенствованный метод многофакторной SMS-аутентификации на основе модифицированных (укороченных) крипто-кодовых систем Нидеррайтера-Мак-Элиса. Рассматриваются математические модели и основные протоколы шифрования/расшифрования в предложенных модифицированных крипто-кодовых системах

Ключевые слова: многофакторная аутентификация, модифицированные крипто-кодовые системы, одноразовые пароли OTP

UDC 621.391
DOI: 10.15587/1729-4061.2016.86175

DEVELOPING OF MULTI-FACTOR AUTHENTICATION METHOD BASED ON NIEDERREITER-MCELIECE MODIFIED CRYPTO-CODE SYSTEM

S. Yevseiev
PhD, Associate Professor*
E-mail: serhii.yevseiev@hneu.net
H. Kots
PhD, Associate Professor*
E-mail: dekanstei@gmail.com
Y. Liekariev*
E-mail: yehorliekariev@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 Internet services in the banking sector in the process of development of electronic technology, functionality expansion of payment cards and remote banking channels (RB) put forward new requirements for providing basic security services (integrity, confidentiality, availability and authenticity) during conducting banking transactions. For authenticity in the financial sphere while creating Internet banking, mobile banking services, an electronic digital signature, based on a multifactor or extended authentication is usually used. It is based on a composite authenticator, physically separated, which greatly increases the safety of information using, at least from the side of users who connect to information systems via secure and non-secure communication channels. Among the multi-factor authentication methods, the method based on SMS authentication became widespread. However, their use carries significant security risks and requires the use of other, safer methods such as the use of one-time password generators (TOTP – Time-based One-time Password Algorithm) with additional cryptographic protection.

2. Literature review and problem statement

Two-factor authentication methods have been widely used in the last in various fields of communication technologies, related primarily to issues of identification and subject access to confidential information. They are entrusted by a large number of companies, including the organizations of the high-tech industry, financial and insurance sectors of the market, large financial institutions and public sector companies, independent expert organizations and research firms, 95 % of the banking sector institutions use multifactor or extended authentication while creating Internet banking and mobile banking services [1].

The SMS authentication method is based on the use of one-time password: the advantage of this approach compared with a permanent password is that the password cannot be reused. Even if we assume that an attacker could intercept the data during the information exchange, he cannot effectively use a stolen password to access the system [2]. The analysis [3] of the use of multi-factor authentication in online banking has shown that 97 % of respondents use passwords in the SMS-authentication, 91 % use mobile apps and daily 47 % of respondents use banking services through RB channels.

However, in a pre-release version of future Digital Authentication Guideline of the USA National Institute of Standards and Technologies (NIST), the SMS OTP mechanism originally is not intended for authentication and cannot be considered a full authentication factor. The document contains a direct reference to the fact that the use of SMS-messages for two-factor authentication may be "unacceptable" and "unsafe" [4].

The analysis [4–11] showed that the main concerns come down to the fact that the phone number can be linked to the

VoIP-service, in addition, attackers can try to convince the service provider that your phone number has changed, and similar tricks need to make impossible. The problem with the two-factor authentication has arisen due to the increasing popularity of smartphones and the desire of owners to synchronize data between different devices. Two-factor authentication relies on the principle of physical separation of devices for protection against malicious software. However, data synchronization makes this segmentation absolutely useless. Symantec's experts have reported a surge of activity of the Android Bankosy malware, able to steal codes for two-factor authentication. The malware intercepts one-time passwords needed for a successful two-factor authentication in banking applications [11].

One of the major disadvantages of the 2FA protocol is the transfer of OTP code via open channels of cellular communication and the possibility of obtaining by an intruder by introducing malicious software in mobile applications, which can lead to the destruction of the banking system as a whole (the theft of the bank customer's monetary assets). To eliminate this threat, [5] proposed to use an RSA asymmetric cryptosystem for OTP code security during transmission over open cellular channels, but this solution significantly reduces the processing speed due to the implementation of crypto-converting operations in an asymmetric cryptosystem. In addition, in [6, 7, 8] for OTP code security it is proposed to use crypto-converting methods (hashing or encryption with provable resistant cryptosystems) or QR codes. However, new attacks discussed in [9, 10] show their complexation (association) with the methods of social engineering, shortcomings in the synchronization systems of Internet gadgets used in electronic banking – due to the increasing popularity of smartphones and the desire of owners to synchronize data between various devices there is no basic principle of physical separation of devices for protection against malicious software. Symantec's experts have reported a burst of activity of the Android Bankosy malware, able to steal codes for two-factor authentication. The malware intercepts one-time passwords, needed for a successful two-factor authentication in the banking applications [11].

Thus, the development of computer technology, the emergence of new areas of threats associated with Internet technologies, cyberspace, their complex application with the methods of social engineering make demands to explore new scientific and technological approaches to improve the methods of SMS authentication based on the synergetic threat model proposed in [12]. Improvement of multi-factor authentication method based on modified crypto-code systems using modified algebraic codes is a promising direction in solving the problem of privacy and reliability when transferring the OTP password over open mobile channels.

3. The aims and objectives of the study

The aim is to analyze the main methods of multi-factor authentication used in automated banking systems, ABS hacking threats based on electronic banking; an improved method of two-factor authentication through SMS messages on the basis of the Niederreiter-McEliece modified crypto-code systems (MCCS), the development of algorithms for encryption/decryption in the MCCS proposed to eliminate the disadvantages of the 2FA protocol based on SMS messages.

To achieve the goal, let us consider the following tasks:

– analysis of the main methods of multi-factor authentication, the 2FA protocol hacking threats through SMS messages;

– development of the structural scheme of the protocol of two-factor authentication through SMS messages using the Niederreiter-McEliece MCCS;

– development of practical algorithms for encryption and decryption of data in the Niederreiter-McEliece MCCS to reduce their energy capacity and the possibility of implementation in digital telephony.

4. An analysis of the main methods of two-factor authentication, assessment of the main threats on the basis of the synergetic threat model

Two-factor authentication or 2FA is a user identification method in a service where two different types of authentication data are used. The introduction of an additional level of security provides better protection for your account against unauthorized access. Using this type of 2FA, the user enters personal password at the first authentication level. The next step, he must enter the OTP token *(OTP – One-time Password Algorithm)*, usually sent via SMS to his mobile device. The OTP will be available only to those who, as supposed in theory, entered a password, inaccessible to unauthorized persons-[1, 4]. General classification of multi-factor authentication methods is shown in Fig. 1 [13]. The analysis [14-18] of multifactor authentication methods showed the following main advantages and disadvantages:

– The advantages of the *methods based on SMS notification* are generation of the OTP code every time you log in and transmission through an additional channel, interception of the user's login and password in the main channel will not lead an attacker to client banking information. Binding of the OTP password to the customer's phone number. The main disadvantages are that the use of mobile open channel does not allow to ensure the confidentiality of the OTP code, using only cellular channels leads to a "loss" of two-factor authentication. There is a theoretical possibility of substitution of numbers the help of an operator or employees of mobile phone shops.

– The use of methods with applications-authenticators (QR Codes) allows you to have multiple accounts in a single authenticator and generate a primary key, there is no need to use a cellular communication lines, the generation of OTP passwords based on the cryptographic algorithms. The main disadvantages are the use of an authenticator on the device of entrance leads to the "loss" of two-factor authentication, an attacker access to the primary key of the user leads to the authentication system cracking.

– *Checking login via a mobile application* allows you to automate the authentication process without user interaction, based on verification of the personal authentication key on the mobile application. The main disadvantages are: the loss/disclosure of the private key results in the authentication system cracking, the possibility of receiving SMS messages by synchronization between the iPhone and the Mac, the use of the authenticator on the device; of entrance leads to the "loss" of comprehensiveness.

– *The physical (or hardware) tokens* are the most reliable method of two-factor authentication. Most often, they are presented in the form of a USB stick with its own

processor, generating cryptographic keys, which are automatically entered when you connect to a computer. The advantages are the absence of the need to use additional mobile applications, software, tokens are completely independent devices. Disadvantages include – multiple accounts lead to "binding" of tokens, not supported by all applications.

– *Backup keys* are the fall-back option in case of loss/theft of the smartphone, which receives one-time passwords or verification codes. Loss/theft of the backup key leads to the destruction of sensitive authentication system.

– *Barcodes of Passwindow system* provide unique static images of the sequence of symbols generated dynamically by the authentication server without the use of cryptographic algorithms. Any interference or tampering with the bar code is passively presented to the user in the form of combinations in a template that do not match the expectations. A significant disadvantage is the possibility of selecting a unique card barcode, proposed in [14].

– Using of *biometrics* as a secondary identification factor is performed by identifying the physical characteristics of a person (fingerprint, iris, etc.). The advantages of the methods include the use of a person's unique physiological characteristics, the absence of additional mobile applications and software. A significant disadvantage is the specific requirements for software and hardware devices of reading the user's biometric data.

Thus, multi-factor authentication systems based on one-time e-mail- or SMS-passwords and different types of tokens are generally used in automated banking systems. To ensure confidentiality of OTP codes, transmitted by the bank, in the remote banking standard, it is necessary to use the encrypted and operator-independent channel of their delivery. This approach is not affected by the majority of known threats, except for social engineering, exploiting the human factor.

Fig. 2 shows a synergetic approach to the classification of multi-factor authentication threats. The synergetic model [12] of threats to banking information provides necessary and sufficient conditions for the development of a new methodology aimed at achieving synergies in the field of security of public and private banking protection systems.

The analysis of threats based on a synergistic approach to threat assessment has shown that today attackers use an integrated approach to obtaining banking user's personal data, based on a combination of social engineering techniques with traditional disguise and infiltration methods. New types of cyber-attacks are also used to effectively embed malware on mobile communication devices, which in turn leads to a decrease in the profitability of multi-factor authentication methods on the basis of SMS messages and OTP passwords in automated banking systems (ABS).

Thus, there is a need for additional means to ensure the confidentiality of information transmission in cellular communication systems.

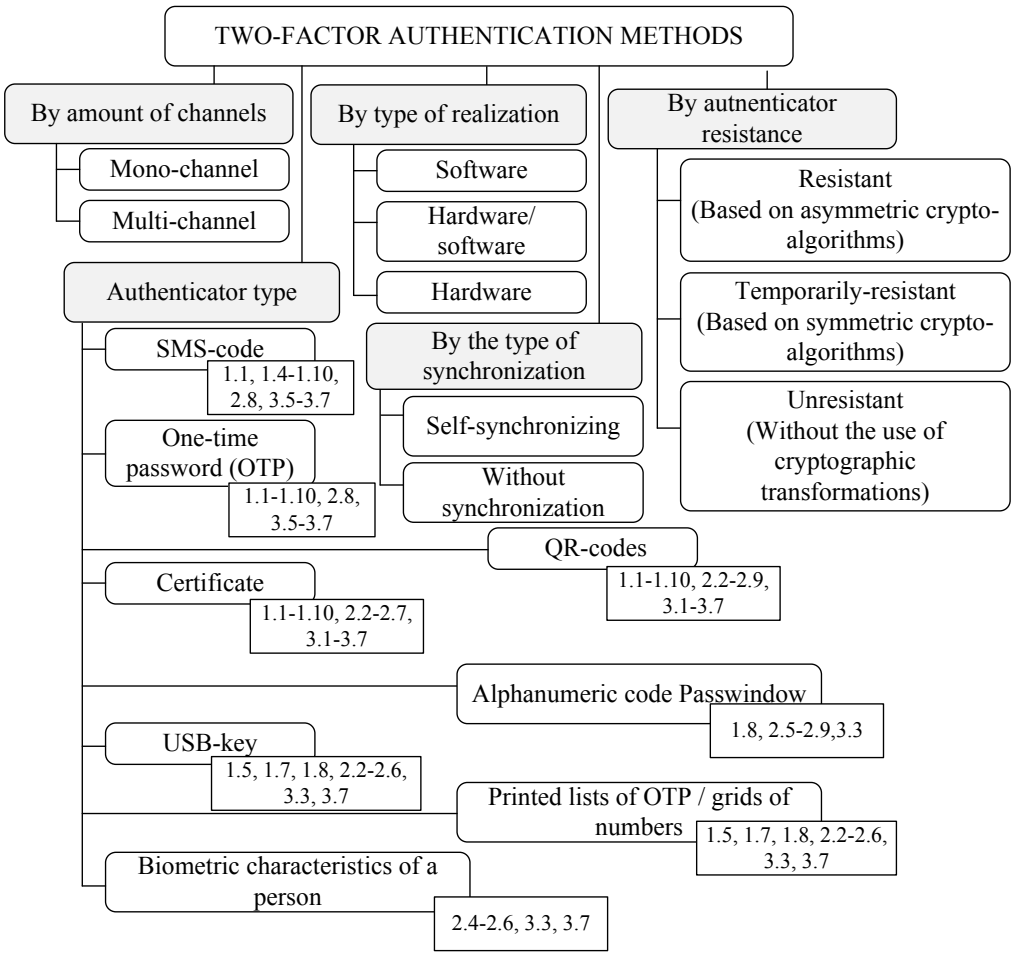


Fig. 1. Classification of multi-factor authentication methods

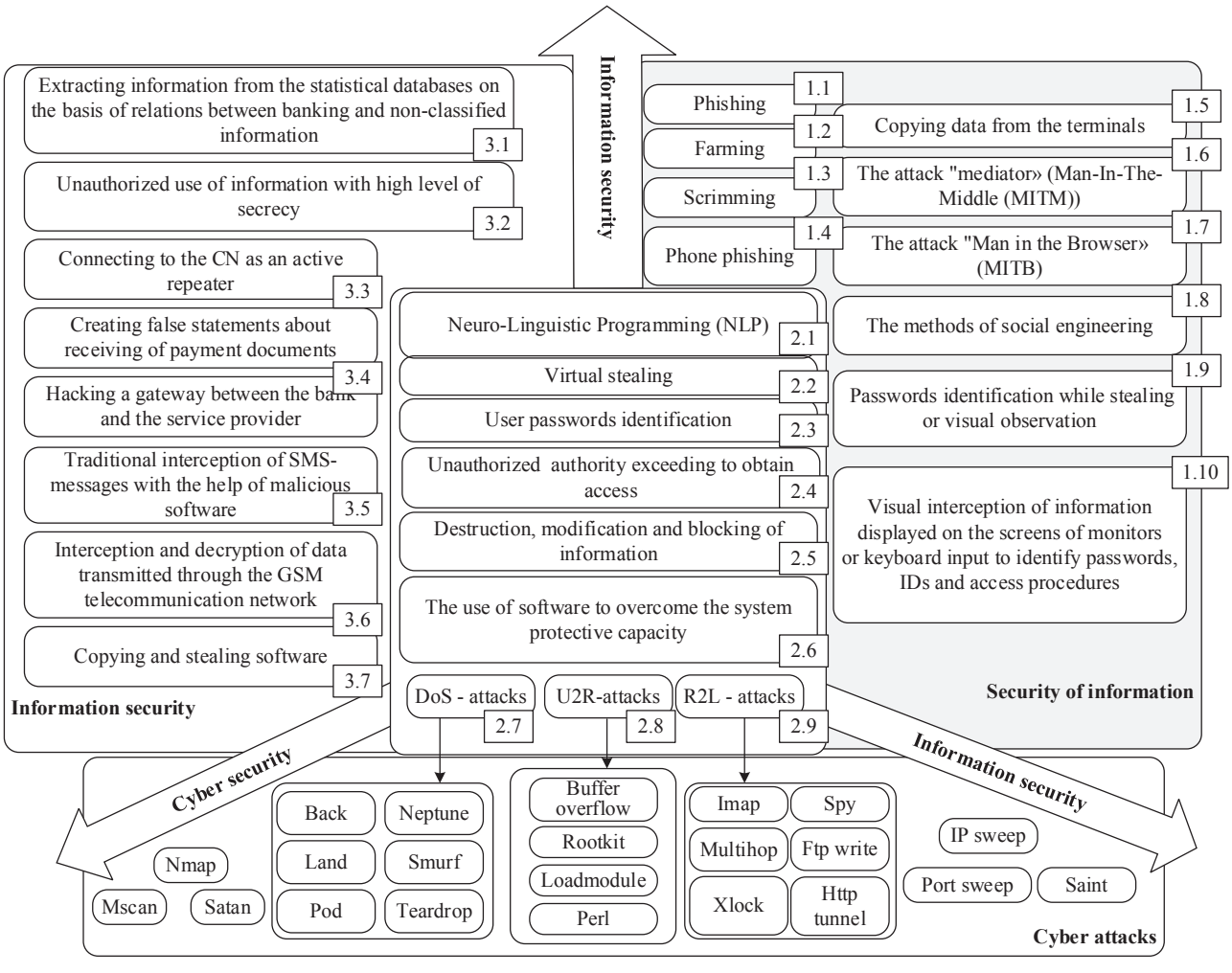


Fig. 2. Synergetic model of banking information security threats

5. Development of multi-factor authentication protocol based on SMS messages using the Niederreiter-McEliece MCCS

Identification of *SMS systems* or multi-factor authentication systems based on mobile phones is wrong, a more precise term is an "out-of-band" authentication. However, with the spread of GSM, smartphones and tablets connected to the network, even this security advantage can be lost if the user transaction authentication is performed on the mobile device. In addition, the growth of unwanted software for mobile devices now allows an attacker to gain access to authentication codes sent via SMS not only through the traditional interception with the help of malicious software. Experts explain their decision by the fact that the SMS security faces new challenges with the introduction of VoIP services. Some of these services allow to hack the SMS system. NIST recommends developers to validate the use of VoIP connections before applying the SMS-based two-factor system. SMS protocol is considered unsafe [8]. The analysis of Internet attacks on multi-factor authentication schemes with SMS messages and advantages of crypto-code systems make it possible to improve the multi-factor authentication scheme to enhance reliability and validity of the generated authenticator.

For this, a bank card (BC) must keep the following data elements [13]:

1. Certification authority public key index – since a terminal can work with multiple CAs, this value specifies which of the keys should be used by the terminal when working the given card.

2. Issuer public key certificate signed by the appropriate certification authority.

3. BC public key certificate is signed by the issuer and is based on the McEliece MCCS.

4. Issuer public key modulus and exponent.

5. BC public key modulus and exponent.

6. Banking card private key.

The terminal that supports the multi-factor authentication scheme must keep the public keys of all CAs and associated information relating to each of the keys.

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

To support multifactor authentication, user banking card (BC) should have a personal key pair (public and private authenticator keys). The BC public key is stored on BC in its public key certificate. Each BC public key is certified by its issuer, and a trusted certification authority certifies the issuer public key. This means that to verify the authenticator card, the terminal must first verify two certificates in order to restore and authenticate the BC public key, which is then used for the BC authenticator verification.

The process of the proposed authentication consists of four stages:

1) Restoring the certificate authority public key by the terminal. The terminal reads the index (1), identifies and retrieves the certificate authority public key modulus – disguising matrix (*X, P, D), curve equations for algebrogeometric code (AGC)*, and associated information, stored in it, selects the necessary algorithms.

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

3) Forming an authenticator on the basis of using the McEliece MCCS. Obtaining a codeword (an authenticator) based on the use of the crypto-code system by adding the received codeword with a session key.

4) Validation of the authenticator. Finding the multiplicity of the error vector and the comparison with the obtained one. The structure of the proposed method of two-factor authentication based on the Niederreiter-McEliece MCCS is shown in Fig. 3.

In the authors' opinion, the significant advantage of using this multifactor authentication scheme is providing of required cryptographic resistance and reliability indexes of transmitted transactions with the use of Niederreiter-McEliece modified asymmetric crypto-code systems. The proposed mechanisms to ensure privacy: the transfer of SMS messages via cellular mobile communication channels with the Niederreiter MCCS (ensures the privacy of the OTP code) and the use of the McEliece MCCS in ABS digital channels (provides the OTP password transmission accuracy and confidentiality) would physically separate channels used for generating the banking transaction authenticator.

Using the session key at each transaction, the physical separation of the authenticator data transmission channels, scalability of the software module by changing the Niederreiter-McEliece MCCS parameters, depending on the error rate in the used ABS communication channels will allow physical separation of transmission of the OTP-code of composite authenticator by the use of the two MCCS schemes in different communication channels and the required level of the 2FA protocol security in electronic banking applications.

6. Developing of MCCS mathematical models and encryption/decryption algorithms

Let us consider protocols of building modified crypto-code systems, used in two-factor authentication protocols. The simplest and most convenient method of modifying a linear block code, which doesn't reduce minimal code distance, is shortening by reducing the information symbols [19–21].

To construct Niederreiter-McEliece modified crypto-code systems, a trusted certificate authority calculates code parameters, and error probability functions, block diagrams of the code parameters calculation function and performance of the given function are shown in Fig. 4, 5, accordingly.

In [22], the basic statements and parameters of constructing a modified crypto-code system on the modified (shortened) codes are considered. Let $I=(I_1, I_2, ..., I_k)$ – information vector (n, k, d) of the block code. We choose the information symbols subset h, $|h|=x$, $x\leq ½k$. We place the information vector I in a subset of h zeros, i. e. $I_i=0, \leftrightarrow I_i \in h$. At other positions of the vector; I, we place information symbols. When encoding the information vector, symbols of the set h are not involved (they are null) and can be discarded, and the resulting code word is shorter by x code symbols.

For modifications (shortening) of elliptic codes, we will use reduction of the set of the curve points. The following statements are true.

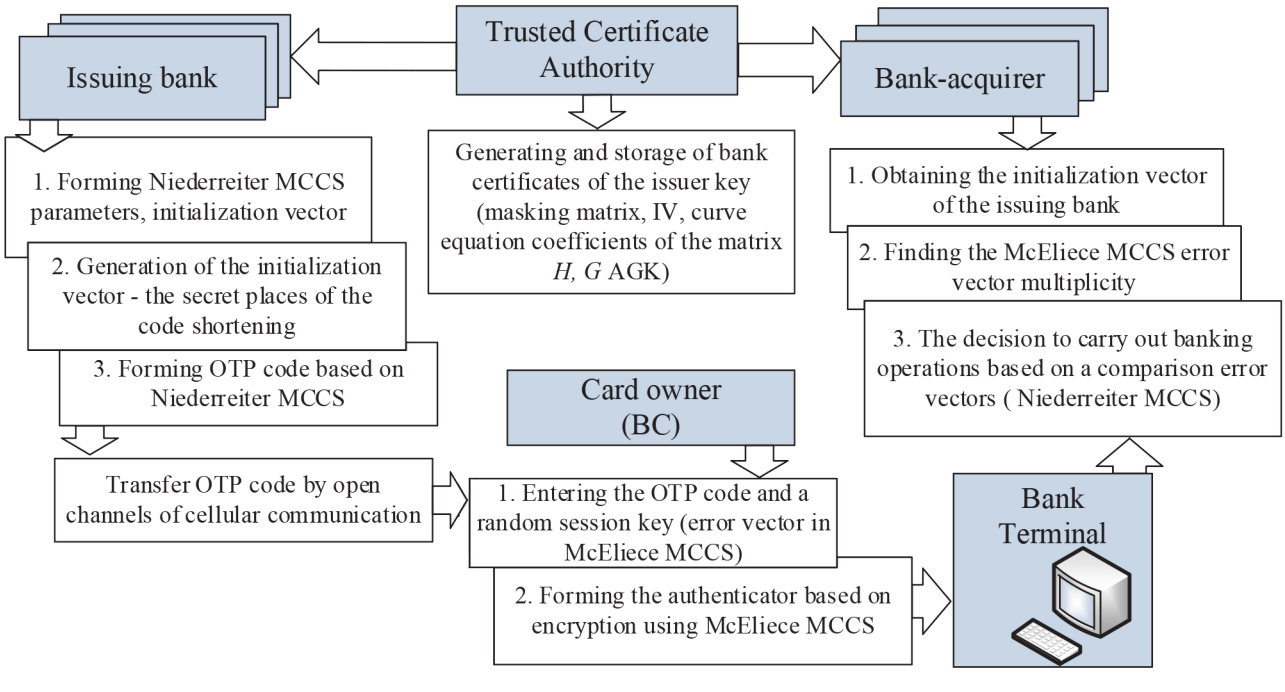


Fig. 3. Protocol structural diagram of the improved method of SMS authentication based on the Niederreiter-McEliece MCCS

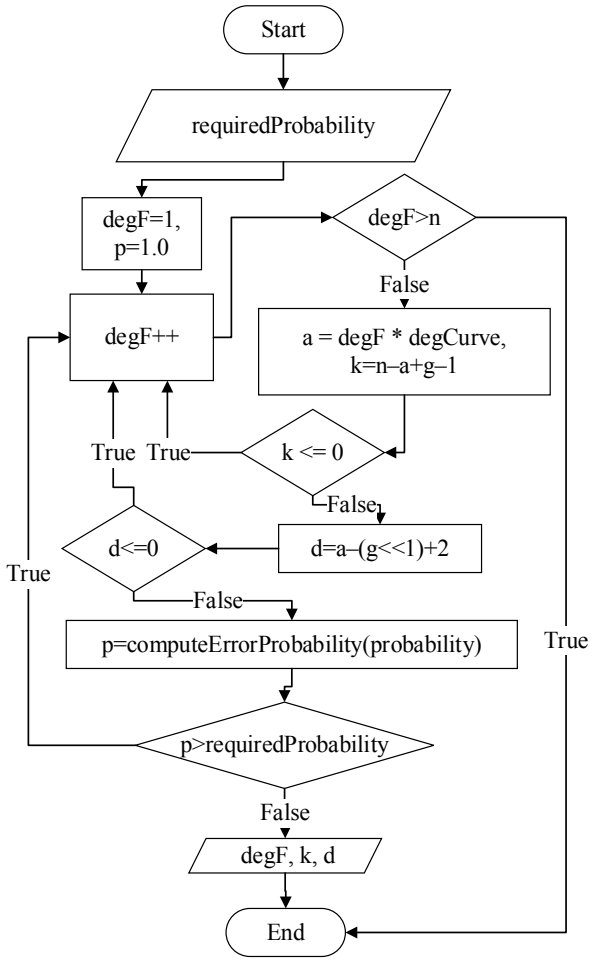


Fig. 4. The block-diagram of the code parameters calculation function: requiredProbability – given probability of block distortion; n – total number of symbols in the code (code length); k – the number of information symbols; d – minimum distance of code combinations by Hamming; g – curve type; degF – generating function degree; degCurve – curve degree

Statement 1. Let EC – elliptic curve over GF(q), g=g(EC) – curve type, EC(GF(q)) – the set of its points over a finite field, N=EC(GF(q)) – their number.

Let X and h – nonintersecting subsets of points, X∪h=EC(GF(q)), |h|=x.

Then shortened elliptic (n, k, d) code over GF(q), built through the projection $\varphi: X \to P^{k-1}$, is bound by characteristics k+d≥n, and:

$$n = 2\sqrt{q} + q + 1 - x, \; k \geq \alpha - x, \tag{1}$$

$d \geq n - \alpha$, $\alpha = 3 \times degF$.

Statement 2. Shortened elliptic (n, k, d) code over GF(q), built through the projection of type $\varphi: X \to P^{r-1}$, is bound by characteristics k+d≥n, and:

$$n = 2\sqrt{q} + q + 1 - x, \; k \geq n - \alpha, \tag{2}$$

$d \geq \alpha$, $\alpha = 3 \times degF$.

Using the result of statement 1, we set the McEliece modified crypto-code system on modified elliptic codes, built through the projection of type $\varphi: X \to P^{k-1}$, on the basis of statement 2 – Niederreiter modified crypto-code system, built through the projection $\varphi: X \to P^{r-1}$. The following statements are true, which define the basic parameters of the McEliece and Niederreiter MCCS, accordingly.

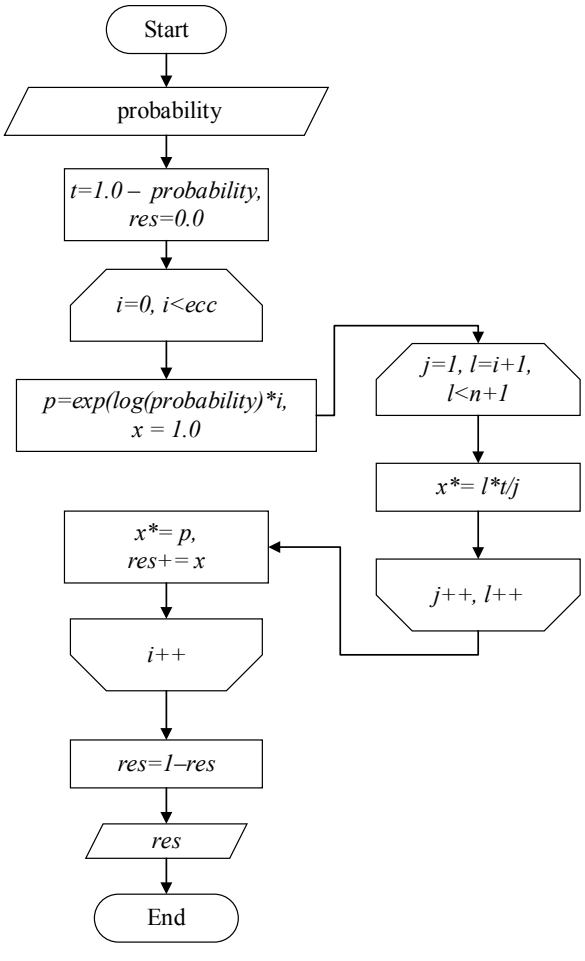


Fig. 5. The function of calculating the probability of error for the given parameters of the code: probability – probability of one symbol distortion; n – total number of symbols in the code (code length); ecc – the number of errors corrected by the code

Statement 3. Shortened elliptic (n, k, d) code over $GF(2^m)$, built through the projection of type $\varphi: X \to P^{k-1}$, defines McEliece modified crypto-code system with the parameters:

$$l_{k+} = x \times \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil, \tag{3}$$

$$l_I = (\alpha - x) \cdot m; \tag{4}$$

$$l_s = \left(2\sqrt{q} + q + 1 - x\right) \times m; \tag{5}$$

$$R = \left(\alpha - x\right) / \left(2\sqrt{q} + q + 1 - x\right). \tag{6}$$

Statement 4. Shortened elliptic (n, k, d) code over $GF(2^m)$, built through the projection of type $\varphi: X \to P^{r-1}$, defines the Niederreiter modified crypto-code system with the parameters:

– the secret key dimension is given by (3);

– the information vector dimension (bits):

$$l_1 = \left(2\sqrt{q} + q + 1 - \alpha\right) \times m, \quad (7)$$

– the codegram dimension is given by (5);
– the relative transmission rate:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(\left(2\sqrt{q} + q + 1 - x\right)\right). \quad (8)$$

Practical algorithms of formation and decryption/decoding of cryptograms/codegrams in a modified asymmetric crypto-code system on the basis of McEliece TCS on elliptic truncated codes are given in [22]. To construct a modified crypto-code Niederreiter system, we use basic algorithms of encryption/decryption of the system, discussed in [23]. Fig. 6 shows a block diagram of the Niederreiter MCCS, the main difference of which from the known–is the use of the mechanism of shortening the error vector symbols after the equilibrium coding algorithm, which will reduce the capacity of the used GF (q) and energy capacity of the computing system in general.

Analysis of the practical implementation of code-converting algorithms in Niederreiter MCCS shows that when forming the codegram based on the initialization vector, shortening is performed – h_e (error vector symbols equal to zero), $|h|=1/2e$, i. e. $e_i=0$, $\leftrightarrow e_i \in h$.

When decryption of the cryptogram (after receiving the error vector, before using the equilibrium encryption algorithm) to obtain information "zero" shortening symbols are introduced. Algorithms for encryption and decryption are shown in Fig. 7, 8, accordingly.

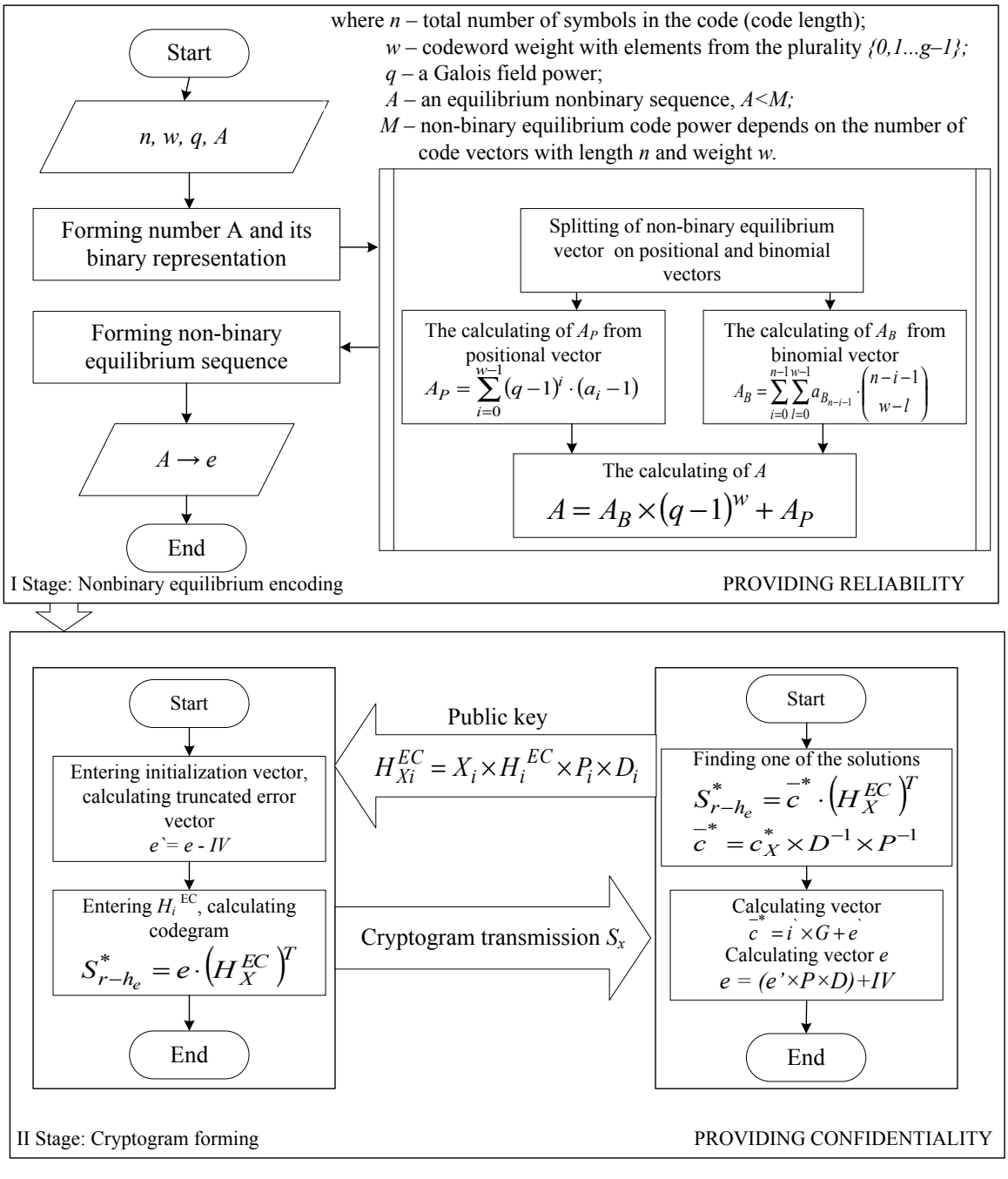
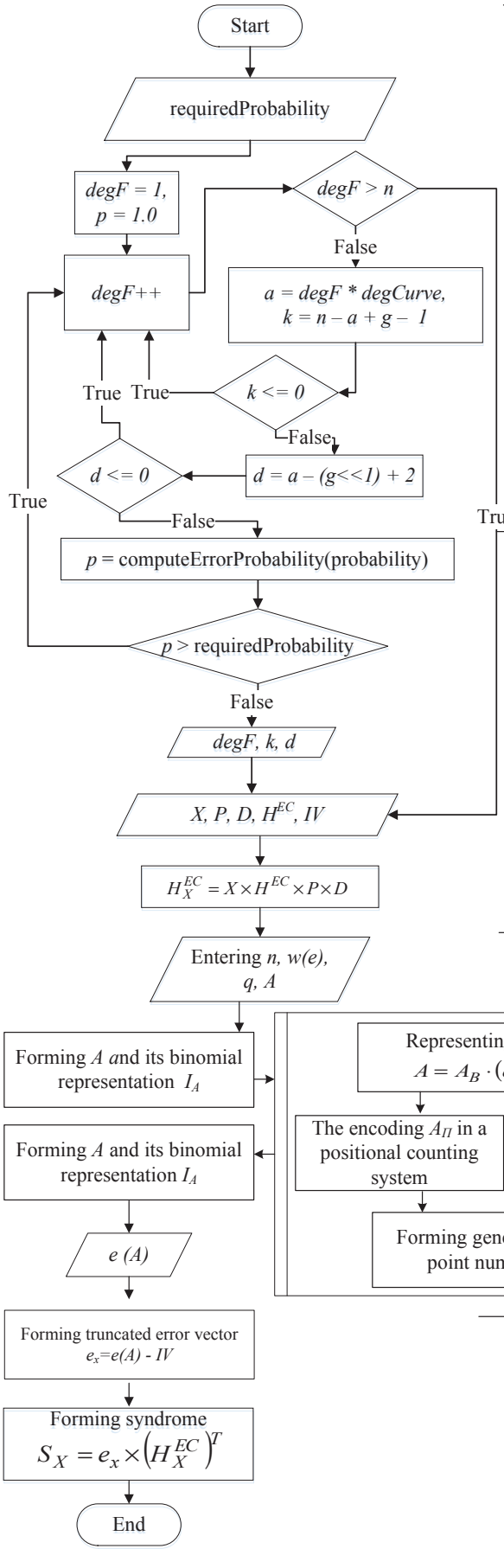


Fig. 6. Structural diagram of a modified Niederreiter CCS



Stage 1. Set code parameters

requiredProbability – given probability of block distortion,
n – the total number of symbols in the code (code length)
k – number of information symbols,
d – the minimum distance of code combinations by Hamming,
g – the genus,
degF – the degree of generating function,
degCurve – the degree of curve.

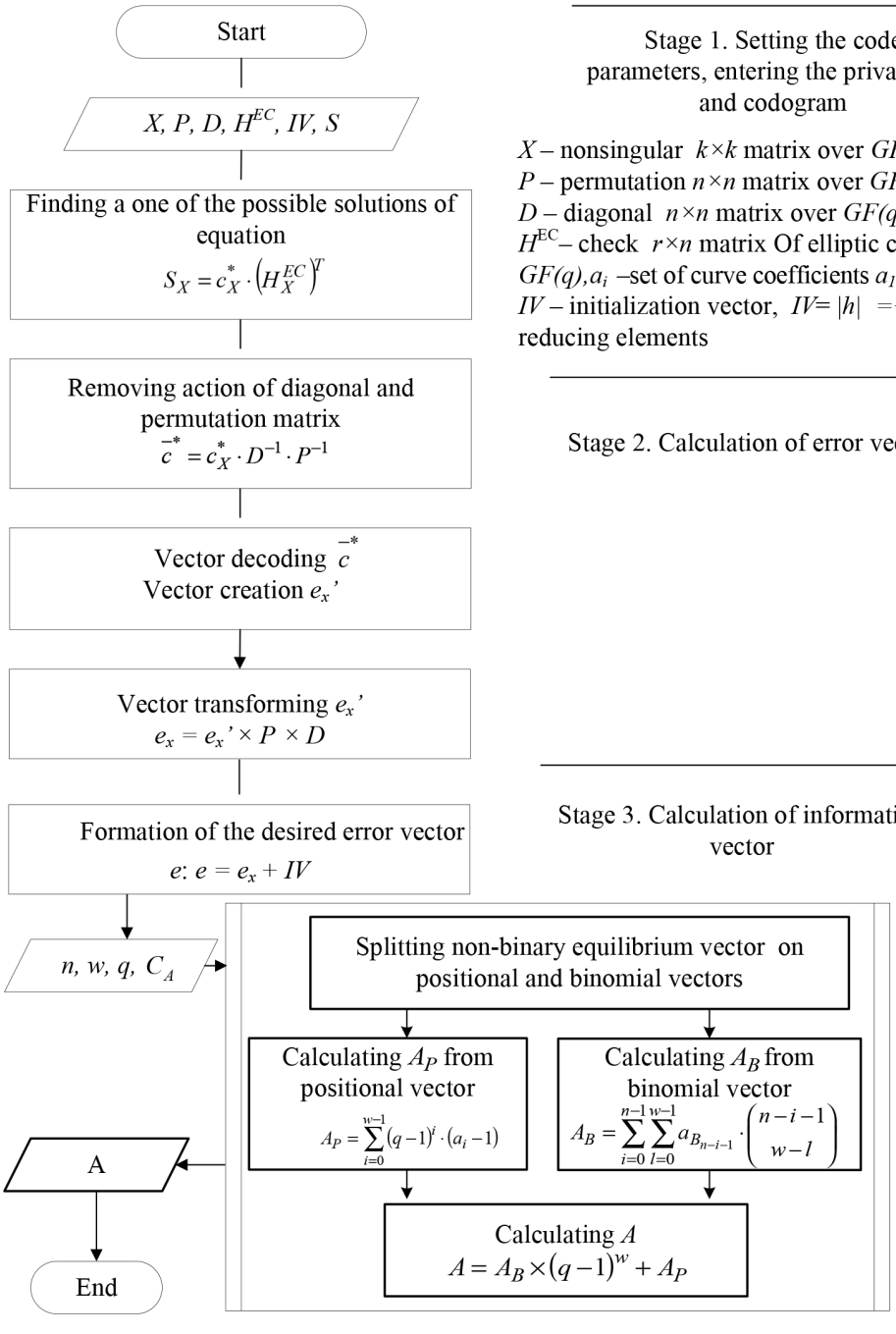
Stage 2. Forming the error vector (equilibrium coding), of the public key

X – non-singular k × k matrix over GF (q),
F – n × n permutation matrix over GF (q),
D – n × n diagonal matrix over GF (q),
NEC– checking r × n matrix of the elliptic code over GF (q),
ai – a set of coefficients of the polynomial curve a1 ... a6,
IV – initialization vector, IV = | h | = ½ shortening elements

Stage 3. Forming error vector

Stage 4. Forming syndrome
Syndrome goes to the communicational channel

Fig. 7. The algorithm for generating the cryptogram in the Niederreiter MCCS



Stage 1. Setting the code parameters, entering the private key and codogram

X – nonsingular $k \times k$ matrix over $GF(q)$,
P – permutation $n \times n$ matrix over $GF(q)$,
D – diagonal $n \times n$ matrix over $GF(q)$,
H^{EC} – check $r \times n$ matrix Of elliptic code over $GF(q)$, a_i –set of curve coefficients $a_1 \ldots a_6$,
IV – initialization vector, $IV = |h| = ½\ h_e$ – reducing elements

Stage 2. Calculation of error vector

Stage 3. Calculation of information vector

Fig. 8. The algorithm for cryptogram decryption in the Niederreiter MCCS

The algorithm for generating the cryptogram in the Niederreiter MCCS is represented as a sequence of the following steps:

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

Step 2. Forming the error vector e, the weight of which is not more than $\leq t$ – correcting ability of the elliptic code based on the algorithm of non-binary equilibrium coding [23].

Step 3. Forming the truncated error vector

$e_x = e(A) - IV$.

Step 4. Forming the codegram $S_X = e_x \cdot \left(H_X^{EC}\right)^T$.

The algorithm for decoding the codegram in the Niederreiter MCCS is represented as a sequence of the following steps:

Step 1. Entering the codegram S_X, to be decoded. Entering the private key – matrixes X, P, D.

Step 2. Finding one of the possible solutions of the equation:

$$S_X = c_X^* \cdot \left(H_X^{EC}\right)^T.$$

Step 3. Removing the influence of diagonal and permutation matrixes:

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}.$$

Step 4. Decoding of the vector $\overline{c}^*$. Forming the vector e'_x.

Step 5. Converting the vector e'_x:

$e_x=e'_x\times P\times D$.

Step 6. Forming the desired error vector e:

$e=e_x+IV$.

Step 7. Transforming the vector *e* based on using the non-binary equilibrium code into information sequence.

A formal description of the mathematical model of the McEliece MCCS on modified (shortened) codes is considered in [22].

Let us consider the formal description of a modified asymmetric crypto code Niederreiter system through the use of the modified elliptical codes.

A mathematical model of the NCCS with using of the Niederreiter TCS based on shortening (reducing of information symbols after converting in the error vector in the algorithm of non-binary equilibrium coding) is formally given by the combination of the following elements [22, 23]:

– a set of open texts

$$M=\left\{M_1,M_{2,}...M_{q^k}\right\},$$

where

$$M_i=\left\{e_0,e_{h_1,}...e_{h_k},e_{e-1}\right\},\quad \forall e_e\in GF(q),$$

h_e – symbols of the error vector equal to zero, $|h|=\frac{1}{2}e$, i. e. $e_i=0$, $\leftrightarrow e_i\in h$;

– a set of private texts *(codegrams)*

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

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 numerous mappings based on using of public key – check matrix of 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 the private (personal) key – disguising matrix)

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

where

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

– a set of keys, parametrizing direct mapping (the 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 $H^{EC_i}_{X_{a_i}}$ – check r×n matrix of algebrogeometric block (n, k, d) code, disguised as random code with elements from GF(q) i. e.

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

a_i – a set of coefficients of the polynomial of the curve $a_1...a_6$, $\leftrightarrow a_i\in GF(q)$, clearly defining a specific set of points on the curve in space P^2.

– a set of keys, parametrizing reverse mapping (personal (private) key of the authorized user)

$$KR=\left\{KR_1,KR_2,...,KR_r\right\}=$$
$$=\left\{\left\{X,P,D\right\}_1,\left\{X,P,D\right\}_2,...,\left\{X,P,D\right\}_r\right\},$$

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

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

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

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

Initial data in the description of the considered modified crypto-code information protection system are:

– algebra-geometric block (n, k, d)-code over GF(q);

– w – weight of codeword with elements from the set {0,1...g–1}, q – power of the Galois field, n – error vector length; A – non-binary equilibrium sequence, A<M; M – power of non-binary equilibrium code defined by the number of vectors of length n and weight w;

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

– IV – initializing vector, IV=|h|=½ h_e – reducing elements (h_e –error vector symbols equal to zero, |h|=1/2e, i. e. $e_i=0$, $\leftrightarrow e_i\in h$);

– disguising matrix mappings, given by a set of matrixes $\left\{X,P,D\right\}_i$, where X – nondegenerate k×k matrix over GF(q), P – permutation n×n matrix over GF(q) with one non-zero element in each line and each row of the matrix, D – diagonal n×n matrix over GF(q) with non-zero elements on the main diagonal.

In the modified Niederraiter crypto-code system on modified (truncated) algebra-geometric (n, k, d)-codes, the information vector is converted in fast algorithm of non-binary equilibrium coding into the error vector. After the operation; of shortening, the error vector is disguised as a random syndrome by multiplying the truncated error vector by the public key of the recipient (the check matrix H^{EC}_X of the code):

$$KU_{a_i}=H^{EC}_X=X^i\times H^{EC}\times P^i\times D^i, i\in\left\{1,2,...,r\right\}.$$

Communication channel receives

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

On the receiving side, an authorized user who knows the disguise rule, the initialization vector (the number and places of zero characters in the error vector) can use a fast algebra-geometric decoding algorithm (polynomial complexity) to recover the plaintext:

$$M_i = \varphi_i^{-1}\left(S^*_{r-h_e}, \{X,P,D\}_i\right).$$

To restore the plaintext, an authorized user searches for one of the solutions of equations:

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

"Undisguises" the codeword, obtained in the previous step

$$\bar{c}^*_X = \bar{c}^* \times D^{-1} \times P^{-1},$$

decodes the obtained vector by the Berlekamp-Massey algorithm [19–21], forms the error vector according to the Chen procedure e'_x, transforms into the vector e'_x by multiplying the previous result of the error vector by disguising matrixes P, D:

$$e_X = e'_x \times P \times D.$$

Forming of the desired error vector e to convert into information vector based on a fast algorithm of non-binary equilibrium coding:

$$e = e_X + IV.$$

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

Thus, modified Niederreiter crypto-code system is presented, which allows to reduce the energy capacity of the group operations, by shortening symbols in the error vector (reducing the syndrome symbols and power of the used Galois field), to increase the entropy of characters of closed texts, transmitted to the communication channel and thus provide the required cryptographic resistance.

7. Discussion of the results

Let us conduct the research of energy costs of implementation of crypto-code information protection means based on the McEliece MCCS on modified (truncated) elliptic codes.

To estimate the time and speed parameters, it is common to use the unit of measurement cpb, where cpb (cycles per byte) – the number of CPU cycles, which should be spent for processing 1 byte of incoming information.

The complexity of the algorithm, is calculated from the expression

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

where Utl – processor core utilization (%); Rate –algorithm throughput (bytes/sec).

Table 1 shows the results of the research of the dependence of the code sequence length of algebra-geometric code in the McEliece MCCS on the number of processor cycles for performing elementary operations in the crypto-code system software implementation.

Table 1

The dependence of the code sequence length on the number of processor cycles

Code sequence length		McEliece on shortened codes			McEliece		
		10	100	1000	10	100	1000
The number of function calls for elementary operations	Symbol reading	10294397	28750457	76759874	11018042	30800328	80859933
	Lines comparison	3406921	9246748	25478498	3663356	10199898	26364634
	Lines concatenation	1705544	5045748	12379422	1834983	5125564	13415329
Total		15406862	43042953	114617794	16516381	46125790	120639896
Duration of the function * in CPU cycles	Symbol reading	295374	810478	2001167	297487	831609	2183218
	Lines comparison	178814	531379	1248684	197821	550794	1423690
	Lines concatenation	544990	1328114	3586486	544990	1522293	3984353
Total		1006781	2749548	7247488	1040298	2904696	7591261
Duration ** in msec		0.52	1.37	3.4	0.55	1.53	4

*Notes: * duration of 1000 operations in processor cycles: symbol reading – 27 cycles, lines comparison – 54 cycles, lines concatenation – 297 cycles; ** the processor with a clock speed of 2 GHz, taking into account the 5 % operating system loading was taken for the calculation*

Table 2 shows the results of the research of estimation of time and speed parameters of the procedures of forming and decoding information in asymmetric crypto-code systems based on the McEliece MCCS.

Table 2

Estimation of time and speed parameters in data conversion procedures

Parameters	Code sequence length	Rate (bytes/sec)	Processor core utilization (%)	Per (cpb)
The number of function calls for elementary operations	100	46 125 790	56	61.5
	1000	120 639 896	56	62.0

The analysis of Tables 1, 2 suggests a significant energy cost of implementation of non-symmetric crypto-code systems in the protocols of communication systems and technologies, which greatly complicates their usage. To eliminate the disadvantage, it is proposed to use MCCS based on error-correcting codes modification, which reduces energy consumption and volumes of key user data by storing the data on the coefficients of the elliptic curve in an affine space for the construction of the corresponding matrices (private and public keys).

The mathematical model, practical encryption/decryption algorithms of the cryptogram/codegram, modified

Niederreiter crypto-code system, describing the sequence of the transformation of the input sequence of plaintext into ciphertext (syndrome vector) are proposed. Use of shortening algorithms can reduce the energy capacity and provide the required cryptographic resistance during data transmission over open cellular channels.

The developed multi-factor authentication scheme based on the McEliece-Niederreiter MCCS eliminates a significant disadvantage of 2FA on the basis of SMS messages – providing the confidentiality of the OTP password transmission via cellular channels The investigations confirm that their application provides high performance at the level of use of symmetric encryption algorithms with BSE, provable cryptographic resistance based on the theoretical and complexity problem of random code decoding (10^{30}–10^{35} group operations are provided), and reliability based on the use of a truncated algebrogeometric code (P_{er} 10^{-9}–10^{-12} are provided). To eliminate the main disadvantage of such crypto-code systems – large amounts of key data (to provide the required cryptographic strength it is necessary to build a system in the field GF (2^{10}–2^{13})) – the paper proposes to use shortened codes, which reduces the power of the Galois field to GF (2^6–2^7), and keeps the cryptographic resistance level. The use of methods of error vector shortening introduces an additional entropy in the arrangement of symbols of the initialization vector, which allows to improve the reliability of transmitted data.

A promising direction for further research is to assess the reliability and reduce energy costs of the Niederreiter MCCS and software layout for multi-factor authentication as a whole.

8. Conclusions

1. The analysis of multi-factor authentication methods showed that in the automated banking systems, 95 % of bank customers use electronic banking based on multi-factor SMS authentication. However, in recent years the development of computing capabilities of intruders, aggregation of threats with the use of social engineering mechanisms, the emergence of cyber threats, significant shortcomings in ensuring the cellular protocol safety makes it impossible to provide guaranteed security when using multi-factor authentication based on physical separation of the channels of transmission of the authenticator components. This is confirmed by a recent study of the USA NIST experts, as well as leading experts in the field of banking sector safety.

2. The mathematical model, practical algorithms of encryption/decryption of the cryptogram/codegram in modified crypto code Niederreiter system, describing the sequence of the transformation of the input sequence of plaintext into ciphertext (syndrome vector) are proposed. The proposed algorithms differ from known by error vector symbol shortening while forming the syndrome and providing the required cryptographic resistance during data transmission through open cellular channels while reducing the energy capacity of group operations.

The proposed modification algorithms in the Niederreiter and McEliece MCCS allow, without sacrificing the reliability, to ensure their practical implementation in multi-factor authentication. This provides cryptographic resistance of the OTP composite authenticator code, transmitted through open cellular channels.

3. The developed multi-factor authentication scheme based on the Niederreiter-McEliece MCCS eliminates the significant disadvantage of 2FA based on SMS messages – ensuring the confidentiality of the OTP password transmission via cellular channels. The studies of Niederreiter and McEliece modified crypto-code systems on elliptic codes confirm their possibility of integrated providing (by one device) reliability and security of transmitted data. In MCCS, it is proposed to use algebrogeometric interference-resistant code on elliptic curves with the probability of error P_{er} 10^{-9}–10^{-12}, and security of cryptosystems is based on the intractable problem – the decoding of the random (n, k, d)-code (10^{30}–10^{35} group operations are provided), at speed of encryption comparable with rate of crypto converting in BSE. The significant disadvantage of their usage are large amounts of key data, which does not allow to use them in applications of digital telephony. In this paper was proposed practical algorithms to reduce energy capacity, which allows without sacrificing the reliability, to use them in applications of digital telephony for transmitting OTP-codes for the composite authenticator in multi-factor authentication. In the authors' opinion, using two MCCS in different transmission channels of the composite authenticator will significantly enhance the safety of its use.

References

1. Reshenie po mnogofaktornoj autentifikacii 2FA One [Electronic resource]. – Available at: https://habrahabr.ru/company/1cloud/blog/277901/
2. Vazhnost' mnogofaktornoj autentifikacii [Electronic resource]. – Available at: http://www.securitylab.ru/analytics/425166.php
3. Jekspress-opros: «Kakie metody autentifikacii vy ispol'zuete doma/na rabote?» [Electronic resource]. – Available at: http://zlonov.ru/2016/07/statistic/
4. Digital Authentication Guideline [Electronic resource]. – Available at: http://www.3dnews.ru/936742?from=related-grid&-from-source=940476
5. Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication [Text] / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon // Computers & Security. – 2017. – Vol. 65. – P. 14–28. doi: 10.1016/j.cose.2016.09.009
6. Harini, N. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code [Text] / N. Harini, T. R. Padmanabhan // International Journal of Engineering and Technology. – 2013. – Vol. 5, Issue 2. – P. 1087–1094. – Available at: http://www.enggjournals.com/ijet/docs/IJET13-05-02-093.pdf
7. D'Mello, D. P. An Alternative Approach in Generation and Possession of Backup Codes in MultiFactor Authentication Scheme [Text] / D. P. D'Mello // BIJIT - BVICAM's International Journal of Information Technology. – 2015. – Vol. 7, Issue 2. – P. 883–885. – Available at: http://www.bvicam.ac.in/bijit/downloads/pdf/issue14/05.pdf

8. Gupta, N. Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography [Text] / N. Gupta, R. Rani // International Journal of Web & Semantic Technology. – 2015. – Vol. 6, Issue 2. – P. 09–17. doi: 10.5121/ijwest.2015.6202
9. Jiang, Q. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks [Text] / Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, Y. Yang // Journal of Network and Computer Applications. – 2016. – Vol. 76. – P. 37–48. doi: 10.1016/j.jnca.2016.10.001
10. Kiljan, S. Evaluation of transaction authentication methods for online banking [Text] / S. Kiljan, H. Vranken, M. van Eekelen // Future Generation Computer Systems. – 2016. doi: 10.1016/j.future.2016.05.024
11. Android-vredonos Bankosy sposoben pohishhat' kody dvuhfaktornoj autentifikacii [Electronic resource]. – Available at: http://www.securitylab.ru/news/478411.php
12. Hryshchuk, R. The synergetic approach for providing bank information security: the problem formulation [Text] / R. Hryshchuk, S. Yevseev // Bezpeka informacii. – 2016. – Vol. 22, Issue 1. – P. 64–74.
13. Evseev, S. P. Usovershenstvovanie metoda dvuhfaktornoj autentifikacii na osnove ispol'zovanija modificirovannyh kripto-kodovyh shem [Text] / S. P. Evseev, V. G. Abdullaev, Zh. F. Agazade, V. S. Abbasova // Sistemi obrobki informacii. – 2016. – Vol. 9, Issue 146. – P. 132–145.
14. Evseev, S. P. Monitoring algorithm of two-factor authentication method based on passwindow system [Text] / S. P. Evseev, V. G. Abdullaev // Eastern-European Journal of Enterprise Technologies. – 2015. – Vol. 2, Issue 2 (74). – P. 9–15. doi: 10.15587/1729-4061.2015.38779
15. Pjat' sposobov dvuhfaktornoj autentifikacii [Electronic resource]. – Available at: https://lifehacker.ru/2016/02/15/two-factor-authentication/
16. RSA SECURID® Autentifikacija po zaprosu [Electronic resource]. – Available at: http://security.demos.ru/auth_access/mfa/ondemand.php
17. Sem' metodov dvuhfaktornoj autentifikacii [Electronic resource]. – Available at: http://www.infosecurityrussia.ru/news/29947
18. Distancionnoe bankovskoe obsluzhivanie klientov: sposoby zashhity tranzakcij [Electronic resource]. – Available at: http://www.prostobiz.ua/rko/stati/distantsionnoe_bankovskoe_obsluzhivanie_klientov_sposoby_zaschity_tranzaktsiy
19. Blejhut, R. Teorija i praktika kodov, kontrolirujushhih oshibki [Text] / R. Blejhut. – Moscow: Mir, 1986. – 576 p.
20. Klark, Dzh.-ml. Kodirovanie s ispravleniem oshibok v sistemah cifrovoj svjazi [Text] / Dzh.-ml. Klark; B. S. Cybakova (Ed.). – Moscow: Radio i svjaz', 1987. – 392 p.
21. Mak-Vil'jams, F. Dzh. Teorija kodov, ispravljajushhih oshibki [Text] / F. Dzh. Mak-Vil'jams, N. Dzh. A. Slojen. – Moscow: Svjaz', 1979. – 744 p.
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. Evseev, S. P. Analiz programmnoj realizacii prjamogo i obratnogo preobrazovanija po metodu nedvoichnogo ravnovesnogo kodirovanija [Text] / S. P. Evseev, H. N. Rzaev, A. S. Cyganenko // Bezpeka informacii. – 2016. – Vol. 22, Issue 2. – P. 196–203.