UDC 004.056:355.45 doi: https://doi.org/10.20998/3083-6298.2025.02.04

Serhii Yevseiev[1], Bogdan Tomashevsky[2], Tetiana Milevska[1], Yelyzaveta Sevriukova[1], Roman Korolov[1]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine
[2] Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

SECURE DISSEMINATION OF COMBAT COMMANDS IN HYBRID WARFARE

Abstract. Topicality. Conducting hostilities in hybrid warfare, accompanied by the digitalization of command and control processes, requires new methods of secure transmission of combat orders and confidential information. The use of traditional automated combat control systems (ACCS) is insufficient due to their vulnerability to electronic countermeasures and limited applicability in support units. **The subject of study** in the article are methods of secure dissemination of combat commands in open and closed communication channels using multi-channel cryptography and post-quantum algorithms. **The purpose of the article** is to develop a new approach for secure transmission of classified information that ensures resistance to current and future cyber threats, minimizes interception risks, and optimizes financial and energy costs. **The following results** were obtained. A model of secure data dissemination based on the principle of “scattering” with multi-channel cryptography on flawed codes is proposed. The developed mechanism guarantees message recovery even in the case of partial fragment loss, increases resilience against interception, and reduces the probability of content disclosure. Comparative analysis demonstrates the advantages of post-quantum crypto-code structures, which combine protection and error correction, surpassing classical symmetric and elliptic-curve systems. **Conclusions.** The integration of post-quantum algorithms with flawed code-based cryptography enables the effective use of both open (mobile, wireless, Internet) and closed communication channels for transmitting combat orders. This provides a reliable foundation for enhancing the resilience of military command systems under hybrid warfare conditions.

Keywords: cryptography on flawed codes; hybrid warfare; automated control system; bringing combat commands; post-quantum cryptography.

Introduction

Shamir's information security and network security require the sharing of secrets in any application used, and in hybrid warfare is an integral part of the management of forces and means. To ensure security, a secret sharing scheme with a threshold (t, n) is used, which allows the secret value S to be distributed among “n” control nodes; so at least (t<n) players are required to recover the secret. Polynomial interpolation and hyperplane geometry are two different types with secret sharing.

Almost all forms of communication and information storage today are in digital form. The security of digital media is a major concern. This led to the development of encryption and cryptography. Mathematicians, cryptographers, and security engineers are more involved in sharing secrets. Naturally, the issue of ensuring security in the conditions of hostilities (power and cyber-physical) phase requires the improvement of mechanisms and procedures for ensuring security, especially when transmitting critical information (combat orders for the movement of forces and means, the performance of combat missions, etc.). At the same time, it is necessary to take into account both the time of “relevance” of this information and the capabilities of the enemy’s anti-radar weapons. The applied regular forces and means of communication do not provide the required level of security, and are practically not suitable for solving such problems. Communication channels can either be muted, blocked, or hacked by the enemy. The use of mobile, wireless Internet channels is associated with the risks of interception, as well as blocking. Thus, the actual problem is the formation of new approaches to the use of all possible communication channels (including open wireless, mobile Internet channels), but with the required security level [1-9].

1. Main research

To ensure security in a full-scale quantum computer, it is not enough to use encryption (symmetric systems can be hacked based on the Grover algorithm, asymmetric systems – based on the Shor algorithm). Thus, it is necessary to combine encryption systems based on quantum algorithms and secret sharing – randomly splitting critical (secret) information into blocks with subsequent transmission over various communication channels. To date, there are three approaches to sharing secrets, which are shown in Fig. 1. This is defined by the protocol, where t stands for power, s stands for secret, and n stands for participant. The secret can only be extracted if the number of participants is greater than the number of elements [6–8].

In general, a protected special purpose information network is a global network, which includes dozens or hundreds of local networks.

To reduce the probability of unauthorized access to confidential data, or data containing state or military secrets, special separate secure information networks are created to serve state authorities, state special communications, military and defense departments and facilities, banking structures and others large state organizations. Such networks, as a rule, do not have a connection to the Internet and form secure information networks of integrated service or secure information networks of special purpose.

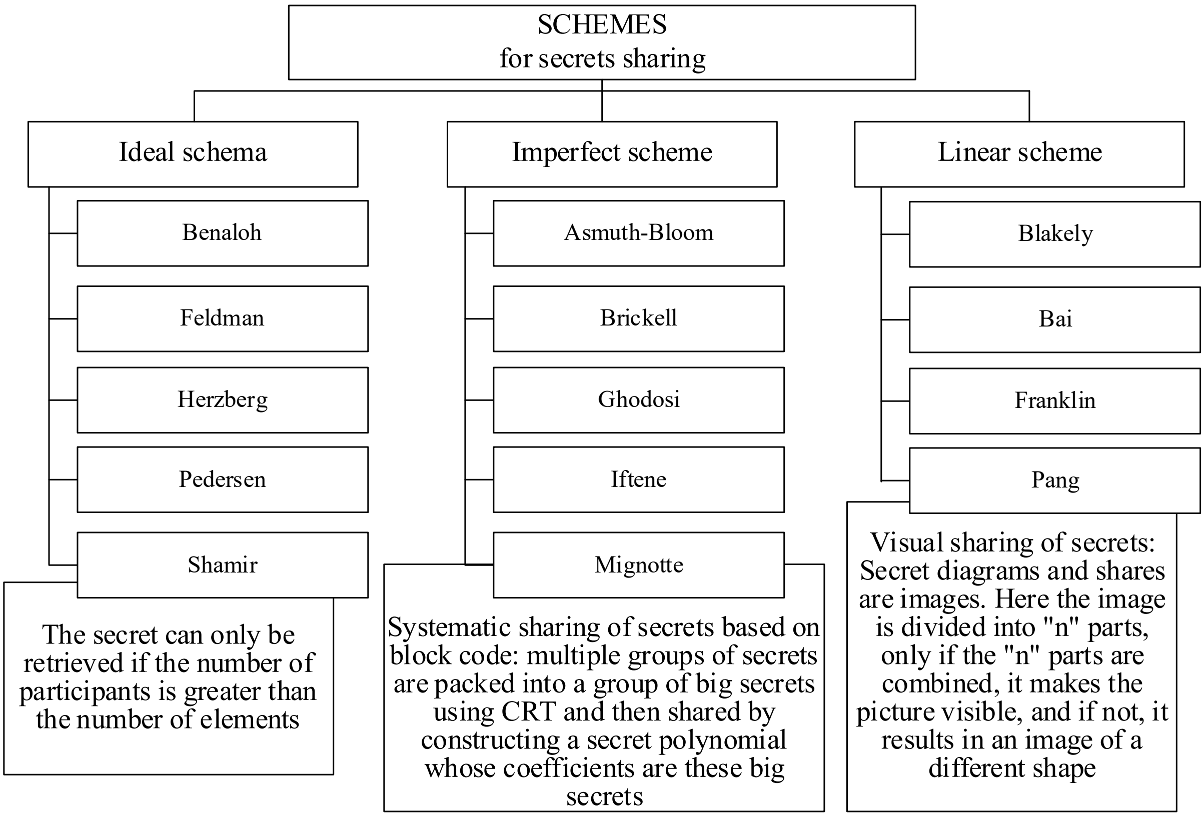

SCHEMES
for secrets sharing
Ideal schema
Imperfect scheme
Linear scheme
Benaloh
Feldman
Herzberg
Pedersen
Shamir
Asmuth-Bloom
Brickell
Ghodosi
Iftene
Mignotte
Blakely
Bai
Franklin
Pang
The secret can only be retrieved if the number of participants is greater than the number of elements
Systematic sharing of secrets based on block code: multiple groups of secrets are packed into a group of big secrets using CRT and then shared by constructing a secret polynomial whose coefficients are these big secrets
Visual sharing of secrets: Secret diagrams and shares are images. Here the image is divided into "n" parts, only if the "n" parts are combined, it makes the picture visible, and if not, it results in an image of a different shape

Fig. 1. Secret Sharing Schemes

In this work, the main attention is paid to ensuring a high level and efficiency of protection of confidential information transmitted in protected special purpose information networks. New highly effective methods of information transmission are proposed, the essence of which is to divide information files into parts randomly, use different keys and methods of information encryption, use different containers to hide the received parts of information, transfer these encrypted parts at different times and by different routes. To ensure security, it is suggested to use the approach of damage based on the use of hybrid crypto-code structures on damaged codes [9, 10]. such an approach will allow the use of post-quantum algorithms on various codes, which in turn can provide the required level of security depending on the criticality (secrecy) and the time of secret information "relevance".

To transfer secret information in open networks and networks for special purposes, it is proposed to use the following model.

A string of N bytes constitutes a file F to be transferred or stored. Each byte, denoted by b_j, j=1, ..., N – it is, for example, an eight-bit byte representing an integer in the range 0 to 255:

$$F = b_1, b_2, ..., b_N$$

$01101100_2=108_{10}$

Byte b_1 is shown as representing $108_{\text{base}10}$. Thus, for some prime number p greater than B (where B is the upper end of the range of integers represented by eight-bit bytes, i.e. 255), the file F is a string of characters b_j, each of which is the remainder modulo p, i.e. element of the finite field Z_p = remainders modulo p.

For example, if p=257, then the byte b=11001011=$203_{\text{base}10}$ is represented as the remainder of b (mod p), namely 203 (mod 257). Any finite field that contains at least as many elements as there are possible characters in the alphabet of characters that make up F can be used. The Z_p field mentioned above has 257 elements and therefore requires 9 bits to represent all possible elements, that is, one bit more than the 8-bit length b_j. Alternatively, for q-bit bytes, the $E=GF(2^q)$ field can be used, for example, for 8-bit bytes, we can use the $E=GF(2^8)$ field of characteristic 2, which has 256 elements. We only need an irreducible polynomial $p(X)$, an element $Z_2[X]$ of degree 8, in order to efficiently perform calculations in the field E [6–8].

We are going to get from the information component F, the number of parts that need to be stored or transmitted. We expect that no more than a certain number (denoted k) of parts will be lost during storage or transmission. Our goal is to reconstruct F from the remaining pieces (numbered at least m). Then n=m+k will be the number of original parts. Given k, we choose m so that n/m does not exceed 1+ε for some acceptable value. That is, n is greater than m by at most an amount that makes n/m greater than 1. For example, n, m, and k could be 6, 4, and 2, respectively. In this case, any two parts may be lost, and the file will be restored from the remaining four parts; then it will be 1/2, i.e., the information costs for this degree of fault tolerance are only 50%. If n, m and k were instead of 6, 5 and 1, then ε would be 1/5, the information cost is only 20%. Thus, ε is a measure of how many lost parts can be tolerated as a proportion of the number of surviving parts without jeopardizing the possibility of recovering F.

To generate n parts that will be transmitted or stored, given the source file F (Fig. 2), we first select n vectors a_i, each of which consists of m coordinates $a_{i,1}$, ..., $a_{i,m}$, which use all elements of the final field:

$$\begin{cases} a_1\left(a_{1,1}...a_{1,m}\right) \\ \vdots \\ a_n\left(a_{n,1}...a_{n,m}\right) \end{cases}$$

The coordinates m for each vector a_i are chosen so that any subset of m vectors a_i is linearly independent (or at least so that a randomly selected subset of m vectors a_i is linearly independent with high probability) (Fig. 2).

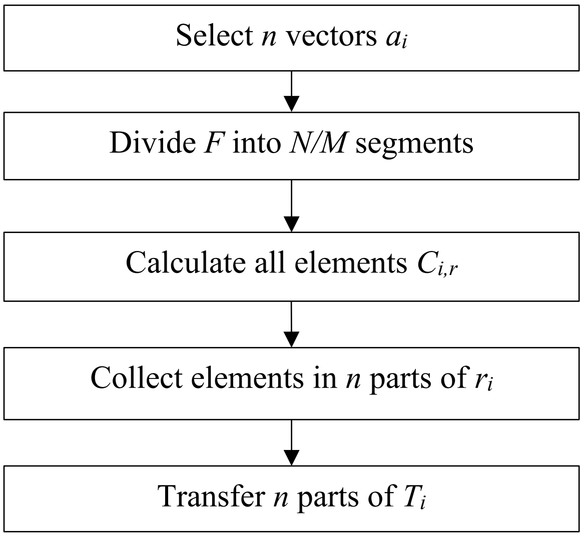

Select n vectors a_i
Divide F into N/M segments
Calculate all elements $C_{i,r}$
Collect elements in n parts of r_i
Transfer n parts of T_i

Fig. 2. Block diagram of the dispersion procedure

Then we divide the characters F into N/m segments s_q of equal length, each of length m characters:

$$F = \underset{S_1}{b_1...b_m}\,\underbrace{b_{m+1}...b_{2m}}_{S_2}...\underbrace{b_{N-m+1}...b_N}_{S_{Nm}}$$

For example, if N = 10,000 and (as above) m = 4, then there are 2500 segments s_q 4 characters each.

Then the n parts to be transferred or stored, called T_i, are assembled as chains of newly constructed elements, $c_{i,r}$, i=1, . . . , n, r=1, . . . , N/m, i.e. T_i=$c_{i,1}$, . . . , $c_{i,N/m}$, i=1, . . . , n. Each element $c_{i,r}$ is calculated as the cross product in the final field of the vector a_i and the segment s_r: $c_{i,r}$ =$a_i.s_r$ =$a_{i,}1.b_{(r-1)m+1}$ +. . . +$a_{i,m}$ b_{rm}.

Then the elements are assembled into n T_i parts. Finally, the n parts T_i (and cryptographic keys, if any) are transmitted over separate communication channels or stored separately (separated in the sense that the loss of one or more parts does not necessarily mean the loss of any other parts).

Assume that after data exchange or storage, only m of the n parts of T_i are available for F to be reconstructed. (We assume that the elements of c have been subjected to standard error correction encoding and decoding, so that there are no bit errors in the m parts available for reconstruction.) Our goal is to get all the original characters (bytes) of F, i.e. b_j, j = 1,. , , , N, from elements $c_{i,r}$.

Let`s first form a square matrix A of size m×m:

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ & \vdots & & \\ a_{v,1} & a_{v,2} & \cdots & a_{v,m} \\ & \vdots & & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,m} \end{bmatrix},$$

having as rows the m initially chosen vectors a_i, so that the vectors a_v, v = 1, …, m, in matrix A, these are those m of the initial n vectors a_i that were used to generate elements c from m parts of T_i, now available for restoring F (Fig. 3). For simplicity, we assume (without loss of generality) that the matrix A contains the first m vectors a_i.

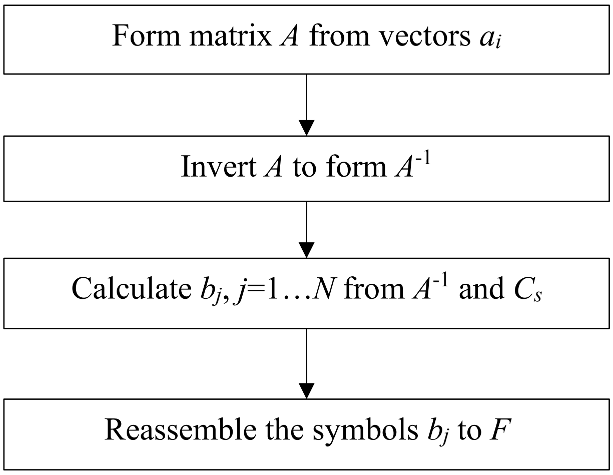

Form matrix A from vectors a_i
Invert A to form A^{-1}
Calculate b_j, j=1…N from A^{-1} and C_s
Reassemble the symbols b_j to F

Fig. 3. Block diagram of the dispersion procedure

The matrix A, multiplied by the first segment s_1 from F, generated the initial first elements $c_{1,1}$, . . . , $c_{m,1}$, from the available m parts of T_i. Thus, A multiplied by s_r, r=1, . . . , m generated all initial elements of all m available parts ща T_i:

$$A \cdot \underset{\substack{\downarrow \\ S_1}}{\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}} = \begin{bmatrix} C_{1,1} \\ \vdots \\ C_{m,1} \end{bmatrix}$$

Then we invert the matrix A times and for all to form an inverted matrix A^{-1}

$$A^{-1} = \begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,m} \\ & \vdots & & \\ d_{m,1} & d_{m,2} & \cdots & d_{m,m} \end{bmatrix},$$

where the vth line of A^{-1} is equal to $d_{v,1}, \dots, d_{v,m}$. Now it is clear that the original segments s_r, r=1, . . . , n, from F can be calculated by multiplying A^{-1} by a vector assembled from the r elements of all m available parts:

$$\underset{\substack{\downarrow \\ S_1}}{\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}} = A^{-1} \cdot \begin{bmatrix} C_{1,1} \\ \vdots \\ C_{m,1} \end{bmatrix}$$

If we express j as $j = mr + v$, where r and v – integers, $v = 1, \dots, m$, $r = 0, \dots, N/m$, then each b_j, $j = 1, \dots, N$, is calculated as row v of the inverse matrix A^{-1}, multiplied by a vector (column) consisting of the r elements of all m available parts T_i. At the end, we assemble symbols b_j to F. Let's consider a simple example (Fig. 4).

If F has a length of N = 8 bytes, if there are four parts of T_i to be transferred or stored (n=4), and if two of them will be available for recovery (m=2 and k=2), then F is divided into N/m=4 segments (s_1, ..., s_4). There are four vectors a_i, each with a length of two coordinates, and four parts T_i, each with four elements c. All operations for calculating T_{is} are performed in the finite field. Now assume that T_2 and T_4 are lost, and T_1 and T_3 are available for recovery. Then the matrix A is a 2×2 matrix, the inverse matrix A^{-1} is a 2×2 matrix with d elements, and b_s are reconstructed from d_s and c_s as described above. All operations are in the final field E used in the procedure.

$$F = \underbrace{b_1 b_2}_{S_1} \underbrace{b_3 b_4}_{S_2} \underbrace{b_5 b_6}_{S_3} \underbrace{b_7 b_8}_{S_4} \tag{1}$$

$$a_1 = a_{1,1}\, a_{1,2} \qquad a_3 = a_{3,1}\, a_{3,2}$$

$$a_2 = a_{2,1}\, a_{2,2} \qquad a_4 = a_{4,1}\, a_{4,2}$$

$$T_1 = C_{1,1}, C_{1,2}, C_{1,3}, C_{1,4} = \left(a_{1,1}b_1 + a_{1,2}b_2\right), \left(a_{1,1}b_3 + a_{1,2}b_4\right), \left(a_{1,1}b_5 + a_{1,2}b_6\right), \left(a_{1,1}b_7 + a_{1,2}b_8\right)$$

$$T_2 = C_{2,1}, C_{2,2}, C_{2,3}, C_{2,4} = \left(a_{2,1}b_1 + a_{2,2}b_2\right), \left(a_{2,1}b_3 + a_{2,2}b_4\right), \left(a_{2,1}b_5 + a_{2,2}b_6\right), \left(a_{2,1}b_7 + a_{2,2}b_8\right)$$

$$T_3 = C_{3,1}, C_{3,2}, C_{3,3}, C_{3,4} = \left(a_{3,1}b_1 + a_{3,2}b_2\right), \left(a_{3,1}b_3 + a_{3,2}b_4\right), \left(a_{3,1}b_5 + a_{3,2}b_6\right), \left(a_{3,1}b_7 + a_{3,2}b_8\right)$$

$$T_4 = C_{4,1}, C_{4,2}, C_{4,3}, C_{4,4} = \left(a_{4,1}b_1 + a_{4,2}b_2\right), \left(a_{4,1}b_3 + a_{4,2}b_4\right), \left(a_{4,1}b_5 + a_{4,2}b_6\right), \left(a_{4,1}b_7 + a_{4,2}b_8\right)$$

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{3,1} & a_{3,2} \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} d_{1,1} & d_{1,2} \\ d_{2,1} & d_{2,2} \end{bmatrix}$$

$$
\begin{aligned}
b_1 &= d_{1,1}c_{1,1} + d_{1,2}c_{2,1} \\
b_2 &= d_{2,1}c_{1,2} + d_{2,2}c_{2,2} \\
b_3 &= d_{3,1}c_{1,3} + d_{1,2}c_{2,3} \\
b_4 &= d_{4,1}c_{1,4} + d_{2,2}c_{2,4} \\
b_5 &= d_{5,1}c_{1,5} + d_{1,2}c_{2,1} \\
b_6 &= d_{6,1}c_{1,6} + d_{2,2}c_{2,2} \\
b_7 &= d_{7,1}c_{1,7} + d_{1,2}c_{2,3} \\
b_8 &= d_{8,1}c_{1,8} + d_{2,2}c_{2,4}
\end{aligned}
\qquad (2)
$$

Fig. 4. Illustration of scattering and reconstruction

To satisfy the requirement that the vectors a_i be linearly independent, it is possible to choose a_i, $i = 1,\ldots, n$:

$$a_j = \left(\frac{1}{x_j y_j} \cdots \frac{1}{x_j y_m} \right) \quad \begin{matrix} x_i + y_j \neq 0 \; for\ all\ i\ and\ j \\ x_i \neq x_j \; and \; y_i \neq y_j \; for\ i \neq j \end{matrix} \;, \quad (3)$$

here x_1, ..., x_n and y_1, ..., y_m – all elements of the finite field that satisfy the condition that x_i+y_j≠0 for all i and j, and for i≠j, x_i≠x_j and y_i≠y_j, that is, all x are different, all y are different, and no sum of x and y is equal to 0.

If A is a matrix which terms consist of any m vectors a_1, ..., a_n, then it is possible to show that its terms a_i are linearly independent.

The inverse matrix A^{-1} needs to be calculated only once, and it can be calculated for a proportional number of operations m^2.

Distribution and recovery methods can be implemented, for example, with the help of appropriately programmed general-purpose processors or, as shown in Fig. 5, with the help of special hardware elements.

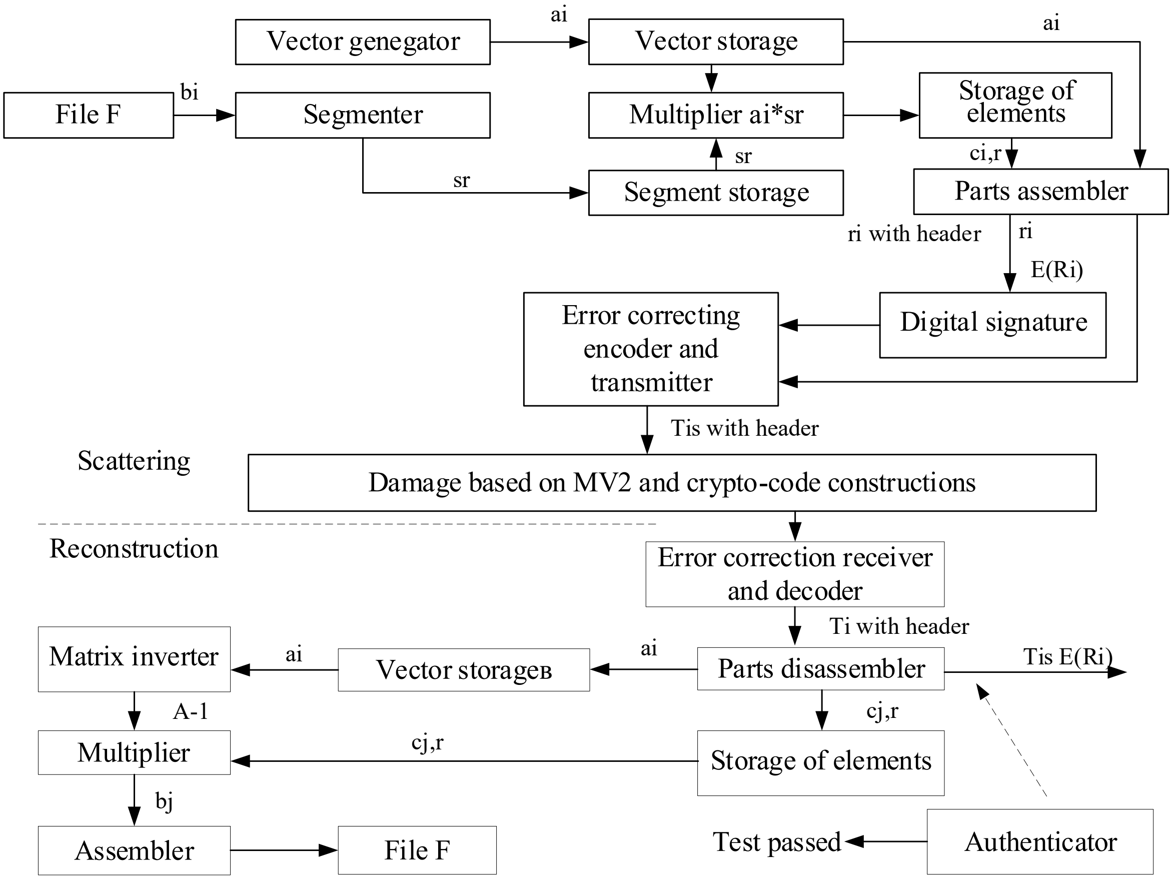


Fig. 5. Block diagram of the scattering and recovery device

In fig. 5, the segmenter accepts a sequence of symbols b_j, which make up the file F, and organizes them into segments s_r, which are temporarily recorded in the segment storage. The multiplier multiplies the symbols of various segments by the corresponding vectors a_i, which were temporarily recorded in the vector store by the vector generator (or were otherwise available in the

vector store). The resulting elements $c_{i,r}$ are temporarily stored in the element store. The element collector collects $c_{i,r}$ for each part of T_i (including for each part a header containing either the vector ai used to create the part, or simply the index of the vector if the vectors are known to the device that must perform the reconstruction). Each part of T_i can also have an electronic signature that delivers the encrypted signature $E(R_i)$ to the encoder and transmitter for transmission or storage with T_i. Then T_i fragments (and electronic signatures, if any) are sent in n independent ways to a channel or carrier using an error-correcting encoder and a transmitter.

To restore at least m out of n fragments of T_i, encoded with error correction (including headers and electronic signatures, if any), are sent to the receiver and error correction decoder, which delivers each decoded fragment of T_i (including its header) to the fragment disassembler and delivers each fragment and electronic signature in the authenticator.

The authenticator checks the electronic signature for authenticity. If the i-th test passes, the parts disassembler splits this fragment into a vector a_i (which is sent to temporary vector storage) and individual elements $c_{i,r}$ (which are sent to temporary element storage). The multiplier multiplies the vectors, each of which consists of the elements $c_{i,r}$ of the available parts, by the inverted matrix A^{-1}, which is generated from the stored vectors a_i by the matrix inverter. The resulting b_j symbols are assembled in assembler to regenerate the F file.

In works [9; 10] considered the theoretical and practical foundations of building lossy codes. Lossy text means text obtained as a result of further deformation of non-redundant letter codes [9].

Thus, a necessary and sufficient condition for the loss of a text with a loss of meaning is the reduction of the length of the codes of the text symbols beyond their redundancy. As a result, the lossy text has a length shorter than the length of the original text, and does not make sense of the original text [9].

At the same time, the amount of information expressing this orderliness will be equal to the decrease in the entropy of the text compared to the maximum possible value of entropy, that is, the equally probable appearance of any letter after any previous letter. The information calculation methods proposed in [10] make it possible to reveal the ratio of the amount of predicted (that is, formed according to certain rules) information and the amount of unexpected information that cannot be predicted in advance. Text redundancy is determined by the expression:

$$B(M) = B_A L_0 = \left(log\, N - \frac{H(M)}{L_0} \right) \times L_0, \tag{4}$$

where M – initial text; B – redundancy of language ($B = R - r$; R – redundancy of language ($R = \log N$; N – alphabet power; r – language entropy per symbol, $r = H(M)/L$; L – message length M in language symbols)); $H(M)$ – entropy (uncertainty) of the message; L_0 – message length in M language symbols with content; B_A – redundancy of language.

To obtain flawed text (FTC) and loss (DCH), the “perfect” compression method is used after performing m cycles of the loss assignment mechanism C_m [9, 10].

The number of cycles required to reduce the length of the initial text is equal to:

$$m \rangle \frac{log\, n - B_A}{log\, \eta}, \tag{5}$$

where n – representation power of the source text symbol; B_A – redundancy of language; η – the number of times the initial text length is reduced in $MV2$ at each step (some constant factor).

A quantitative measure of the efficiency of inflicting damage is the degree of change of meaning, which is equal to the difference in the entropies of the damaged text and the original text at different segments of the length of the damaged text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i) p_i, \quad \sum_{i=1}^{s} p_i = 1, \quad s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right], \tag{6}$$

where M_i – part of the source text corresponding to the i-th segment; p_i – its probability; L_0 – length of M_i, which is equal to the length L_{FTC} – flawed text; s – the number of segments.

For the ergodicity of the symbol source of the source text, we have:

$$d_{max} = log\, L_{FTC} - H(M_i). \tag{7}$$

Fig. 6 shows the structural diagram of one step of the universal damage mechanism.

The *information core* of a certain text is understood as the flawed text CFT, obtained as a result of the cyclic transformation of the universal mechanism for causing damage C_m.

Universal damage mechanism C_m can be described as [9,10]:

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

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

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

where

$$CFT / CH_{FT} = CFT / CH^{i}_{FT},...,CFT / CH^{m}_{FT},$$
$$KU^{EC} = \varphi(K^{i}_{D},...,K^{m}_{D}, KU^{EC}_{1},...,KU^{EC}_{m}, \qquad .$$
$$CHD / CH_{D} = CHD / CH^{i}_{D},...,CHD / CH^{m}_{D}$$

Thus, as a result, we have two ciphertexts (damage (*CHD*) and flawed text (*FTC*)), each of which does not make sense either in the alphabet of the initial text or in the alphabet of the ciphertext. In fact, the ciphertext of the original message (*M*) is presented as a combination of two lossy ciphertexts, each of which individually cannot restore the original text.

It is not necessary to know the intermediate damage sequences to restore the original sequence. It is necessary to know only the last damage sequence (the last flawed text after the execution of all cycles) and all damage with the rules of their application.

The *unity distance* for a model of a random cipher for which there is a probability of obtaining a meaningful text upon a random and equally likely selection of the key *K* and an attempt to decipher the ciphertext at $N_S = H(K)\dfrac{2^{HL}}{|I|^{L}} = 1$ is equal to:

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B\log|I|}, \tag{8}$$

where *B* – redundancy of the original text; *H* – entropy per letter of meaningful text in the input alphabeti *I*, |*I*| >2; 2^{HL} – approximate value of the number of meaningful texts.

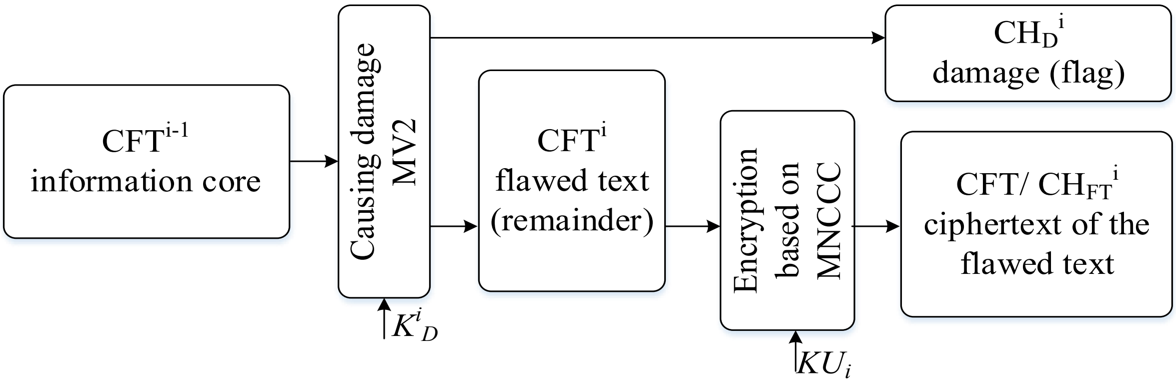
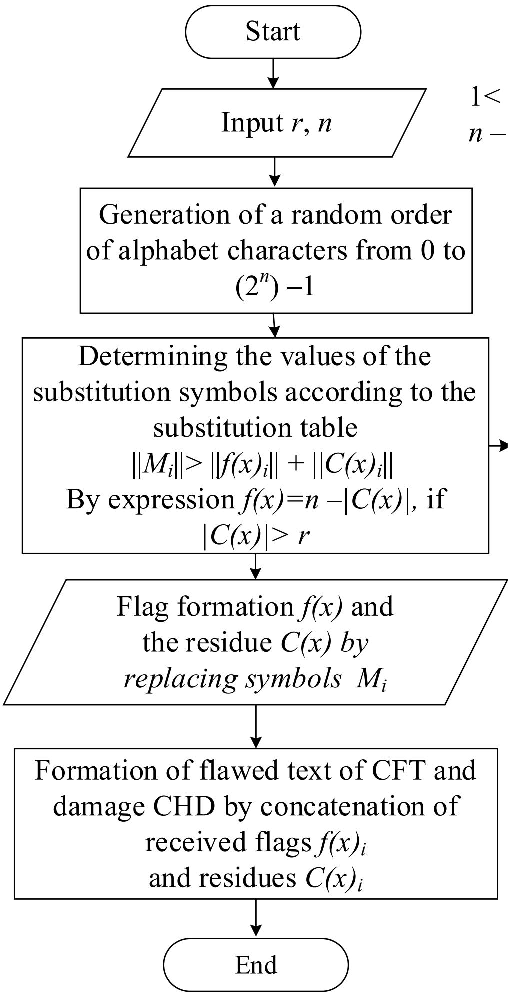

CFT^{i-1} information core
Causing damage MV2
CFT^{i} flawed text (remainder)
Encryption based on MNCCC
CH_D^{i} damage (flag)
CFT/ CH_{FT}^{i} ciphertext of the flawed text
K^{i}_{D}
KU_i

Fig. 6. Block diagram of one step of the universal damage mechanism

In works [9; 10] the cyclic algorithm for obtaining flawed texts is understood as a universal mechanism for causing damage (C_m, where *m* – number of cycles), which consists in randomly replacing the bit representation of each character of the source text with a tuple of a smaller or equal number of bits, followed by their concatenation.

Fig. 7 shows the universal mechanism for inflicting damage (*MV2* algorithm (formation of flawed text)).


Start
Input r, n
Generation of a random order of alphabet characters from 0 to $(2^n) - 1$
Determining the values of the substitution symbols according to the substitution table
$\|M_i\| > \|f(x)_i\| + \|C(x)_i\|$
By expression $f(x) = n - |C(x)|$, if $|C(x)| > r$
Flag formation $f(x)$ and the residue $C(x)$ by replacing symbols M_i
Formation of flawed text of CFT and damage CHD by concatenation of received flags $f(x)_i$ and residues $C(x)_i$
End

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

Symbol	Residue length	Residue $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
...	…	…	…
S_{2^n}	r	1^r	0^{n-r}

CFT/ CH_{FT} – ciphertext of the flawed text
CHD/CH_D – damage cipher text
FTC/ FT_{CH} – damaged cipher text
DCH/D_{CH} – cipher text damage
$f(x)$ – flag (damage)
$C(x)$ – residue (damaged code)

Fig. 7. Universal damage mechanism – MV2 algorithm (formation of flawed text)

The scope of definition of the transformation in the *MV2* algorithm is a set $\{0, 1\}^n$ – we consider it as the power of the alphabet of some family of source texts, which is associated with a certain probability distribution of the letters of this alphabet, and the symbols of the source text are the values of a discrete random element [9]. Let X be a random discrete element that acquires a value $x_i \in \{0,1\}^n$ with probability p_i, and $T = (c, f) \in F_n^r$ – arbitrary fixed transformation *MV*2.

Then for any $y \in U_{r\,n-1}$ (some binary string from a set of strings of variable length) and for any $1 \le i \le |y|$ the following equality holds:

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

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

$$H(FTC / FT_{CH}) \le \log(2^n - 2^r),\ H(CHD) \le \log(n - r + 1).$$

Thus, with a uniform distribution of inputs (flags) of the *MV2* algorithm, a uniform distribution of the output (residue) is formed:

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

The conducted analysis of methods of inflicting damage [9, 10] showed that the first and second methods of inflicting damage with subsequent crypto-transformation are the most suitable for use, which allows to reduce the power of the alphabet when forming a cryptogram in crypto-code structures. The distance of unity for the first method will be transformed:

$$U_0 = \frac{\sum_{i=1}^{m} \left(H\left(CHD^{(i)}\right) \right) + H(KU_i^{EC})}{B \log |I|}. \tag{9}$$

Such a system is based on the irreparability of distortion damage and ensuring stability due to the use of encryption based on crypto-code structures in the future. This leads to the impossibility of finding out the ciphertext of the flawed text.

Thus, inflicting damage will allow the use of various open communication channels (wireless, mobile, Internet channels), closed communication channels, and combat control channels. This approach significantly increases resistance to channel monitoring, hacking, and information interception.

Table 1 – **Comparative characteristics of wireless and mobile Internet technologies**

Technology	*Security services provision*					*The degree of information secrecy (βᵢ)*				
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	*1,0*	*0,75*	*0,5*	*0,25*	*0,01*
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (WiFi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE802.16m (WiMAX2)	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1 Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
Mobile technologies + CCC on EC (MEC)	+	+	+	+	+	+	+	+	+	+
Mobile technologies + HCCC on EC (MEC)	+	+	+	+	+	+	+	+	+	+
Mobile technologies + CCC on LDPC-codes	+	+	+	+	+	–	–	+	+	+

Table 1 shows the comparative characteristics of the use of crypto-code structures in the post-quantum period, taking into account the integration with various standards of wireless and mobile Internet technologies, as well as taking into account the criticality (degree of secrecy) of the information. Such an approach makes it possible to ensure the required level of operational efficiency, reliability, and stability in the conditions of conducting hostilities (hybrid wars).

Analysis of the table. 1 shows that the use of classical (symmetric) cryptosystems based on block and stream ciphers (which are used in the KNX standard) do not provide full confidentiality and integrity services. Application to ensure the distribution of key data for symmetric cryptosystems, as well as authenticity and participation services. In addition, the use of cryptosystems based on elliptic curves also does not provide the required level of resistance to hacking algorithms based on quantum computing.

Thus, to ensure security in a promising combat control system, it is proposed to use post-quantum algorithms – crypto-code constructions, which, in contrast to modern security service mechanisms (KNX standards, IEEE802.11h, IEEE802.16e - use symmetric encryption algorithms) make it possible to provide the required level of cryptographic strength. In addition, crypto-code constructions based on the proposed algebraic and/or algebraic-geometric codes allow for an integrated increase in the level of reliability (due to their error correction properties), efficiency (in terms of the speed of crypto-transformations, they are compatible with symmetric cryptography algorithms) and the required level of energy intensity, the results of comparative studies on criteria for cryptographic strength, efficiency, and energy intensity are given in [10–13].

2. Discussion of results

The results obtained in this study confirm the relevance of developing new approaches to the secure dissemination of combat orders in the context of hybrid warfare. Traditional automated control systems and classical cryptographic methods demonstrate insufficient resistance to modern threats, especially in conditions of active electronic countermeasures and the potential emergence of quantum computing. The proposed model, based on multi-channel cryptography and the concept of information "scattering" with the use of flawed codes, provides both theoretical justification and practical opportunities for strengthening confidentiality during information transmission.

A key advantage of the developed approach is the possibility of using open communication channels (wireless, mobile, Internet) without a critical decrease in the level of information security. This is especially important in the conditions of modern hostilities, where regular communication systems are often suppressed or unavailable. The dispersion mechanism and post-quantum crypto-code constructions ensure not only high cryptographic strength but also fault tolerance in case of partial loss of transmitted fragments. This significantly reduces the probability of successful interception or reconstruction of original data by an adversary.

An additional strength of the proposed solution is the combination of cryptographic and error-correction properties. This makes it possible to optimize the balance between security, reliability, and energy efficiency of transmission processes. The comparative analysis of wireless and mobile standards with the integration of crypto-code structures demonstrates that such methods provide a higher level of resistance compared to classical symmetric or elliptic-curve cryptosystems. Moreover, the use of flawed text transformation mechanisms allows achieving an additional layer of protection, as neither intercepted fragment nor damaged ciphertext retains semantic meaning without full reconstruction.

Therefore, the presented results show that the integration of post-quantum algorithms with flawed cryptography creates a promising direction for the secure distribution of combat commands. The developed model not only addresses current security gaps but also anticipates the risks of future quantum-based attacks. This makes it a practical and forward-looking solution for military communications under hybrid warfare conditions.

3. Conclusions

To ensure security in the conditions of hybrid wars, it is proposed to use all possible channels, both open and closed (regular) channels of command and control. To ensure the security of secret information, a new approach is proposed, which is based on the integration of post-quantum algorithms with flawed cryptography. In this case, not only are various channels of transmission of the key (damage) and cryptogram (damaged text) used, but before that, changes are made to the "plaintext" itself (before damage and encryption based on crypto-code structures) using secret distribution schemes.

References

1. Laptiev, O, Savchenko, V., Pravdyvyi, A., Ablazov, I., Lisnevskyi, R., Kolos, O. and Hudyma, V. (2021), "Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model", *International Journal of Communication Networks and Information Security (IJCNIS),* Vol. 13, No. 1, pp. 48–54, doi: https://doi.org/10.17762/ijcnis.v13i1.4902
2. Barabash, O., Laptiev, O., Sobchuk, V., Salanda, I., Melnychuk, Yu. and Lishchyna, V. (2021), "Comprehensive Methods of Evaluation of Distance Learning System Functioning", *International Journal of Computer Network and Information Security (IJCNIS),* Vol. 13, No. 3, pp.62–71, doi: https://doi.org/10.5815/ijcnis.2021.03.06
3. Svynchuk, O., Barabash, A., Laptiev, S. and Laptieva, T. (2021), "Modification of query processing methods in distributed databases using fractal trees", *1 International Scientific And Practical Conference "Information Security And Information Technologies",* (13-19 September, 2021). Kharkiv – Odesa, Ukraine. pp.32–37, ISBN 978-966-676-818-9
4. Vlasyk, H., Zamrii, I., Shkapa, V., Kalyniuk, A. and Laptieva, T. (2021), "The method of solving problems of optimal restoration of telecommunication signals", *IEEE 3rd International Conference on Advanced Trends in Information Theory,* ATIT, pp. 71–75.
5. Savchenko, V., Akhramovych, V., Dzyuba, T., Lukova-Chuiko, N. and Laptieva, T. (2021), Methodology for calculating information protection from parameters of its distribution in social networks, *IEEE 3rd International Conference on Advanced Trends in Information Theory,* ATIT, pp. 99–105.
6. Chandana, L. and Brajendra, P. (2001), "Evaluating damage from cyber-attacks: A model and analysis", *Systems and Humans, IEEE Transaction,* Vol. 31, No. 4, pp. 300–310, doi: https://doi.org/10.1109/3468.935047
7. Metalidou, E. "The Human Factor of Information Security: Unintentional Damage Perspective", https://www.sciencedirect.com/science/article/pii/S1877042814040440
8. Blackwell, C. (2009), "A Security Architecture to Protect against the Insider Threat from Damage", *Fraud and Theft,* https://www.researchgate.net/publication/229002207_A_security_architecture_to_protect_against_the_insider_threat_from_damage_fraud_and_theft 10.1145/1558607.1558659
9. Mishchenko, V. and Vilansky, Yu. (2007), *"Damaged texts and multichannel cryptography",* Minsk, Encyclopedic, 292 p.
10. Yevseiev, S., Ponomarenko, V., Laptiev, O. and Milov, O. (2021), "Synergy of building cybersecurity systems: monograph" / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 188 p.
11. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O., Kostiak, M., Volkov, A., Lezik, A. and Susukailo, V. (2022), "Development of crypto code structures on LDPC-codes", *Eastern-European Journal of Enterprise Technologies,* 2/9 (116), pp. 44–59.
12. Yevseiev, S. and other (2021), "Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model", *Eastern-European Journal of Enterprise Technologies,* 5/9 (113), pp. 30–47.
13. Yevseiev, S. and other (2018). "Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes", *Eastern-European Journal of Enterprise Technologies,* 6/4(96), pp. 24 –31.

Received (Надійшла) 27.08.2025
Accepted for publication (Прийнята до друку) 05.09.2025

Відомості про авторів/ About the Authors

Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;

Serhii Yevseiev – Doctor of Technical Sciences, Professor, Head of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;

e-mail: Serhii.Yevseiev@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-1647-6444;

Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190440690.

Томашевський Богдан Паїсійович – кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки, Тернопільський національний технічний університет ім. І. Пулюя, Тернопіль, Україна;

Bogdan Tomashevsky – PhD, Associate Professor, Associate Professor Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine;

e-mail: bogdan_tomashevsky@tntu.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-1934-4773; Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57208026171.

Мілевська Тетяна Сергіївна – старший викладач кафедри кібербезпеки, Національний технічний університет Харківський політехнічний інститут", Харків, Україна;
Tetiana Milevska – Senior lecturer of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: milevskats@gmail.com;ORCID Author ID: https://orcid.org/0009-0006-5218-9353;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58505618100.

Севрюкова Єлизавета Олександрівна – доктор філософії, доцент кафедри кібербезпеки, Національний технічний університет Харківський політехнічний інститут", Харків, Україна;
Yelyzaveta Sevriukova – PhD, Associate Professor of the Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: elizavetasevryukova@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-0757-490X;
Scopus ID: https://id.elsevier.com/settings/redirect?code=xaA97O7kQqL9KGS_oS5KayF4fJIPqynH9TByHmrJ.

Корольов Роман Володимирович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Roman Korolov – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: korolevrv01@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-7948-5914;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57204143490.

БЕЗПЕЧНЕ ПОШИРЕННЯ БОЙОВИХ КОМАНД У ГІБРИДНІЙ ВІЙНІ

С.П. Євсеєв, Б.П. Томашевський, Т. С. Мілевська, Є. О. Севрюкова, Р. В. Корольов

Анотація. Актуальність. Ведення бойових дій в умовах гібридних війн, що супроводжується цифровізацією управління військами, потребує нових методів захищеної передачі бойових наказів та конфіденційної інформації. Використання традиційних автоматизованих систем управління бойовими діями (АСУБ) виявляється недостатнім через їхню вразливість до радіоелектронної протидії та неможливість широкого застосування у військах забезпечення. **Предметом дослідження** є методи безпечного поширення бойових команд у відкритих і закритих каналах зв'язку з використанням багатоканальної криптографії та постквантових алгоритмів. **Метою статті** є розробка нового підходу до захищеної передачі секретної інформації, який забезпечує стійкість до сучасних і перспективних кіберзагроз, мінімізує ризики перехоплення та оптимізує фінансові й енергетичні витрати. **Були отримані наступні результати**. Запропоновано модель безпечної передачі даних, засновану на принципі «розсіювання» з використанням багатоканальної криптографії на дефектних кодах. Розроблений механізм забезпечує відновлення повідомлень навіть при частковій втраті фрагментів, підвищує стійкість до атак і знижує ймовірність розкриття змісту інформації. Порівняльний аналіз показав переваги постквантових криптокодових структур, які поєднують захист і корекцію помилок, перевищуючи класичні симетричні та еліптичні системи. **Висновок.** Інтеграція постквантових алгоритмів із криптографією на дефектних кодах дозволяє ефективно використовувати як відкриті (мобільні, бездротові, інтернет), так і закриті канали зв'язку для передачі бойових команд. Це створює надійну основу для підвищення стійкості систем військового управління в умовах гібридних війн.

Ключові слова: криптографія на основі дефектних кодів; гібридна війна; автоматизована система управління; наведення бойових команд; постквантові алгоритми.