Methods of information systems protection

UDC 681.3.06 **doi: 10.20998/2522-9052.2019.3.13**

S. Yevseiev[1], L. Bakirova[2], M. Sushchenko[3]

[1] Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
[2] Azerbaijan State Oil Academy, Baku, Azerbaijan Republic
[3] University of Science and Technology of China, China

MATHEMATICAL MODELS OF HYBRID CRYPTO CODE CONSTRUCTIONS ON DAMAGED CODES

Abstract. The **subject** are mathematical models of building hybrid (complex) cryptosystems based on Mac-Elis crypto-code constructions on damaged codes. The **purpose** of this work is cryptographic mechanisms design in post-quantum cryptography to provide basic security services. The use of crypto-code structures in the mechanisms of strong authentication based on OTP passwords Development of practical algorithms for their implementation based on the proposed mathematical models. The **tasks**: analysis of the main threats of using OTP passwords; basics of construction and using multi-channel cryptography systems on damaged codes; a formal description of mathematical models of hybrid crypto-code constructions on damaged codes based in the modified McEliece and Niederreiter crypto-code systems in elliptic curves; development of algorithms for data encryption and decryption at the Niederreiter-McEliece hybrid crypto code constructions (HCCC). **Conclusion:** The comprehensive protection mechanisms proposed in the article ensure the use of a strong authentication protocol in post-quantum cryptography based on OTP passwords. The use of damaged codes extends the possibilities of using crypto-code structures by significantly reducing the power of the alphabet while maintaining the required level of cryptographic resistance.

Keywords: hybrid crypto code constructions; McEliece crypto code constructions; cryptography on damages codes.

Introduction

The results of research carried out by NIST specialists in March 2018 demonstrated that crypto-resistant algorithms to brute force attacks will significantly decrease after the advent of a full-scale quantum computer. At the same time, the cryptographic strength of symmetric and asymmetric cryptography algorithms, as well as algorithms based on elliptic curves, is being questioned. At the same time, both symmetric and asymmetric cryptography algorithms, as well as algorithms based on elliptic curves, are questioned for cryptographic strength. According to NIST experts one of the promising areas are McAlice and Niederreiter crypto-code constructions. However, their practical application involves the use of significant computational costs, which significantly reduces their profitability and economic attractiveness. The mathematical models based on McAlice and Niederreiter crypto-code constructions using cryptography on defective codes and their practical algorithms are proposed in this paper. This approach allows to provide a significant reduction in the power of the alphabet and to ensure practical implementation on any platform without reducing the required level of cryptographic resistance in post-quantum cryptography. One use is to create a two-factor authentication protocol (strong authentication) based on an OTP password with the ability to use open channels of digital telephony.

Wide-spread usage of automated banking systems (ABS) is one of the most aspects of doing business. Mobile communications provide the full access to the financial services, electronic document management, and administrative functions. Electronic authentication is the one of the main security components. It's a procedure that confirms the authenticity of the source of the message. The main mechanisms for electronic authentication based on symmetric and asymmetric encryption, digital signatures (X.509 standard, IPSec, PGP, S/MIME certificates), MDC and MAC code generation procedures [3–11].

Two-factor authentication methods based on various smart cards, USB keys, OTP passwords [9, 10, 12–14] is one extra layer of security. Multifactor authentication methods are now entrusted by great number of international companies.

Problem analysis

Consumerization trend in ABS has huge impact on customers and gives the alternatives in usage of mobile devices [9, 10]. One-time password technology (OTP) can be implemented as strong two-factor authentication, and does not require significant implementation resources [9]. OTP is virtually invulnerable to attack by network packet analysis, and requires the user to enter a PIN-code, which increases authentication strength [9].

The disadvantage of OTP passwords is the possibility of an attack by text (SMS) with one of the token parts. Attackers can compromise text-based two-factor authentication in different ways: by social engineering methods, intercepting messages of International Mobile Subscriber Identity (IMSI), or usage of shortcomings in protocols that allow Operators to exchange data between networks [15, 16]. Because of this the NIST in [6] is ready to prohibit the usage of two-factor authentication codes based on OTP passwords for services that connect to public IT systems. Thus, there is a contradiction between the usage of OTP passwords in the two-factor authentication protocols and transmission security.

The purpose of this work is to analyze the main threats of OTP passwords usage, considering the basics of building multi-channel cryptography systems on defective codes, to provide a formal description of mathematical models of hybrid crypto-code constructs on defective codes, and to develop encryption/ decryption algorithms. To achieve the goal, we consider the following tasks:

– analysis of the main threats of using OTP passwords;

– basics of construction and using multi-channel cryptography systems on defective codes;

– a formal description of mathematical models of hybrid crypto-code constructions on defective codes based in the modified McEliece and Niederraiter crypto-code systems in elliptic curves;

– development of algorithms for data encryption and decryption at the Niederrheit-McEliece hybrid crypto code constructions (HCCC).

We are using Niederreiter and McEliece cryptosystems in our work. Cryptosystem (in some sources also crypto-code) is a suite of cryptographic algorithms needed to implement a particular security service. Our cryptosystems consist of three algorithms: key generation, encryption and decryption. To understand the basic principles of constructing cryptosystems on defective codes we rely on the Shannon and Mishcenko works. Flawed text is understood the text obtained by further deformation of non-redundant codes of letters.

Analysis of the main threats of using OTP passwords. Digital authentication ensures the users identity. For services that use successive logins, authentication guarantee risk-free access [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 implementation of an additional security level provides more effective protection for the account from unauthorized access. Using this type of 2FA, the user enters the password on the first level of authentication. The next step is to enter the One-Time Password (OTP) that is usually sent via SMS. OTP is available only to the end-user and server [13, 14].

To ensure strict authentication in the critical IT-infrastructures, it is necessary to use two-factor authentication methods based on multichannel cryptography on persistent crypto algorithms that ensure the security of OTP authentication passwords [3 -22].

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

The Passwindows-based method allows generating OTP passwords without using cryptographic procedures. Method is based on the seven-segment barcode. However, the studies have shown hacking availability in 3 to 5 sessions by forming a bar code of the user's card of banking services.

To obtain the personal user's data attackers use an integrated approach. They are combining social engineering skills with traditional hacking methods. Thus, it became necessary to ensure confidentiality the data transfer in open switched mobile systems/4G LTE.

Two-factor authentication, or 2FA – a method of user identification in any service that uses two different types of authentication data. The introduction of an additional level of security provides better protection against unauthorized account access. Using this type of 2FA, the user enters the first level of authentication personal password. The next step, he must enter the OTP token (OTP – One-time Password Algorithm), usually sent by SMS to his mobile device. OTP will be available only to those who are supposed in theory, introduced the available third-party password [23]. Methods strict (two-factor) authentication is often used in the financial sector, but in principle can be applied in almost any other field. The main methods of construction of two-factor authentication classified [23]:

1. Software to identify a specific computer. In computer installed a special program that sets it a cryptographic token. Then, in the authentication process will involve two factors: the password and token embedded in a PC. Since the marker is always on the computer, the user login only need to enter a user name and password.

2. Biometrics. The use of biometrics as a second factor of authentication is done by identifying the physical characteristics of the person (finger print, eye membrane, etc.).

3. Disposable e-mail- or sms-password. Use as a secondary factor authentication password OTP, perhaps by sending the second one-time password to the registered email address or mobile phone.

4. Token with a single password. User is a device that generates a constantly changing passwords. These passwords entered by the user in addition to your regular password when authenticating.

5. Control outside. This method involves a call from the bank at a pre-registered phone number. The user must enter the password on the phone, and only then he will get access to the system.

6. Identification using gadgets. Such identification is performed by placing cryptographic tag to any user device (e.g. USB-drive, iPad, memory card, etc.). When registering, the user must connect the device to a PC.

7. Card with a layer. The user is issued a card with PIN-code is used only once.

General classification methods multifactor authentication shown in Fig. 1. Given in [23] multifactor authentication methods analysis showed the following major advantages and disadvantages:

– The advantages of the methods based on SMS – you notifications OTP generation-codes at each entrance and transfer to additional channels, intercept login and password on the main channel will not lead to the attacker bank client information. Binding OTP-password to the phone numbers. The main disadvantages are: use of open channel provider can not provide confidentiality OTP-codes using only cellular channels leads to "losing" two-factor authentication. There is a theoretical possibility of substituting numbers across service provider or employees mobile shops.

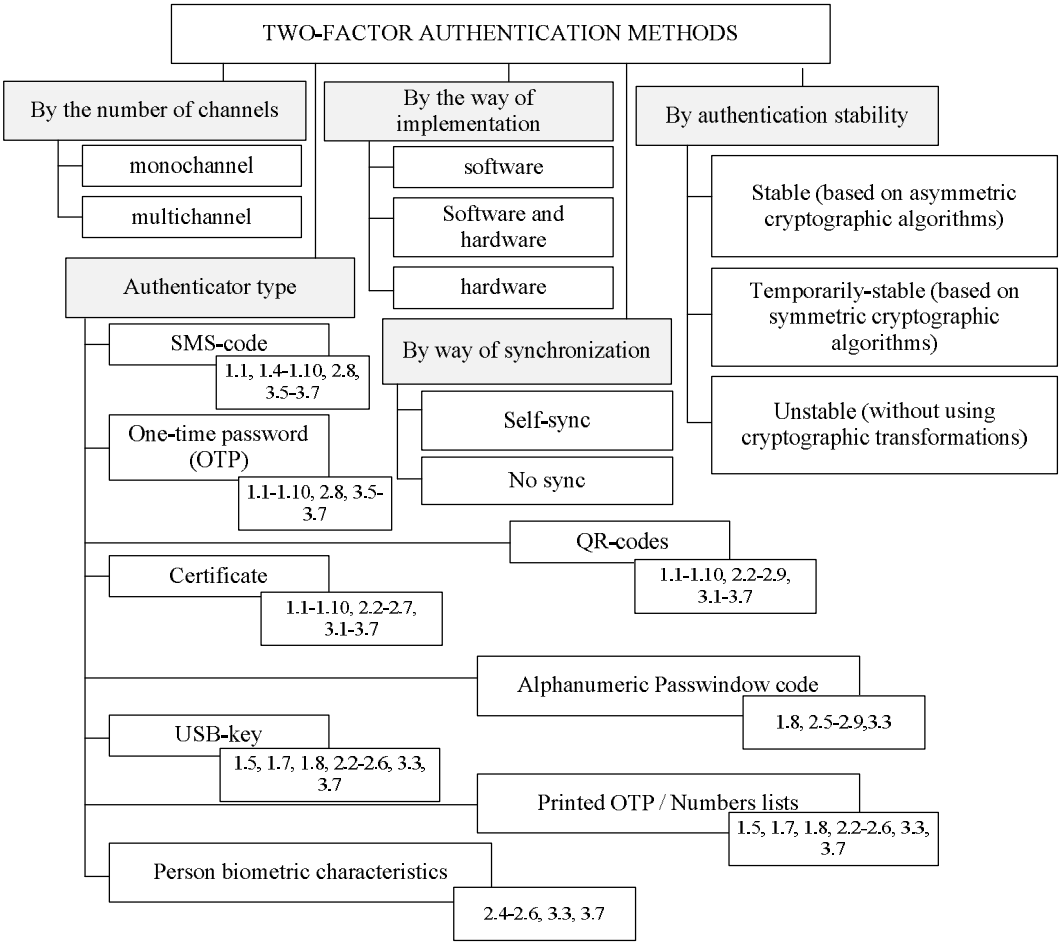


Fig. 1. Multifactor authentication methods classification

– Using methods of extra-authenticator (QR-codes) can support multiple accounts in a single authenticator and create a primary key, no need to use cell lines, OTP generation-Password-based encryption algorithms. The main disadvantages are – authenticator using the same device from which the entrance leads to a "loss" two-factor access to primary attacker user key leads to cracking the authentication system.

– Check the log using mobile applications automates the authentication process without user verification based private key authentication in the mobile application. The main disadvantages are: loss / private key disclosure results in cracking the authentication system, the possibility of receiving SMS-messages through synchronization between iPhone and Mac, use authenticator on the same device from which the entrance leads to a "loss" multifactorial.

– Physical (or hardware) tokens is the most reliable method of two-factor authentication. Often they are presented as USB-sticks with its own processor, which generates cryptographic keys that are entered automatically when connected to a computer. The advantage is the absence of an additional mobile applications, software, tokens are completely independent device. The disadvantages include- using multiple accounts leads to "bundle" tokens that are not supported by all applications.

– Back keys are spare option in case of loss / theft of smartphones, which come one-time passwords or codes confirmation. Loss / theft of keys reserve leads to destruction of privacy authentication system.

– Bar-Passwindow system codes provide unique static image sequence of characters generated dynamically authentication server without encryption algorithms.Any-interference pattern or fake bar-code is passively presented to the user in the form of combinations appearance in a pattern that does not meet expectations. A major drawback is the possibility of a unique selection bar-code card proposed in [23].

– The use of biometrics as a secondary factor authentication is done by identifying the physical characteristics of the person (fingerprint, iris, etc.). Advantages of the method is to use the unique physiological characteristics of the person, the absence of additional mobile applications and software. A major drawback is the specific requirements for software-hardware devices readable biometric user data.

Thus, in automated banking systems are generally used multifactor authentication systems based on one-time e-mail or sms-password and different types of tokens. To ensure privacy standard remote banking OTP Bank transferred-must use encrypted codes and independent operators channel delivery. This approach is not subject to the majority of known threats, in addition to social engineering that exploits the human factor.

The analysis of threats [23–29] indicates a significant transformation and their hybridity. From a purely threats IS, CB, SI infrastructure ABS, displays

signs of hybridity threat began to occur as a result of simultaneous action on the object of protection – SI in ABS by the emergence of the phenomenon of synergism [24]. Fig. 2 shown synergistic approach to classifying threats multifactor authentication combined with shown in Fig. 2 classification methods 2FA.

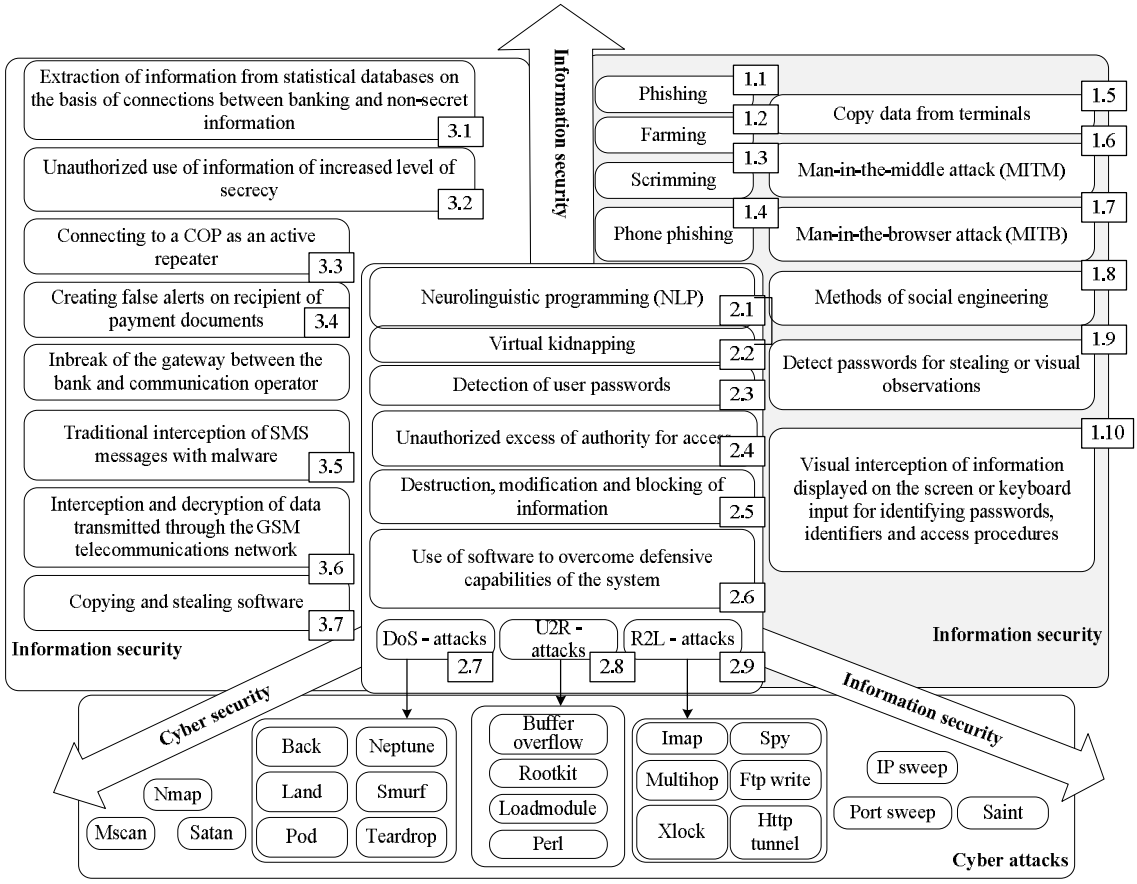


Fig. 2. Synergetic model of banking information security threats

Analysis of current authentication systems showed that their safety is measured by dividing the difference between the cost benefit attacks and for attacking the cost of protection against them. So expensive, although safer methods such as cryptographic PKI-protected devices with their own channels, screens and keypads are rated so low on a scale of security, while the banking system is still largely based on the cheapest and seemed be the least secure method of using PIN-codes and passwords. Total cost and complexity of deploying such devices often outweighs the benefit of their extremely high security.

Threats to the security of the network ABS can be divided into network attacks (information coming from the remote agent) and local attacks originating from malware already installed on the client system, such as Trojans, rootkits, and so on. Often authentication security assessment focused primarily on network attacks suggesting that the terminal (ie, desktop computer, laptop or mobile device) is protected platform [23]. However, often the attacker has full access to the victim's computer through the hidden processes of communication that remained from malware using uncorrected security holes licensed software.

Typical methods of attacks on Bing are:

Fracture online databases – stealing information stored in commercial databases, data.

Man in the middle / phishing – third party intervenes and represents the client and server, making recording and / or alter each other.

Attacks in social engineering – cheating customers with a view to find out their personal information for transmission by hackers.

"Man in the Browser" – malicious software that is installed on the computer victim to report network activity, keystrokes and screen data captured by a hacker, allowing him to intercept data transfer funds, which funds may be unintentionally distorted by changing the information displayed in the browser user.

Attack with full-force passwords – polled the server with all possible combinations of passwords.

Simple theft – written details about authentication or card can be physically taken and copied.

Observations from the back – an attacker can quietly watch as the user enters details of the transaction.

With the proliferation of GSM, smartphones and tablets connected to the network, even this safety advantage can be lost if user authentication transactions carried out on the same mobile device. In addition, the growth of unwanted software for mobile now allows an attacker to gain access to the authentication codes sent via SMS not only through traditional means of interception by malicious software [22]. But by

intercepting and decrypting data transmitted via GSM-network telecommunications [23].

Attacks mobile authentication successfully conducted without such technology. Instead, an attacker impersonating a user device and asks that all SMS messages sent to another phone number throughout the attack [23]. Another method of authentication using mobile camera to read the barcode image on a workstation user who encrypted with OTP information about the transaction. This method has a problem, assuming that the operating system on the mobile device is not subject to such a vulnerability to malicious software, like all other forms of software that works with the network [23].

When using biometric authentication user data available for online authentication. However, biometric authentication devices can not communicate with local devices or network without facing malware attacks and / or attacks "mediator" [23]. This method is as impossible to change again, after the attacker gave himself for user using biometric authentication.

Biometric authentication provides the user with a convenient way to generate online user name, but the network and tapped the infected mobile device, the overall performance of the safety of such methods is better than using normal user name and password.

Electronic hardware tokens come in several forms and include various security features authentication. The most common hardware tokens generating one-time passwords (OTP) using cryptographic algorithms with an internal key, or, more often, the secret key is generated based on common, synchronized system time values. The user device reads the displayed numbers and manually enters them into their terminals to cross-reference with the authentication server.

This simple method of electronic OTP generation remains vulnerable to attacks "mediator", as users are required to disclose OTP no means of checking the authentication context. In response, many manufacturers have added a small token numeric keypad, significantly increasing the size of the marker, but allowing the user to enter information about specific transactions encrypted with a secret key before the user enters the result in his terminal. This is a type of check or signing a transaction and does provide some protection from attack "mediator".

However, this method is still vulnerable to attacks using laborious manual process of signing the transaction. The time and attention required to perform manual operations have been successfully used to distract the user from the transaction context information that the user takes, and therefore attacks can be successfully implemented on a mass scale [25].

Printed lists OTP / grid numbers. The older method of providing one-time passwords – a printed list of randomly generated passcodes or transaction authorization codes on paper or scratch cards. Each access code is requested in sequence and is used to authenticate a transaction.

An alternative may be used printing character and authentication server will issue a barcode, asking symbols are in certain coordinates.

Both methods use the keys and signals that can be communicated verbally. This allows the attacker to ask the user follows the actual code via malware using social engineering or phishing attacks. In addition, the relatively low entropy lists or grids require frequent changing of keys to prevent repetition code request attacker.

These methods are vulnerable to the full range of attacks "intermediary" for the same reasons that all authentication methods with unknown context.

Fake (weakened) barcodes. An attacker could try to weaken the protection PassWindow, changing the frame rate of this (intercepted) bar code before delivering weakened (Simplified) barcode person. This method reduces the entropy of the bar code to change the details that would facilitate analysis intercept requests / responses. But obviously damaged barcode passively warns the user attempted attack, causing suspicion about the use of computers and communication channels.

Research methods for constructing OTP password. Trends in ABS lead to the fact that users must use different devices to access the resources of financial services ABS – used stationary or mobile computer, tablet or smartphone [23]. Technology-time password (OTP), can help implement a strict two-factor authentication, and requires significant costs of implementation and support [23, 30]. OTP virtually invulnerable to attack the network analysis package, and further requires the user to enter a PIN-code, which is an additional factor of authentication [23, 30]. Thus, a two-factor user authentication system based on the possession of something (Authentication by Ownership) or based on knowledge of something (Authentication by Knowledge) [24]. The downside of using OTP-password is the ability to "intercept" malicious text (SMS-messages) from one part of the token. Attacking may compromise your 2FA based on text in several ways: based on the methods of social engineering (forwarding messages through ISP) intercept messages using the IMSI-catcher (International Mobile Subscriber Identity – international identification of mobile subscribers), using flaws in the protocols that allow operators due to exchange data between networks [23]. For this reason, the National Institute of Standards and Technology USA (NIST) in [31] prepared to ban the use of two-factor authentication based OTP-passwords for services that are connected to the public IT systems. Thus, there is a contradiction between the OTP-use passwords and protocols two factor authentication security for their use.

In [32], the following authentication confidence level (Authenticator Assurance Levels, are shown in Fig. 3.

The analysis of requirements in [15. 31, 32] to OTP-forming methods passwords showed that:

– secret authenticator memorable – commonly called password or if numeric, PIN – a secret meaning that for selecting and storing user must consist of 8 characters, be very difficult to remember and kept secret. To form a secret authenticator proposed to use algorithms of MAC codes: HMAC [FIPS 198-1], SHA-3 [FIPS 202], CMAC [SP 800-38B] or Kecacak Message Authentication Code (KMAC), customizable SHAKE (cSHAKE) or Parallelhash [SP 800-185];

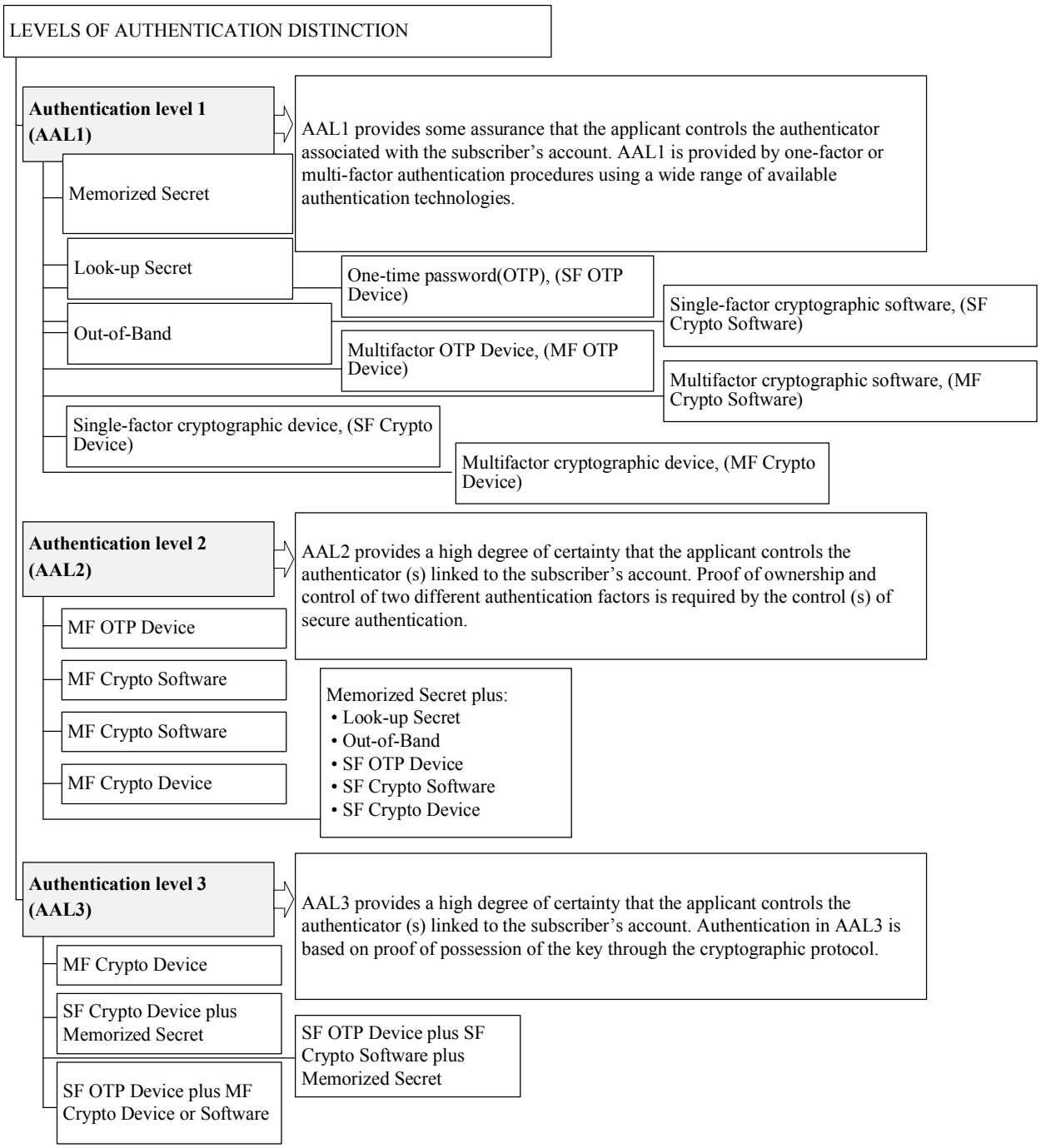


Fig. 3. The levels of reliability and authentication mechanisms of OTP password

– secret authenticator Look-Up – represent a physical or electronic record, which stores the set of secrets that are shared between the applicant and CSP (Center for Security Policy - Center for Security Policy). To create the list of secrets standardized random bit generators [SP 800-90Ar1] [18];

– authenticator-band – the physical device that uniquely addressable and can communicate securely with the verifier through a separate channel, called the secondary channel. The device has also supervised the applicant and supports private communications by the secondary channel, separate from the primary channel for electronic authentication. To form the second channel can be used by public network, dial (4G LTE). Authenticator is transmitted in encrypted form [17];

– single-OTP-generating unit OTP. This includes hardware devices and software generators OTP, installed on mobile gadgets. These devices have built-in secret, which is used as a key for OTP generation and requires activation via a second factor. To generate the key using symmetric and asymmetric crypto algorithms. OTP is displayed on the device and entered manually for transfer to the verifier, thus proving ownership and control device;

– multi-device generates OTP for use in authentication after activation with an additional authenticator. The device uses hardware devices and software OTP generator based on symmetric encryption algorithms or hash functions that are installed on mobile gadgets. The second factor authentication can be

achieved by using a built-in input area integrated biometric reader (e.g. fingerprint) or direct computer interface (e.g. USB-port). OTP is displayed on the device and entered manually for transfer to the verifier;

– single-factor authenticator encryption software - a cryptographic key stored on disk or some other "soft" media. Crypto-factor authenticator software encapsulate a secret key that is unique to the authenticator. Authentication is performed by checking the ownership and control key;

– single-cryptographic device is a hardware device that performs cryptographic operations using secure cryptographic key and providing output authenticator via direct connection to the endpoint user. The device uses a built-in symmetric or asymmetric cryptographic keys and requires activation via a second factor of authentication. Authentication is performed by checking the ownership of the device authentication protocol;

– multi authenticator encryption software – a cryptographic key stored on disk or some other "soft" media that requires activation via a second factor of authentication. Authentication is performed by checking the ownership and control key;

– multi cryptographic device – a hardware device that performs cryptographic operations using one or more cryptographic keys protected and requires activation via the second content authentication. Authentication is done by checking the device ownership and control key. Exit authenticator provided a direct connection to the endpoint user and depends heavily on the particular device and the cryptographic protocol. Multifactor authenticator devices use cryptographic protected from unauthorized access equipment to encapsulate the secret key. Fig. 4 are the main threats authenticator that can be classified based on the types of attacks authentication factors [23].

The analysis of threats based on a synergistic approach to threat assessment [18] Shows that criminals today use a comprehensive approach to obtain personal data of users and creators service authenticator ABS.

Typically, hacking techniques based on combining social engineering techniques with traditional methods of masquerade and penetration.

Also used and new types of cyberattacks to effectively embed malware on mobile communications, which in turn leads to lower profitability multifactor authentication methods based on SMS-messages and passwords OTP-ABS. Thus, there is need for additional means of transmission authenticator privacy in open systems mobile / 4G LTE, dial. In the next section the method of two-factor authentication based on HCCC*MEC*, which can eliminate the contradictions.

Basic principles of constructing cryptosystems on defective codes. In [20, 21], theoretical and practical bases of construction of defective codes are considered. By *flawed text is understood the text obtained by further deformation of non-redundant codes of letters.*

Thus, a necessary and sufficient condition for the loss of text with loss of meaning is the shortening of the lengths of the code symbols of the text beyond their redundancy. Consequently, the defective text has alength shorter than the length of the source text, and there is no sense in the source text [20]. The construction base of damage codes is to remove the plaintext's symbols order and to decrease the redundancy of the language symbols in the flawed text.

The methods of computing the information by K. Shannon allow us to determine the predictable information ratio and the amount of unexpected information.

Redundancy of the text is calculated by the

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

where M – original text; B – language redundancy ($B = R - r$, R – absolute entropy of a language ($R = \log N$, N – alphabet power, r – language entropy per character, $r = H(M)/L$, L – length of the M message in the language symbols); $H(M)$ – entropy of message; L_0 – the length of the message M; B_A – language redundancy.

To obtain a defective text (FTC) and damage (DCH), the "perfect" compression method is used [20, 21]. The number of cycles required to reduce the length of the source text is:

$$m > \left(\log n - B_A\right)/\log \eta,$$

where n – the character power of the plain text; B_A – language redundancy; η – the number of times the plain text length in MV2 decreases at each step (Fig. 5).

To measure the damage efficiency we need to define the degree of plain text meaning destruction. It is equal to the entropy and length difference of the defective and plain texts.

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

$$s = \left[\left(L_0 - L_{FTC}\right)/L_{FTC}\right],$$

where M_i– part of the source text corresponding to the i-th segment, p_i – its probability, L_0 – length $M_i$equal to the length L_{FTC} – flawed text, s – number of segments. For an ergodic source of the source code characters:

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

The information core of some text is the flawed text of CFT, obtained by cyclic transformation of the universal damage mechanism C_m.

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

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

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

As a result we have two ciphertexts (damage (CH_D) and flawed text (FTC)). Each has no meaning either in the source code or in the alphabet of the ciphertext. The the original message (M) ciphertext is represented as a set of two defective ciphertexts, that cannot individually restore the original text. To restore the original sequence, there is no need to know the intermediate faulty sequences. It is necessary to know the last flawed sequence and all the damages (damage rules included).

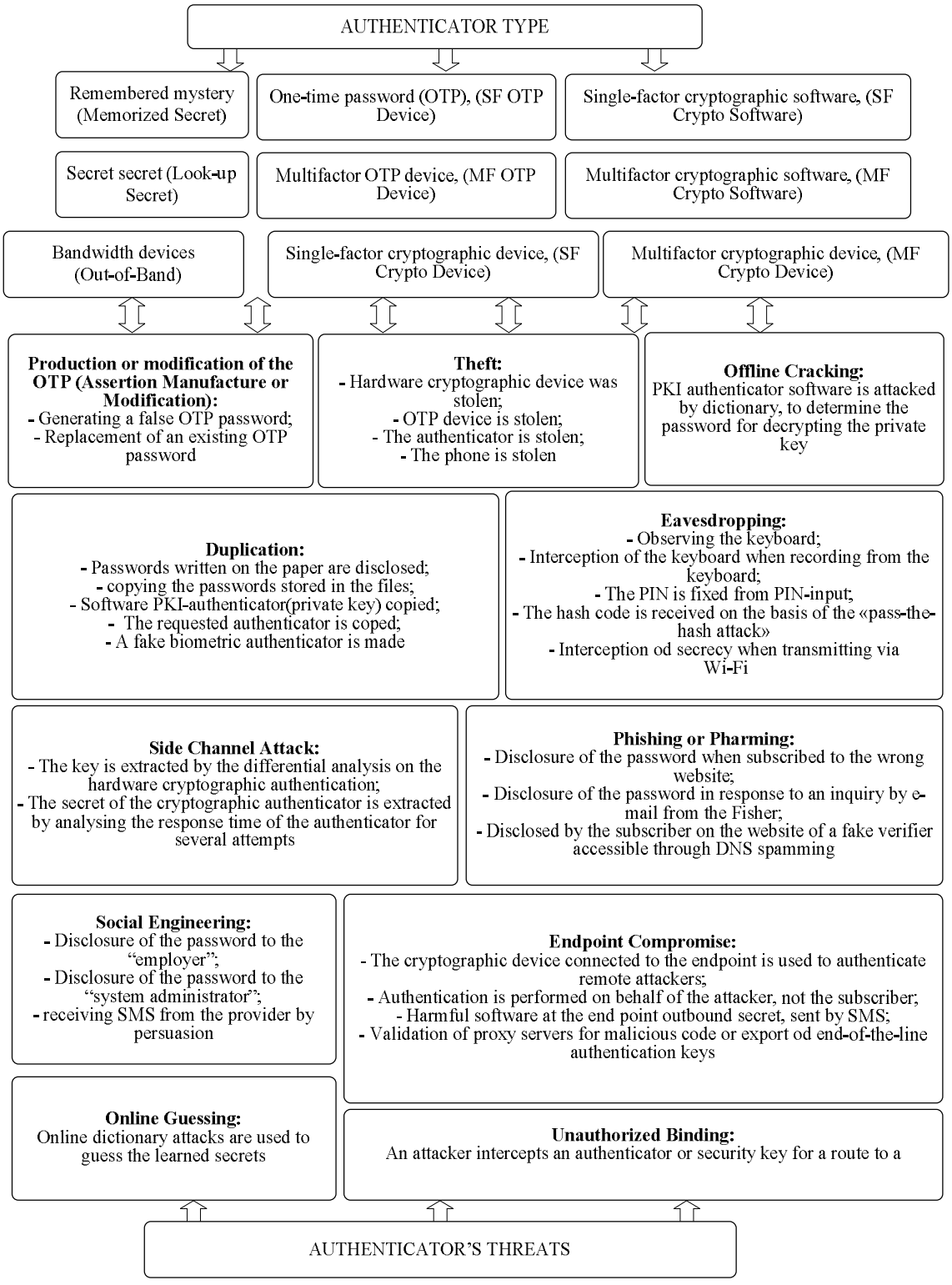


Fig. 4. Classification by type of threats authenticator

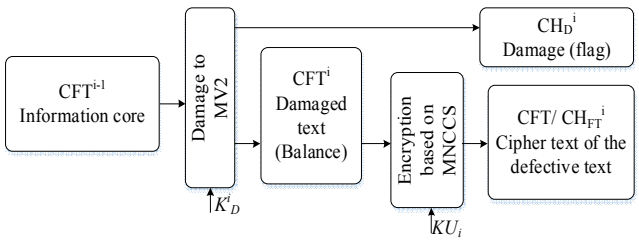


Fig. 5. The structural diagram of first step of the universal mechanism of damage

The main advantage of the proposed methods is the usage of defective codes is the use of non-BS, and MNCCS McEliece and Niederreiter. It ensures the cryptographic strength of damage and/or defective text.

To estimate the cryptographic strength [20, 21] we are using the Shannon concept of the "uniqueness distance" of the cipher. The corresponding message is recovered from the known cipher text by using the min natural number L, and the "uniqueness distance" is the minimal natural number L as well.

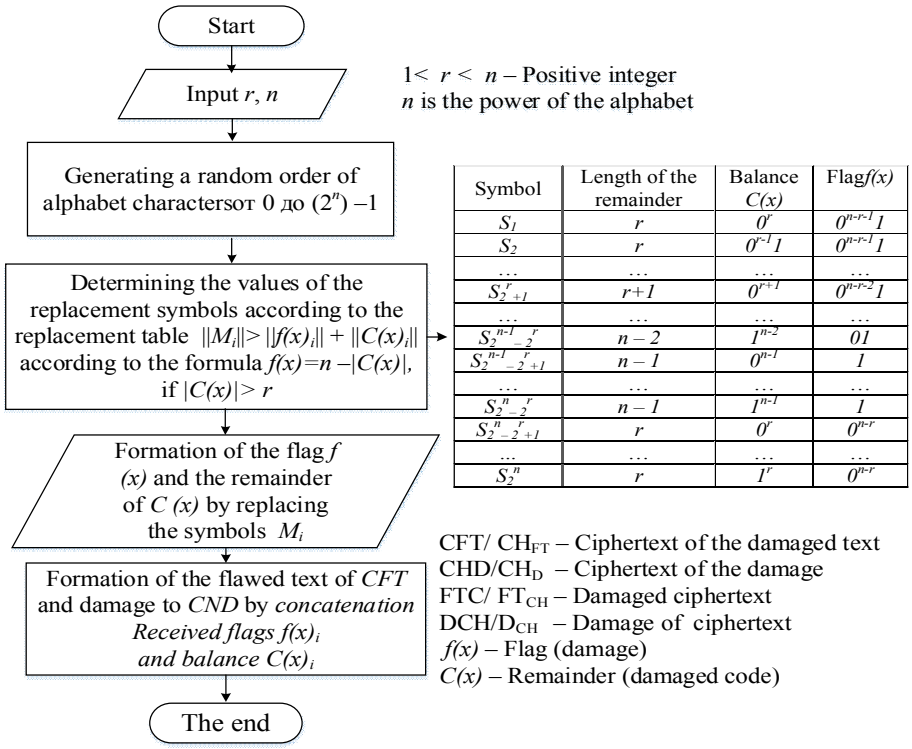
The uniqueness distance of the random cipher model: it is possible to obtain the meaningful text; randomly chosen key K; decryption attempt:

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

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

where L – redundancy of source code; H – entropy on the letter of a meaningful text in the input alphabet I, $|I| > 2$, 2^{HL} – approximate value of the number of meaningful texts.

The cyclic algorithm for obtaining defective texts, is a universal damage mechanism (C_m, where m – the number of cycles). It is a random replacement of the each symbols bit in the plain text. Replacement goes by a tuple of a smaller or equal bits number with their concatenation. Fig. 6 shows the universal mechanism of causing damage (MV2 algorithm (formation of the flawed text)).



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}

Fig. 6. The universal mechanism of damage (MV2 algorithm)

The transformation domain in the algorithm MV2 is the set $\{0, 1\}^n$. Let X – be the random discrete element that takes values $x_i \in \{0,1\}^n$ with probabilities p_i and $T = (c, f) \in F_n^r$

Is a fixed MV2 transformation. Then for any $y \in U_{r\,n-1}$ (Some binary string of a set of strings of variable length) and for any $1 \le i \le |y|$ performed:

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

Regardless of the random element probability distribution for the FTC and CHD entropies, we have the following equations:

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

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

Thus, with a uniform distribution of the inputs (flags) of the MV2 algorithm we can obtain the distribution:

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

Multichannel cryptography based on the defective codes allows integrating of crypto systems with crypto-code constructions (MNCCS McEliece). Systems complement each other and provide safe and reliable connection.

The analysis of harming methods have shown that the first method is suitable for IOS. Damage with subsequent crypto-conversion allows reducing the alphabet power in McEliece algorithm. The uniqueness distance for the expression 1 will transform:

$$U_0 = \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right) \Big/ \left(B\log|I|\right),$$

Mathematical models of McEliece and Niederreiter defective codes and their implementation algorithms. We consider the formal description of the modified McEliece crypto code system on the defective codes that used in the two-factor authentication protocol. To build a mathematical model, we use the basis from [21] to define the secret system. In [22], we have consider the formal description of the mathematical model of MNCCS McEliece on modified elliptic codes. The McKenzie symbols reduction mathematical model is defined by the following elements [22]:

- great number of open texts

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

where $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j – information symbols equal to zero, $|h| = k/2$, i. e. $I_i=0$, $\forall I_i \in h$;

– many *codograms*

$$C = \{C_1, C_2, ..., C_{q^k}\},$$

where $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$ – the set of direct mappings (based on the use of the public key - the 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 maps (based on the use of a private key) $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}$, where $\phi_i^{-1} : C_{k-h_j} \to M$, $i = 1, 2, ..., s$ – the number of damaging texts *CFT*, $CFT = \{CFT_1, CFT_2, ..., CFT_{q^k}\}$ – set of damages *CHD*, $CHD = \{CHD_1, CHD_2, ..., CHD_{q^k}\}$ – a lot of direct damage (based on the use of a key – K^i_{MV2}, and algorithm MV2) – $E = \{E^1_{K_{MV2}}, E^2_{K_{MV2}}, ..., \phi^S_{K_{MV2}}\}$, $i = 1, 2, ..., s$; $f(x)_i$ – flag (damage, *CHD*), $C(x)_i$ – remainder (damaged text, *CFT*); $f(x)=n - |C(x)|$, if $|C(x)| > r$, where r – some parameter $r \in_R Z_{q^m}$, $0 \langle r \langle n$ – set of maps *MV2* F^r_n is given by a objective mapping between the set of permutations $\{S_1, S_2, ..., S_{2^n}\}$ and set of $\#F^r_n$, $\#F^r_n = \#\{(c, f)\} = 2^n!$;

– meaningful text set (based on key usage – K^i_{MV2}, and algorithm MV2)

$$E^{-1} = \{E^1_{K_{MV2}}{}^{-1}, E^2_{K_{MV2}}{}^{-1}, ..., E^S_{K_{MV2}}{}^{-1}\},$$

where $E^{-1}_{K_{MV2}} : \|f(x)_i\| + \|C(x)_i\| \to M$, $i = 1, 2, ..., s$; $f(x)_i$ – flag (damage, *CHD*), $C(x)_i$ – remainder (flawed text, *CFT*); $f(x)=n - |C(x)|$, if $|C(x)| > r$, where r – some parameter $r \in_R Z_{q^m}$;

– set of keys that parametrize direct mappings (public key of an authorized user)

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G^{EC1}_{X\ a_i}, ..., G^{ECs}_{X\ a_i}\},$$

where $G^{ECi}_{X\ a_i}$ – generating $n \times k$ matrix 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 – set of coefficients of a polynomial of a 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 the inverse mapping)

$$K^* = \{K^*_1, K^*_2, ..., K^*_s\} =$$

$$= \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\},$$

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

where X^i – a masking non-degenerate randomly generated source of keys $k \times k$ matrix with elements from $GF(q)$; P^i – randomly generated by the source of the keys $n \times n$ matrix with elements from $GF(q)$; D^i – diagonal key source $n \times n$ matrix with elements from $GF(q)$, i. e. $\phi_i^{-1} : C \xrightarrow{K^*_i} M$, $i = 1, 2, ..., s$, – the complexity of performing a reverse mapping ϕ_i^{-1} without known key $K^*_i \in K^*$ is associated with the solution of the theoretic-complexity problem of decoding a random code; – set of keys for converting defective codes $K^i_{MV2} \in K_{MV2}$.

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

- Algebraic block *(n, k, d)* code C_{k-h_j} under *GF(q),* i. e. multiple codewords $C_i \in C_{k-h_j}$ such that equality $C_i H^T = 0$, where H – the verification matrix of the algebraic block code;

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

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

– masking matrix mappings given by a set of matrices $\{X, P, D\}_i$, where X – Non-degenerate $k \times k$ matrix under *GF(q),P* – permutation $n \times n$ matrix under *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 under *GF(q)* with non-zero elements on the main diagonal; r –parameter $r \in_R Z_{q^m}$, $Z_{q^m} = \{0, 1, ...2^n - 1\}$, n – some parameter $n \in_R Z_{q^n}$, $Z_{q^n} = \{1, ...2^n\}$;

– set of maps *MV2* F^r_n.

In McEliece, the modified algebraic geometric *(n, k, d)* code C_{k-h_j} with a fast decoding algorithm is masked for random *(n, k, d)* code C_{k-h_j} * by multiplying the generator matrix G^{EC} code C_{k-h_j} on secretive masking matrices X^u, P^u и D^u, design of an authorized user's public key: $G^{ECu}_X = X^u \cdot G^{EC} \cdot P^u \cdot D^u$, $u \in \{1, 2, ..., s\}$, where G^{EC} – generating $n \times k$ matrix of algebraic geometric block (n, k, d) code with elements from $GF(q)$. Based on the usage of the polynomial coefficients of the curve chosen by the user $a_1 ... a_6$, $\forall a_i \in GF(q)$, uniquely defining a particular set of points of a curve from the space P^2.

Design of closed text $C_j \in C_{k-h_j}$. We get the open text $M_i \in M$ and the given public key $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ by forming a codeword of the masked code with randomly generated vector $e=(e_0,e_1,...,e_{n-1})$:

The Hamming weight of the vector e does not exceed the correcting ability of the algebraic block code: $0 \le w(e) \le t = \lfloor (d-1)/2 \rfloor$, $\lfloor x \rfloor$ – the integer part of the real number x.

For each closed text we generate the $C_j \in C_{k-h_j}$ corresponding vector $e=(e_0,e_1,...,e_{n-1})$ as a one-time session key, i.e. randomly created vector e for a specific E_j.

The MV2 algorithm receives

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

in the communication channel $\left\| f(x)_i \right\|$ u $\left\| C(x)_i \right\|$, the transmission can be carried out either one at a time or two independent channels.

On the receiver side, we have an authorized user who knows how to damage F_n^r, and about masking, the null information symbols number and location. He can use the fast algorithm for decoding algebraic geometric code to recover plain text:

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

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

To do it, an authorized user adds null information symbols $C_j{}^* = C_j + C_{k-h_j}$, from recovered private text C_j and removes the action of secret permutation and diagonal matrices P^u и D^u:

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

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

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

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

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

Let us decode the resulting vector by Berlekamp-Messi algorithm [15]:

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

it's eliminates $(G)^{ECT}$ and removes the masking matrix X^u. We multiple $M_i \cdot \left(X^u\right)^T$ by $\left(X^u\right)^{-1}$: $\left(M_i \cdot \left(X^u\right)^T \right) \cdot \left(X^u\right)^{-1} = M_i$. That's the way to obtain the plain text M_i.

Encryption algorithm inGKKK McEliece on the defective codes:

Step 1. Fix a finite field *GF(q)*. 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 $EC(GF(q)):(P_1, P_2, ..., P_N)$ under *GF(q)*. Fix a subset of points $h(GF(q)): (P_{x1}, P_{x2}, ..., P_{xx})$, $h \subseteq EC(GF(q))$, $|h|=x$ and keep it as secret.

Step 2. Form the initialization vector $IV=EC-h_j$, h_j

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

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

Step 4. We form a random error vector e such that $w(e) \le t$, $t = \lfloor (d-1)/2 \rfloor$. Add the generated vector to the codeword, we get the code word: $c^*=c+e$.

Step 5. Form the code, by removing the symbols of the initialization vector: $c_X{}^*=c^*-IV$.

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

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

The decoding algorithm HCCC McEliece:

Step 1. By using the MV2 algorithm obtain the text :

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

Step 2. Enter the codogram that needs to be decoded. Enter the private key - the generator and / or the verification matrix of the elliptic code.

Step 3. The codogram is the code word with errors in the elliptic code. Weight of the error vector $w(e) \le t$. We should decode the codogram that's how we find the error vector.

Step 4. We form the required information vector.

Description of *Niederreiter hybrid mathematical model*:

– many open texts

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

where $M_i = \left\{ e_0, e_{h_1}, ... e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$, h_e – the error vector symbols equals zero, $|h| = e/2$, i. e. $e_i=0, \ \forall e_i \in h$;

– many closed texts

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

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

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

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

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

– set of inverse maps (based on the use of a private (private) key)

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

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

– set of keys that parametrize direct mapping (public key of an authorized user)

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

where $H_{X_{a_i}}^{EC_i}$ – $r \times n$ check matrix of the algebraic geometric block (n, k, d) code with elements from $GF(q)$, i. e. $\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*_{r-h_e}$, $i = 1,2,...,e$, a_i – set of curve's polynomial coefficients polynomial $a_1 ... a_6$, $\forall a_i \in GF(q)$, defining a specific set of a curve points in the space P^2.

– a set of keys that parameterize the inverse mapping (the private (private) key of the 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 – a masking non-degenerate random source of keys $k \times k$ matrix with elements from $GF(q)$; P^i – randomly generated $n \times n$ matrix with elements from $GF(q)$; D^i – diagonal key source $n \times n$ matrix with elements from $GF(q)$, i.e. $\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M$, $i = 1,2,...,s$,

- many flawed texts *CFT*,

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

– set of damages *CHD*,

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

– a lot of damaged (based on the use of a key – K^i_{MV2}, and algorithm MV2)

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

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

– set of maps *MV2* F_n^r that given by a bijective mapping between the set of permutations $\{S_1, ..., S_{2^n}\}$ and set of $\# F_n^r$, $\# F_n^r = \#\{(c,f)\} = 2^n!$;

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

The initial data for the asymmetric crypto-code system are:

– non-binary balanced code over GF (q), i.e. set of length sequences n and weight $w(\varepsilon_i)$;

– algebraic geometric block *(n, k, d)* code *C* under *GF(q),* i.e. multiple codewords $C_i \in C$ where $C_i H^T = 0$, H algebraic geometric block code should be checked matrix;

– *IV* – initialization vector, *IV*= $|h|$ =½ h_e – elements of reduction (h_e – error vector symbols equal to zero, $|h|=1/2e$, т. е. $e_i = 0$, $\forall e_i \in h$);

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

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

– set of maps *MV2* F_n^r.

The closed text $C_j \in C$, open text $M_i \in M$ and the given key H_X^{ECu}, $u \in \{1,2,...,s\}$ performed by forming a noise-immune sequences S_{X_j} that corresponding to the balanced 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 of the vector M_i does not exceed the correcting ability of the algebraic block (n,k,d):

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

The power of the sets M and C is determined by the spectrum of the weights $w(M_i)$. In 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 – Binomial coefficient, $C_n^i = \dfrac{n!}{i! \cdot (n-1)!}$.

The value $w(M_i)$ select according to the transmission security value. For $w(M_i) = const = w(e)$: $m = (q-1)^{w(e)} \cdot C_n^{w(e)}$. By mapping ψ we get sequences $M_i = \{e_0, e_1, ..., e_{n-1}\}$ from the set of $M = \{M_1, M_2, ..., M_m\}$. Mapping ψ implemented by excessive coding of non-binary balanced codes of inessential information sequences.

Private text $C_j \in C$ corresponds to the vector $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Initialization vector $IV=EC–h_j$, h_j assessed by information symbols equal to zero, $|h| = \frac{1}{2}k$, i. e. $I_i = 0, \forall I_i \in h$.

Shortened error vector $e_x=e(A) – IV$.

The public key assessed by multiplying the verification matrix of the algebraic geometric code by masking matrices $H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u$, $u \in \{\overline{1,s}\}$, where H^{EC} – $n\times(n-k)$ check matrix of algebraic geometric block code (n,k,d) 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 receive $S^*_{r-h_e}$,

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

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

On the receiver side, an authorized user who knows the damaging F_n^r and masking $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) rules and the IV: $E^{-1}_{K_{MV2}} : \left\|f(x)_i\right\| + \left\|C(x)_i\right\| \to S^*_{r-h_e}$, forms a code sequence $c^*_{X_i}$ as one (any) of the possible solutions for equation $S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j}$. Finds a vector $c^*_{X_i}$, that can be decomposed into

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

where c_{X_i} – one of the possible code words of the masked (n,k,d) Code with a check matrix $H^T_{X_j}$, i.e. $c_{X_i} \cdot H^T_{X_j} = 0$. An authorized user have a set of matrices $\{X,P,D\}_u = \{X^u, P^u, D^u\}$ and forms a vector $\overline{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$, i.e. unmask the code sequence $c^*_{X_i}$.

After substitution, we get the equality:

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

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

An authorized user who has generated a vector $\overline{c}^*$ has the ability to apply a fast algorithm for noise-immune decoding and form vectors

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

and $M_i^u = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$ to restore the balanced sequence M_i. It is enough to multiply the vector M_i^u on the masking matrices D^u и P^u but in 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 error vector e: $M = M_i + IV$

The encryption/decryption algorithms analysis shows that if the cryptogram is implemented after the generating of error vector (with balanced coding algorithm based on the IV) h_e will be shorted(symbols of the error vector equal to zero), $|h|=1/2e$, i. e. $e_i = 0, \forall e_i \in h$.

To get information we set "zero" shortening symbols in the decryption process.

Niederreiter encryption algorithm:

Step 1. Enter the information and public key H_X^{EC}.

Step 2. Form the error vector e with weight that does not exceed $\le t$ (the corrective power of the elliptic code based on the non-binary balanced coding algorithm [13, 14]).

Step 3. Form a shortened error vector: $e_x=e(A) – IV$

Step 4. Form codogram

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

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

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

***Decoding algorithm Niederreiter*:**

Step 1. Obtain the text of the codogram by using MV2 algorithm:

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

Step 2. Enter the S_X code that should be decoded. Enter private key - matrix *X, P, D*.

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

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

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

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

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

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

Step 7. Form the error vector e: $e = e_x + IV$

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

The proposed models and practical algorithms allow to reduce the energy costs by 12–15 times [23] and ensure the formation of a strong authentication protocol based on OTP passwords.

Development of two factor authentication protocol on hybrid designs crypto code of unprofitable codes. The analysis attacks on multifactor authentication

schemes authenticator using OTP-password allows us to formulate the basic requirements for the following protocols:

– an increase in multi-factor authentication;

– increasing the length of secrets, sustainable use of standard encryption algorithms;

– use encryption procedures in the transmission channels open Internet (GMI), open mobile networks;

– increasing requirements of safety in the system and network devices GMI and mobile networks;

– improving information and cyber literacy users.

To meet the requirements of the authors proposed to use a crypto-code system considered in [23]. The practical crypto algorithms hybrid coding structures on unprofitable codes that allow improved multi-authentication scheme to enhance the reliability and reliability authenticator, which is formed.

For this bank card (BC) should keep the following data elements [23]:

(1) Index of public key certificate authority – so that the terminal can handle multiple certification centers, this value specifies that the keys must use the terminal when working with this card;

(2) the public key certificate issuer – signed by the Certification Center;

(3) Public Key Certificate BC – signed by the issuer and is based MNCCS McEliece;

(4) module and the public key exponent of the issuer;

(5) module and the public key exponent BC;

(6) The secret key BC.

The terminal that supports multifactor authentication scheme, should keep public keys of all CAs and associated information related to each of the keys.

The terminal should also be able to choose the appropriate key index based on (1) and some special identity.

To support multifactor authentication bank card the user should have its own key pair (public and private key authenticator). The public key is stored on the BC in BC public key certificate. Each public key BC certified by the issuing bank, and trusted certification authority certifies the public key of the issuing bank. This means that the authenticator to verify the card terminal must first check the two certificates to authenticate and restore BC's public key, which is then used when checking authenticator BC.

The process proposed authentication method consists of five steps:

(1) Restore the terminal public key certificate authority. The terminal reads the code (1) identifies and extracts the module public key certificate authority stored in it – masking matrix (*X, P, D*), the equation curve geometrical code (AGC) and associated information, chooses the appropriate algorithms.

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

(3) Formation authenticator on the basis of McEliece MNCCS. Getting codeword (authenticator) by adding the received codeword with the session key.

(4) Formation of unprofitable text authenticator and loss [23, 24].

(5) Check the validity authenticator. Finding a multiplicity of vector errors and comparison of obtained. The structure of the proposed method of two-factor authentication based on HCCDUC shown in Fig. 7.

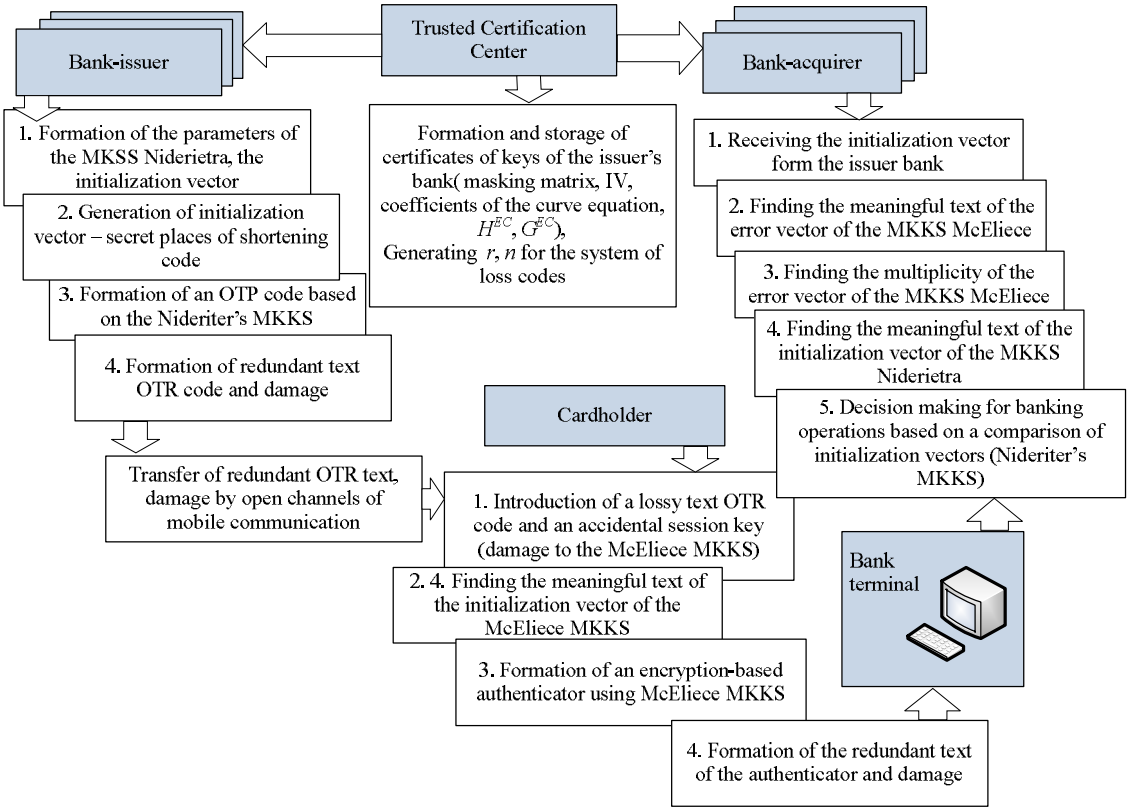


Fig. 7. Block diagram of the improved method based 2FA HCCDUC

Thus, hybrid crypto-code constructions on unprofitable codes can increase the number of token authenticator, use two asymmetric crypto-code system, two / four channels unprofitable text authenticator and loss.

Scalable software module by changing the parameters MNCCS Niederreiterand / or McEliece, depending on the requirements put forward communication channel ABS ensures its implementation in mobile gadgets and compatibility with the protocols of Internet banking OPS.

Studying the properties of the proposed method of two-factor authentication.

The improved method of rigorous two-factor authentication password OTP-based crypto-code constructions MNCCS McEliece and Niederreiter eliminates the main drawback of this protocol 2FA – transfer some token authenticator open channels of mobile communication. Block diagram of the practical implementation of proposed 2FA on HCCDUC shown in Fig. 8.

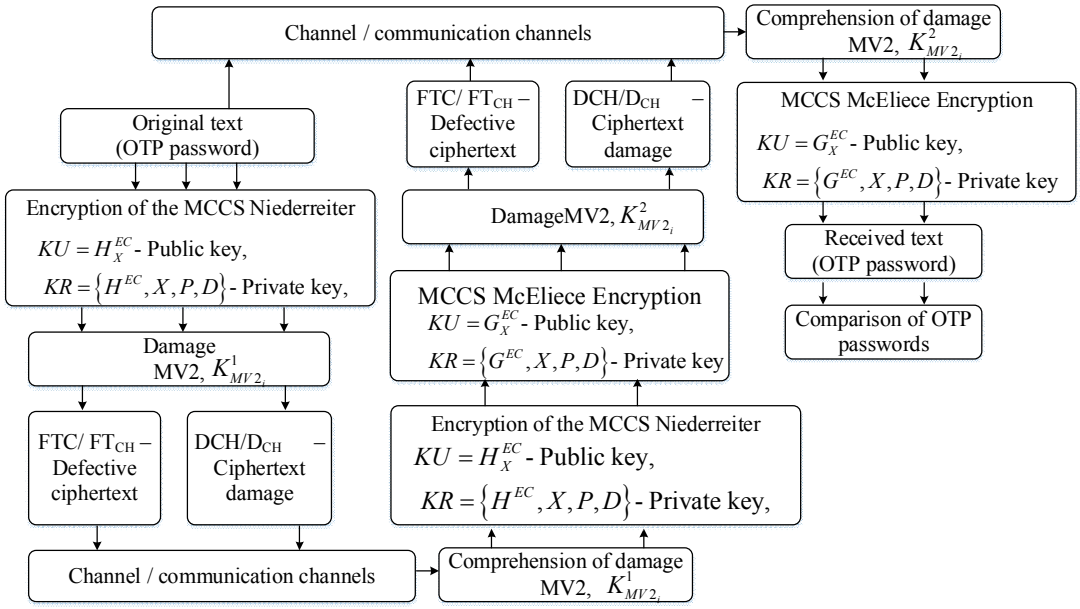


Fig. 8. Implementation structural diagram

Evaluation of the reliability of the proposed MNCCS on unprofitable codes.

To assess the reliability of use proposed in [23] entropy method of reliability assessment.

The proposed hybrid cryptosystem is comparable to the stability of the damage to the second method – damage to ciphertext, considered in [23].

In this case we have a set of ciphertext unprofitable and loss, all individually do not meet the initial meaningful text.

The cryptographic strength evaluation of the proposed algorithms. To assess the algorithms strength, we use the entropy method [1] and the structural diagram shown in Fig. 8.

The proposed hybrid cryptosystem is comparable in stability with the causing damage method - damaging the cipher text in [23, 24].

In this case, we have a set of defective ciphertexts and damages, and all of them do not correspond to the original plain text.

With a complete set of defective ciphertexts and all damages, the unicity distance increases due to additional key damage of the ciphertext.

Thus, additional encryption allows to obtain an increased uniqueness distance:

$$\aleph = H\left(H^{EC}\right) + H\left(X_N^{EC}\right) + H\left(P_N\right) + H\left(D_N\right) +$$
$$+H\left(G^{EC}\right) + H\left(X_{Mc}^{EC}\right) + H\left(P_{Mc}\right) + H\left(D_{Mc}\right) +$$
$$+\sum_{i=1}^{m} H\left(\left(K^i_{MV2_N}\right) + H\left(K_i\right)\right) +$$
$$+\sum_{i=1}^{m} H\left(\left(K^i_{MV2_{Mc}}\right) + H\left(K_i\right)\right);$$
$$U_0 = \aleph / B \log |I|,$$

where U_0 – Uniqueness distance, H^{EC}, X_N^{EC}, P_N, D_N – Personal key in the NJC Niederreiter, G^{EC}, X_{Mc}^{EC}, P_{Mc},D_{Mc}– Personal key in NJC McEliece, $K^i_{MV2_N}$ – Key in the NDC of the Niederreiter Committee on Damaged Codes, $K^i_{MV2_{Mc}}$ – Key in the McEliece on defective codes, $|I|$ – Number of meaningful texts, B – Source code, redundancy, m – Number of damages.

Expression (1) makes it possible to estimate the stability of the proposed hybrid crypto-code constructions of McEliece and Niederreiter on defective codes. The proposed method provides strict protocol continued use of OTP authentication password, no significant change channels, improve performance software used encryption algorithms that provide hybrid attacks on opposition cybersecurity.

Conclusions

1. The analysis of multifactor authentication methods has shown that 95% of bank customers use e-

banking. It is usually based on multifactorial OTP authentication. However, the use of OTP passwords in open data transmission systems does not meet the security requirements. NIST experts recommend using additional authentication factors with mandatory transfer of OTP passwords in encrypted form and/or through closed communication channels. To solve the problem we propose the method of improving 2FA based on the hybrid crypto-code constructions.

2. We proposed innovative mathematical models and encryption/decryption algorithms for cryptograms in hybrid crypto-code constructions based on modified Niederreiter and McEliece crypto-code systems on flawed codes. They are more effective because of the shortening the error vector symbols (initialization vector) and provide required cryptographic stability in the data transmission in open mobile channels.

3. The developed scheme of multifactor authentication based on the Niederreiter – McEliece allows to eliminate a significant 2FA deficiency in SMS by providing confidential transmission of the OTP password via mobile communication channels. The conducted researches confirm that the application of these algorithms provides high performance, stable work based on the theoretic-complexity problem of random code decoding ($10^{30} – 10^{35}$ group operations), and reliability based on the use of a truncated algebraic geometric code ($P_{err} 10^{-9} – 10^{-12}$).

To reduce the alphabet power (the Galois field up to GF ($2^4 – 2^6$) we propose to use systems on defective codes, that allows to form multi-channel cryptosystems simultaneously.

Reference

1. Scott, Rose (2016), *Domain name systems-based electronic mail security*, available to: https://nccoe.nist.gov/sites/default/files/library/sp1800/dns-secure-email-sp1800-6-draft.pdf
2. Quynh, Dang (2012), *Recommendation for Applications Using Approved Hash Algorithms*, available to: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
3. Schneider, Bruce (2016), *Applied cryptography. Protocols, algorithms, source texts in the C language*, available to: https://www.labirint.ru/books/345501/
4. Digital Identity Guidelines (2018), available to: https://doi.org/10.6028/NIST.SP.800-63b
5. The Cybersecurity Framework (2019), available to: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf.
6. Guide to LTE Security (2019), available to: csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
7. Shapiro, Leonid (2012), *Authentication and one-time passwords. Theoretical basis. Part 1*, available to: https://elibrary.ru/item.asp?id=20464464
8. Shapiro, Leonid (2012), *Authentication and one-time passwords. Part 2. Implementing OTP for authentication in AD*, available to: https://elibrary.ru/item.asp?id=20464277
9. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash (2019), available to: https://csrc.nist.gov/publications/.../800-185/sp800_185_draft.pdf.
10. Evseev, S.P. and Abdullaev, V.G. (2015), "Algorithm for Monitoring the Two-Factor Authentication Method Based on the Passwindow System", *East European Journal of Advanced Technologies*, Issue. 2/2 (74), pp. 9–15.
11. Evseev, S.P., Abdullaev, Zh., Agazade, F. and Abbasova V.S. (2016), "Improvement of the method of two-factor authentication based on the use of modified crypto-code schemes", *System of information boxes*, No. 9 (146), pp. 132–145.
12. Evseev, S.P., Kots, G.P. and Lekarev E.V. (2016), "Development of the method of multifactor authentication based on the modified Niedereiter-McEliece crypto-code systems", *East-European Journal of Advanced Technologies*, 6/4 (84), pp. 11–23.
13. Robert, Hackett (2016), *You're implementing this basic security feature all wrong*, available to: http://fortune.com/2016/06/27/two-factor-authentication-sms-text/
14. Guide for Cybersecurity Event Recovery (2019), available to: https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf
15. Security requirements for cryptographic modules (2019), available to: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
16. Annex A: Approved Security Functions for FIPS PUB 140-2 (2019), available to: csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf
17. Annex B: Approved Protection Profiles for FIPS PUB 140-2 (2019), available to: csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf
18. Annex C: Approved Random Number Generators for FIPS PUB 140-2 (2019), available to: https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf
19. Evseev, S.P., Rzaev, Kh.N. and Korol, O.G. (2016), "Development of the modified asymmetric crypto-code system of McEliece on truncated elliptic codes", *East European Journal of Advanced Technologies*, Kharkiv, Is. 4/9 (82), pp. 4–12.
20. Mishchenko, V. A. and Vilansky, Yu. V. (2007), *Damage texts and multichannel cryptography*, Encyclopedic, Minsk, 292 p.
21. Mishchenko, V. A. ,Vilansky, Yu. V. and Lepin, V.V. (2006), *The cryptographic algorithm MV 2*, Minsk, 177 p.
22. Shannon, K.E. (1963), "The theory of communication in secret systems", *Work on the theory of information and cybernetics*, Moscow, pp. 333–402.
23. Hryshchuk, R., Yevseiev, S. and Shmatko, A. (2018), *Construction methodology of information security system of banking information in automated banking systems*, monograph, Premier Publishing s. r. o., Vienna, 284 p.
24. Schwartz, M. J. (2011), "Zeus Banking Trojan Hits Android Phones", *Information week*, available: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909
25. Trojan Writers Target UK Banks with Botnets (2010), TechWorld, available to: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets
26. Grishchuk R., Danik Yu. (2016), *Fundamentals of cyber security*, Zhitomir: ZHNAEU, 228 p.
27. Kiberbezopasnost 2016–2017: Otitogov k prognozam (2017), available to: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf

28. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack (2019), available to: http://storage.pardot.com/44731/127332/Cybercrime_Trends_Report___2016_Year_in_Review__1_.pdf
29. HP research: average annual damage from cyber attacks increased up to 15 million USD for organization (2015), available to: http://www.connect-wit.ru/issledovanie-hp-crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organizatsiyu.html
30. Data Bank of Information Security Threats (2019), available to: http://bdu.fstec.ru/vul
31. Guide for Cybersecurity Event Recovery (2019), available: https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf
32. Guide to LTE Security, [Online]. Available: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf

Received (Надійшла) 21.05.2019
Accepted for publication (Прийнята до друку) 24.07.2019

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Євсеєв Сергій Петрович – доктор технічних наук, старший науковий співробітник, завідувач кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені С. Кузнеця, Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Senior Research, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: serhii.yevseiev@hneu.net; ORCID ID: https://orcid.org/0000-0003-1647-6444

Бекірова Лала Рустамівна – доктор технічних наук, доцент, завідувач кафедри інструментальної інженерії, Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан;
Lala Bakirova Rustam – Doctor of Technical Sciences, Associate Professor, Head of Department "Instrumentation Engineering", Azerbaijan State Oil and Industry University; Baku, Azerbaijan;
e-mail: lala_bekirova@mail.ru; ORCID ID: http://orcid.org/0000-0003-0584-7916

Сущенко Марія – магістрант, Університет науки і техніки Китаю, Китай;
Mariia Sushchenko – masters student, University of Science and Technology of China, China;
e-mail: MSushchenko@gmail.com; ORCID ID: http://orcid.org/0000-0002-3275-235X

Математичні моделі крипто-кодових конструкцій на збиткових кодах

С. П. Євсеєв, Л. Р. Бекірова, М. Сущенко

Анотація. Предметом дослідження є математичні моделі побудови гібридних (комплексних) криптосистем на основі крипто-кодових конструкцій Мак-Еліса на збиткових кодах. **Метою** даної роботи є побудова криптостійких механізмів в умовах постквантовой криптографії для забезпечення основних послуг безпеки. Використання крипто-кодових конструкцій в механізмах суворої автентифікації на основі OTP-паролів. Розробка практичних алгоритмів їх реалізації на основі пропонованих математичних моделей. **Завдання**, які необхідно вирішити – аналіз основних загроз використання OTP-паролів ; аналіз основ побудови і використання багатоканальних криптографічних систем на збиткових кодах; формальний опис математичних моделей гібридних крипто-кодових конструкцій на збиткових кодах на основі модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера на модифікованих еліптичних кодах; розробка алгоритмів шифрування і дешифрування даних в гібридних крипто-кодових конструкціях Мак-Еліса – Нідеррайтера. **Висновок:** запропоновані в статті комплексні механізми захисту забезпечують використання протоколу суворої автентифікації в умовах постквантової криптографії на основі OTP-паролів. Використання збиткових кодів розширює можливості використання крипто-кодових конструкцій за рахунок значного зниження потужності алфавіту зі збереженням необхідного рівня криптостійкості

Ключові слова: гібридні крипто-кодові конструкції; крипто-кодові конструкції Мак-Еліса; криптографія на збиткових кодах.

Математические модели крипто-кодовых конструкций на ущербных кодах

С. П. Евсеев, Л. Р. Бекирова, М. Сущенко

Аннотация. Предметом являются математические модели построения гибридных (комплексных) криптосистем на основе крипто-кодовых конструкций Мак-Элиса на ущербных кодах. **Целью** работы является построение криптостойких механизмов в условиях постквантовой криптографии для обеспечения основных услуг безопасности. Использование крипто-кодовых конструкций в механизмах строгой аутентификации на основе OTP-паролей. Разработка практических алгоритмов их реализации на основе предлагаемых математических моделей. **Задачи**: анализ основных угроз использования OTP-паролей; анализ основ построения и использования многоканальных криптографических систем на ущербных кодах; формальное описание математических моделей гибридных крипто-кодовых конструкций на ущербных кодах на основе модифицированных крипто-кодовых систем Мак-Элиса и Нидеррайтера на модифицированных эллиптических кодах; разработка алгоритмов шифрования и дешифрования данных в гибридных крипто-кодовых конструкциях Мак-Элиса – Нидеррайтера. **Вывод**: предлагаемые в статье комплексные механизмы защиты обеспечивают использование протокола строгой аутентификации в условиях постквантовой криптографии на основе OTP-паролей. Использование ущербных кодов расширяет возможности использования крипто-кодовых конструкций за счет значительного снижения мощности алфавита с сохранением требуемого уровня криптостойкости.

Ключевые слова: гибридные крипто-кодовые конструкции; крипто-кодовые конструкции Мак-Элиса; криптография на ущербных кодах.