UDC 681.32:007.5
DOI: 10.15587/1729-4061.2025.323195

DEVELOPMENT OF POST-QUANTUM CRYPTOSYSTEMS BASED ON THE RAO-NAM SCHEME

Yevhen Melenti
PhD, Associate Professor
First Vice-Rector
National Academy of the Security Service of Ukraine
Mykhaila Maksymovycha str., 22, Kyiv, Ukraine, 03066
Olha Korol
Corresponding author
PhD, Associate Professor*
E-mail: korol.olha2016@gmail.com
Volodymyr Shulha
Doctor of Historical Sciences, Senior Researcher
Rector
State University of Information and Communication Technologies
Solomyanska str., 7, Kyiv, Ukraine, 03110
Stanislav Milevskyi
PhD, Associate Professor*
Oleksandr Sievierinov
PhD, Associate Professor
Department of Information Technology Security**
Oleksandr Voitko
PhD, Associate Professor
Head of the Institute
Strategic Communications Institute***
Khazail Rzayev
Doctor of Technical Sciences, Associate Professor
Department of Computer Technologies
Azerbaijan Technical University
Javid ave., 25, Baku, Azerbaijan, AZ 1073
Iryna Husarova
PhD, Associate Professor, Professor
Department of Applied Mathematics**
Serhii Kravchenko
PhD, Associate Professor
Department of Land Forces ***
Sevinj Pashayeva
Senior Lecturer
Department of Informatics
Nakhchivan State University
Khatai neighb., Corner 17, 32D, Nakhchivan, Azerbaijan, AZ 7012
*Department of Cybersecurity
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
**Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
***National Defence University of Ukraine
Povitryanikh Sil ave., 28, Kyiv, Ukraine, 03049

The object of the research is the process of ensuring the protection of data transmission in communication channels of critical infrastructure objects based on mobile and smart technologies. The development of quantum computing technologies based on Grover and Shor algorithms provides practical cracking of symmetric and asymmetric cryptosystems in polynomial time. The emergence of systems based on artificial intelligence allows creating hybrid systems for detecting weaknesses (critical points) in security systems not only on critical infrastructure objects. In addition, a full-scale quantum computer will open a new era of implementing post-quantum cryptography algorithms. Among the winners of post-quantum algorithms, the crypto-code constructions (CCC) of McEliece and Niederreiter are separately highlighted, which allow to provide the required level of protection and the required level of reliability of information transmission in an integrated manner. But a significant drawback is the possibility of cracking such systems on linear codes, as well as the need to build them on the Galois field 210–213, which significantly reduces their use in low-capacity systems based on smart and mobile technologies. To solve this drawback, the work proposes the use of a symmetric CCC based on the Rao-Nam scheme on algebrogeometric and flawed codes, which provides the possibility of significantly reducing the volume of key data (construction of CCC over the Galois field 24–26). When using the Rao-Nam CCC, a quantum symmetric algorithm is formed, which ensures the preservation of the level of stability and reliability of information transmission (safe time 1025–1035). This approach provides the possibility of forming intelligent information protection systems (IIPS). The given structural scheme of the IIPS construction ensures timely detection of threats with an assessment of the computational and financial and human capabilities of attackers, as well as the use of the necessary CCC/algebraic (flawed) codes to ensure the required level of security

Keywords: *Rao-Nam crypto-code constructions, algebraic codes, intelligent protection systems*

Received 27.11.2024
Received in revised form 22.01.2025
Accepted date 07.02.2025
Published date 28.02.2025

How to Cite: *Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov, O., Voitko, O., Rzayev, K., Husarova, I., Kravchenko, S., Pashayeva, S. (2025). Development of post-quantum cryptosystems based on the Rao-Nam scheme. Eastern-European Journal of Enterprise Technologies, 1 (9 (133)), 35–48. https://doi.org/10.15587/1729-4061.2025.323195*

1. Introduction

The development of the computing capabilities of a full-scale quantum computer, the emergence of new areas of application of artificial intelligence, the synthesis of smart technologies with the Internet of Things forms new, more stringent requirements for the construction of information protection systems. The most widely used symmetric cryptography algo-

rithms (key length 128–256 bits) can be broken based on the quantum Grover algorithm. Cryptosystems based on public-key cryptography, including cryptography on elliptic curves, a full-scale quantum computer can solve (break) using the Shor algorithm [1–3]. Almost all asymmetric cryptography used today can be effectively broken by quantum algorithms [4, 5].

On the other hand, symmetric cryptography is able to withstand attacks by quantum computers. The best quantum attacks on symmetric ciphers and hash functions known to date use Grover's algorithm [5]. To find a 256-bit symmetric key from a set of plaintexts and ciphertexts, or to find a preimage for a 256-bit hash function, Grover's algorithm requires approximately 2128 iterations. In practice, there can be significant overhead due to quantum error correction [6, 7]. However, the advent of a full-scale quantum computer will ensure that current key exchange algorithms can be broken [5]. In February 2016, NIST published a draft report on post-quantum cryptography, in which it determined that the creation of a large quantum computer is simply a significant engineering challenge [8]. [8, 9] provide estimates of the possible hacking of a full-scale RSA-2048 quantum computer in a matter of hours by 2030.

Quantum computers have already successfully factorized small integers [10, 11]. Thus, an attacker can store intercepted key exchanges and ciphertexts. In addition, they can decrypt them when a large-scale quantum computer becomes available. Depending on when (and if) powerful quantum computers become available, this could render symmetric and asymmetric cryptography "unsuitable" for encrypting key data and transmitting confidential information.

Particular attention is paid to the construction of crypto-code structures that provide the construction of post-quantum algorithms of asymmetric cryptography (McEliece, Niederreiter CCC) [12, 13]. Symmetric CCC is built on the Rao-Nam scheme or a modified scheme [14–16]. Thus, the use of integrated mechanisms to ensure the required level of security and reliability services during data transmission is an urgent task.

2. Literature review and problem statement

The analysis conducted in [17, 18] showed that the stability of McEliece crypto-code constructions is based on the NP-complete problem of decoding a random linear code. The main idea used in such systems is based on the use of masking matrices. The speed of encoding (cryptotransformations) is much higher than in public-key cryptosystems, but the volume of key data is much higher. Thus, on the one hand (the first) is an advantage, on the other (the second) is a significant disadvantage. In the works [19, 20], the results of studies of the crypto-resistance of public-key CCCs are presented, and an effective algorithm for breaking asymmetric McEliece cryptosystems based on Reed-Solomon codes is shown. Due to the orthogonality of the matrices (generating G and checking H, $||G||\times||H||^T=||0||$) algorithm can also be applied to Niederreiter CCC, the use of algebrogeometric codes (codes built on elliptic curves) or cascade codes is proposed. In [21], McEliece CCC on quasicyclic low-density parity check codes is proposed, which allows overcoming the main limitations of the original cryptosystem. This allows countering the Sidelnikov attack, but increases the volume of key data. In [22], a symmetric cryptosystem based on the Rao-Nam scheme with a hyperchaotic fractional order system and extended quasicyclic low-density parity check (EDF–QC–LDPC) codes is proposed. A four-dimensional hyperchaotic fractional order system is proposed, which provides the formation of a pseudo-random sequence. Due to the replacement of error syndromes with a pseudo-random sequence and dynamic permutation of the encoded message, stability is ensured, but at the same time the volume of key sequences increases. In [23], the McEliece CCC on modified (shortened and extended) elliptic codes was considered, but the volume of key data does not allow their use for providing security services of system architectures based on smart technologies. In works [24, 25], Niederreiter CCCs on elliptic (modified (shortened, extended)) codes were proposed. Elliptic (algebrogeometric codes, elliptic codes – EC) provide counteraction to the Sidelnikov attack, and the modification of the codes provides for the reduction of key data. But the volume of key data remains large for smart technologies. In addition, the construction of CCCs over the field 2^{10}–2^8 is critical in terms of computational capabilities for critical infrastructure objects based on mesh networks. In work [26], a polynomial time structural attack against the McEliece system based on Gopa codes from a quadratic finite field extension is presented. This attack uses the fact that Gopa codes can be distinguished from random codes to calculate some filtering, i.e. a family of nested subcodes that will reveal their secret algebraic description. Thus, almost all noise-resistant m-linear codes enable the CCC to be hacked. In [27, 28], hybrid McEliece and Niederreiter CCCs based on modified (shortened, extended) elliptic codes (MEC) with the subsequent use of flawed codes are proposed, which allows the use of multichannel cryptography. This approach provides a reduction in the power of the Galois field (construction of CCC over the field 2^4–2^6), but the volume of key data and the speed of cryptographic transformations are higher than in the Rao-Nam CCC. In [29], McEliece CCC on low-density quasicyclic parity check codes (QC-LDPC) is proposed. This provides both security and error correction simultaneously in a specific network coding system. The characteristics of the cryptosystem allow it not to require additional reduction of the information rate to ensure security. Messages are encoded using QC-LDPC and transmitted over the network, where the network coding error correction scheme is implemented. However, the stability of such systems depends on the number of errors that occur in intermediate links and will not exceed the minimum distance of QC-LDPC codes. In addition, such systems require an increase in the volume of key data along with CCC on the EC. In [30], the stability of the McEliece and Niederreiter CCC is analyzed. A variant of the McEliece cryptosystem is also proposed, which, by replacing the secret permutation matrix with a more general transformation matrix, can avoid the public code being the permutation equivalent of the secret code. This allows to prevent attacks on classical families of codes, such as GRS (General Reference System) codes, and to view them as possible good candidates in this framework. The more general transformation matrix is already present in the GPT cryptosystem variant that uses a column scrambler, but its use leads to an increase in the volume of key data and computational resources. In [31], the authors propose a new version of the McEliece cryptosystem based on the Smith form of convolutional codes. They use the Smith form to hide part of the code in a public matrix, while keeping the other part secret. The secret part will then be used for decryption. They hide this part by left-multiplying it by a random matrix, and add a random matrix that has several conditions. Their scheme has a small public key size compared to the original McEliece scheme and resists the unique decoding attack against the convolutional structure presented in [31] at

the PQCrypto 2013 conference. In addition, a full search attack is impossible for their system. However, using convolutional codes significantly increases the size of the key sequence. In [32], it is shown that the McEliece cryptosystem over rational Gopa codes and the Niederreiter cryptosystem over classical Gopa codes resist precisely the attacks to which RSA and El Gamal cryptosystems are vulnerable. This eliminates the strong Fourier discretization approach on which almost all known exponential speedups using quantum algorithms are based.

Thus, the analysis of the use of McEliece and Niederreiter CCCs showed that these systems provide the construction of asymmetric cryptosystems and integratedly provide an increase in the level of probability of obtaining information. But the use of noise-resistant codes does not fully provide the necessary level of stability in the post-quantum period and requires the use of algebro-geometric codes. In addition, a significant amount of key data remains, which limits their practical use in smart and mobile technologies. Rao-Nam CCC allows to "remove" these shortcomings, but their construction on linear codes does not provide the necessary resistance to attacks in the quantum period.

3. The aim and objectives of the study

The aim of this study is to develop a Rao-Nam crypto-code construction based on EC (modified elliptic codes – MEC) and flawed codes. The developed constructions will provide a practical possibility of their use in critical infrastructure facilities based on smart and mobile technologies.

To achieve the aim of the work, it is necessary to solve the following tasks:

– to develop a CCC (modified CCC (MCCC) Rao-Nam on algebrogeometric codes);

– to develop hybrid Rao-Nam CCCs on algebrogeometric codes;

– to evaluate the main parameters of the proposed Rao-Nam CCCs (MCCCs, hybrid CCCs – HCCCs);

– to develop a structural diagram for building an intelligent information protection system using CCC.

4. Materials and methods

The object of the study is the process of ensuring data transmission protection in communication channels of critical infrastructure facilities based on mobile and smart technologies.

The hypothesis of the study is as follows. To ensure the provision of security services: confidentiality, integrity and authenticity, it is proposed to use crypto-code constructions based on the Rao-Nam scheme. The Rao-Nam CCC is formed on the basis of algebrogeometric codes – noise-resistant codes, which are built on the basis of algorithms of the theory of noise-resistant coding (Weierstrass matrix) and uses the geometric parameters of the points of the corresponding curve.

CCCs provide information protection from accidental and intentional influence and were first proposed in [12–15]. The main idea of such schemes is to use algebraic block (n, k, d)-code with encoding and decoding algorithms that are easy to implement. By masking an algebraic code under a random code (a general state code), the decoding task can be presented to the attacker as a computationally difficult task. Indeed, not knowing the masking rule, the attacker is forced to use a complex random code decoder, and the entire encoding-decoding process, in this case, is equivalent to a one-way cryptographic function [17–19]. Thus, the basis of the CCC is the use of the theoretically difficult problem of decoding a random code.

The main criterion for choosing an algebraic (n, k, d)-block code is the complexity of the encoding and decoding algorithms. In the general case, codes are chosen with a polynomial dependence of the complexity of the encoding and decoding algorithms on the length of the algebraic code and/or on its correcting ability $t=(d-1)/2$. Such codes are, for example, BCH codes (Bowse-Chhothuri-Hockvingham), RS (Reed-Solomon), Gopa codes, algebrogeometric codes, and others.

The task of masking an algebraic code is to present it to an attacker as a random code (a general state code). The complexity of decoding a random code, in the general case, increases exponentially with the length of the code and/or its correcting ability. The main means of masking an algebraic code as a random code in the classical Rao-Nama scheme is the generating matrix G, and the error vector, which can be used as a session key.

A cryptogram (codegram) is formed by calculating the codeword of a block code. Based on the algorithms for constructing a codegram (n, k, d)-code with the addition of a random error vector. If the algebraic block (n, k, d)-code is given by the generating matrix G, then the formation of the cryptogram can be represented by the following expression[14, 15]:

$$c=IG^T+e, \quad (1)$$

where $I=\{I_1, I_2,..., I_k\}$ – information vector (plaintext block), $e=\{e_1, e_2,..., e_n\}$ – random error vector, weights $w(e)\leq t$, where t – correcting ability of a noise-tolerant code.

In the modified Rao-Nam CCC, the cryptogram (codegram) is formed by computing the codeword of the block code by multiplying the information vector by the generating matrix G, adding a random error vector, and multiplying by the masking matrix Z. The masking matrix Z is of size $n\times n$, and is a permutation matrix (one in each column and row) [16]:

$$c=(IG^T+e)\times Z. \quad (2)$$

The main disadvantage of Rao-Nam cryptosystems is their resistance to cracking during the period of the emergence of a full-scale quantum computer and the large volume of key data, as well as cracking by the "Sidelnikov attack" – finding the elements of the generating matrix. Due to the orthogonality of the generating and checking matrices, this attack allows cracking both the McEliece CCC and the Niederreiter CCC on flawed codes [19, 20].

The combination of geometric parameters of elliptic curves (EC) (curve points) with the mathematical apparatus of noise-resistant coding (Weierstrass matrix) provides the formation of algebrogeometric codes. In addition, as an additional initialization vector in addition to the elliptic curve points, irreducible coefficients of the curve equation are used. This initialization vector allows to determine the equation by which the generating and/or verification matrix is formed, and can be used as a key sequence [24–28].

To construct, a generating matrix is used, in which the elements are projective points $P_i(X_i, Y_i, Z_i)$. The values of the generating functions from the specified points provide the formation of the generating matrix of the elliptic code [24–28], which is defined by the expression:

$$G=\begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix}=\left\|F_j(P_i)\right\|_{n,k}, \quad (3)$$

At the same time, in affine space $\boldsymbol{A}^2$ over the field $GF(q)$ the elliptic curve is given by the expression [24–28]:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \quad (4)$$

or in projective space P^2 [24–28]:

$$y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3, \quad (5)$$

$a_i \in GF(q)$, genus of the curve $g=1$.

The total number of points on the curve is determined by the Hase-Wehl theorem [24–28]:

$$N \le 2\sqrt{q}\cdot g+q+1, \quad (6)$$

where g – genus of the curve, $q=p^m$ – Galois fields.

Thus, the Hase-Wehl theorem (limit) determines the maximum number of points that can be defined as elements of an elliptic code. Algebrogeometric (n, k, d)-code specifies the following parameters of the noise-resistant code: $k+d \ge n$, $n \le 2\sqrt{q}+q+1$, $k \ge \alpha$, $d \ge n-\alpha$, $\alpha=3\times degF$ [24–28]. To ensure cryptostability, NIST (National Institute of Standards and Technology) USA specialists recommend building CCC using noise-resistant codes with elements on GF (2^{10}–2^{13}), which is very difficult to implement in practice in smart and mobile technologies [1, 2]. Thus, an approach is needed to reduce the set of the Galois field while maintaining the level of cryptostability of the system as a whole. To reduce the size of the key data and the field strength (at a given level of stability), in [24–28] it is proposed to use modified elliptic codes (MEC).

Methods for modifying noise-resistant coding provide parameters (n, k, d) of linear block code with modifications [23, 24]. Fig. 1 shows the most common methods of modification.

In this case, to ensure the required level of stability among the parameters of the noise-resistant code, it is necessary to fix the parameter d – constructive distance, which determines the number of error detection and correction in the codeword [23, 24, 33, 34].

Thus, to ensure the required level of stability of the Rao-Nam CCC, it is necessary to use modification methods that do not allow a decrease in the minimum code distance [23, 24, 33, 34]. The analysis of Fig. 1 showed that d (constructive distance) does not change when using the parameters of the noise-resistant code when they are reduced (the number of symbols in the code word is reduced).

To modify (reduce) elliptic codes, let's use the reduction of the set of curve points [23, 24, 33, 34]. To form a symmetric cryptosystem based on the Rao-Nam scheme, the reduction vector forms an initialization vector (IV_1), which provides an additional level of entropy and increases the level of uncertainty for the attacker. To construct a Rao-Nam CCC on extended MEC, after reducing the codeword, it is proposed to use a second initialization vector (IV_2). This approach provides the definition of "places" for inserting plaintext symbols, which also provides a level of stability, and reduces the field strength (reduces the volume of key data).

To further reduce energy costs for software (software and hardware implementation) while maintaining the level of stability, let's propose a hybrid Rao-Nam CCCC (HCCC) with MEC based on the use of flawed codes.

The CCC formation is based on the reduced loss of each symbol (determined by any protocol of signal-code structures, for example, ASCII table) [35, 36]. In this case, the MV2 reduction algorithm is used, provides a surjective mapping of code elements and determines the loss, which is formed by a pseudorandom number generator (PRNG) and a damaged text (formed after the damage is applied) [34, 35]. This approach forms multi-channel cryptography by transmitting the damage and damaged code over two open communication channels, the main theoretical foundations of flawed codes and CCC parameters on flawed codes are given in [24, 25, 27, 28].

Thus, the proposed methods for constructing noise-resistant codes on algebrogeometric and flawed codes provide the construction of Rao-Nam CCC, which is capable of providing the necessary level of security in the post-quantum period.

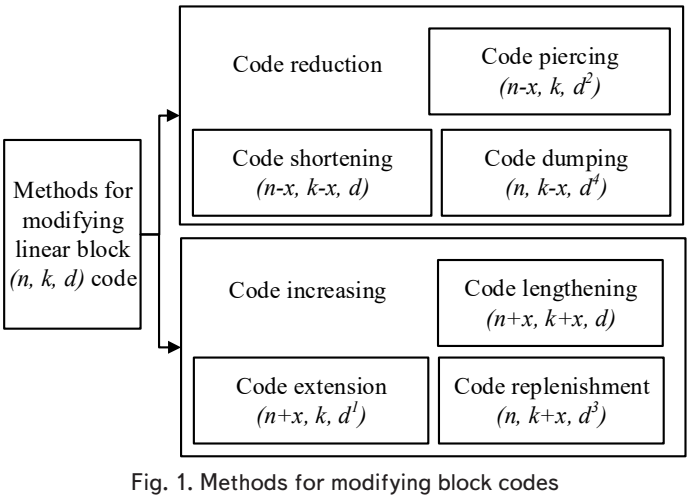

Fig. 1. Methods for modifying block codes

5. Results of the development of Rao-Nam crypto-code constructions

5. 1. Development of the CCC (modified (MCCC) Rao-Nam on algebrogeometric codes)

To build a symmetric cryptosystem based on the Rao-Nam crypto-code construction on EC, lets define:

G^{EC} – elliptic code generating matrix of dimension $k \times n$ over $GF(q)$ – cryptosystem secret key.

A cryptogram (codegram) is a vector of length n and is calculated according to the rule:

$$\tilde{n}^* = i \times G^{EC} + e, \quad (7)$$

where the vector $c^* = i \times G^{EC}$ belongs to (n, k, d)-code, i – k-digits information vector, vector e – secret error vector of weight $\leq t$ (the correcting ability of the code).

The scheme of transmitting a secret message from subscriber A to subscriber B in a symmetric cryptosystem based on the Rao-Nam scheme using elliptic codes is shown in Fig. 2.

To build a symmetric cryptosystem based on the modified Rao-Nam crypto-code construction on EC, lets define:

– G^{EC} – the generating matrix of EC dimension $k \times n$ over $GF(q)$;

– Z – permutation matrix (one unit in each column and row) of dimension $n \times n$ – masking matrix.

Matrices G^{EC} and Z – the secret key of the cryptosystem. The cryptogram (codogram) is a vector of length n and is defined:

$$\tilde{n}^* = \left(i \times G^{EC} + e\right) \times Z. \quad (8)$$

The scheme of transmitting a secret message from subscriber A to subscriber B in a symmetric cryptosystem based on the modified Rao-Nam scheme on *EC* is shown in Fig. 3.

The proposed approach provides the necessary level of stability and reliability through the use of a noise-resistant algebrogeometric code. *EC* (n, k, d)-code over $GF(q)$ sets the following parameters: $k+d \geq n$, $n \leq 2\sqrt{q}+q+1$, $k \geq \alpha$, $d \geq n-\alpha$, $\alpha = 3 \times degF$. The complexity of the non-systematic coding algorithm is formally $O(3 \times degF \times n)$ or $O((n-d) \times n)$.

To further reduce the computational capacity and the volume of key data, it is proposed to use modified *EC* (*MEC*) – shortened and extended. This approach provides a reduction in the field strength for constructing the Rao-Nam CCC to GF (2^6–2^8). Fig. 4, 5 show the exchange protocols based on the Rao-Nam symmetric cryptosystem on *MEC* (shortened, extended), Fig. 6, 7 – based on the modified Rao-Nam scheme on *MEC* (shortened, extended).

The main properties of *MEC* and parameters of post-quantum cryptosystems based on CCC schemes on *MEC* are given in [24, 25, 27, 28].

Thus, the proposed approach provides the use of mathematical apparatus for constructing noise-resistant codes on elliptic curves and flawed codes. This approach will provide practical implementation of symmetric cryptosystems in mobile applications for providing security services. To further reduce the power of the Galois field, symmetric cryptosystems based on hybrid CCCs of the Rao-Nam scheme are proposed.

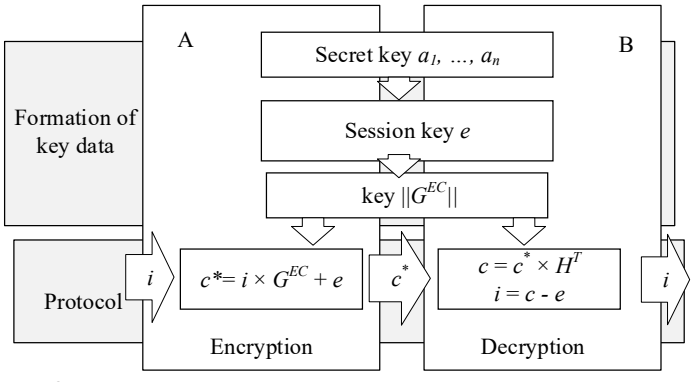

Fig. 2. Information exchange protocol in a symmetric cryptosystem based on the Rao-Nam crypto-code construction on elliptic codes

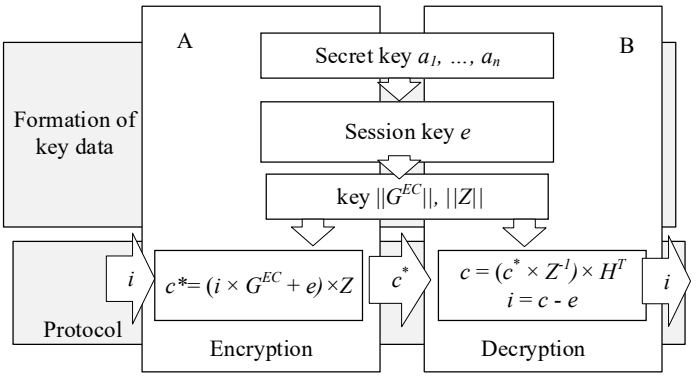

Fig. 3. Information exchange protocol in a symmetric cryptosystem based on a modified Rao-Nam crypto-code construction on elliptic codes

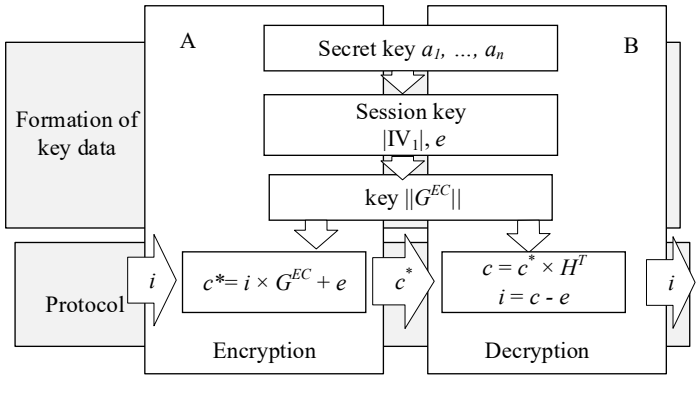

Fig. 4. Information exchange protocol in a symmetric cryptosystem based on the Rao-Nam crypto-code construction on modified elliptic codes (*shortened codes*)

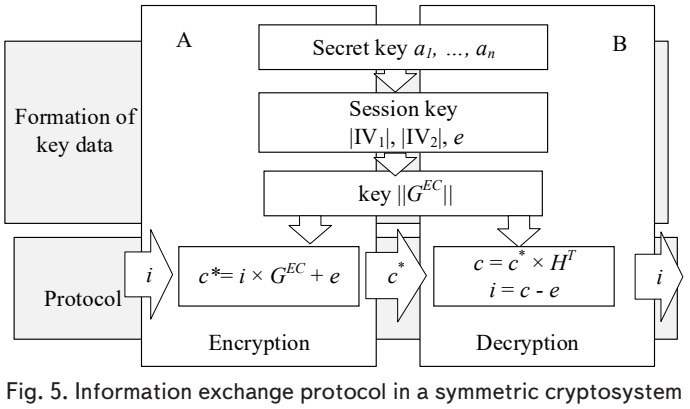

Fig. 5. Information exchange protocol in a symmetric cryptosystem based on the Rao-Nam crypto-code construction on modified elliptic codes (*lengthened codes*)

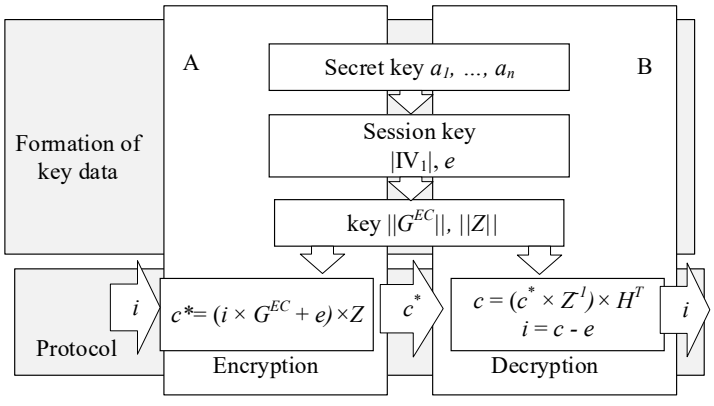

Fig. 6. Information exchange protocol in a symmetric cryptosystem based on a modified Rao-Nam crypto-code construction on modified elliptic codes (*shortened codes*)

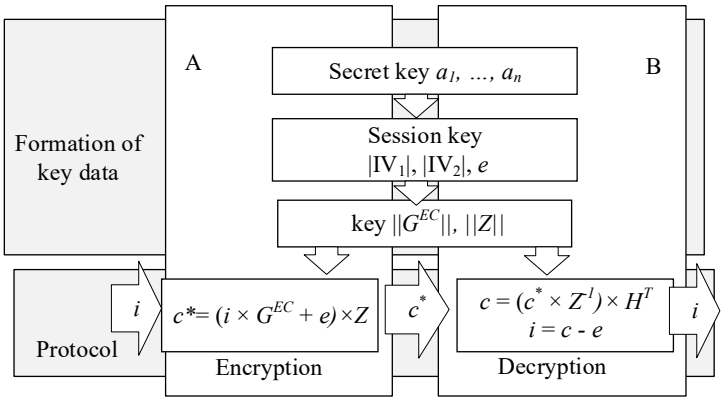

Fig. 7. Information exchange protocol in a symmetric cryptosystem based on a modified Rao-Nam crypto-code construction on modified elliptic codes (*lengthened codes*)

For the research, the proposed Rao-Nam CCC on algebro-geometric codes is implemented in C++. The hardware and software implementation of the CCC is implemented on a Raspberry Pi3, model B+ (RPI3-MODBP) based on the SoC (system-on-a-chip) BCM2837B0. The formation over the Galois field $GF(2^4)$ is used. The standard NIST STS 822 package is used to assess the stability, which provides a check of the sequence 10^8 for randomness.

5. 2. Development of a hybrid Rao-Nam crypto-code construction based on algebrogeometric codes with damage

To use the proposed crypto-code constructions over Galois fields (2^4–2^6), which provides a reduction in the volume of key data, it is proposed to use flawed codes that build hybrid (complex) cryptosystems. Flawed cryptography is multi-channel cryptography, which in this case provides additional entropy and cryptographic stability of the system as a whole. Cryptographic flawed texts are texts obtained by such methods [35–38]:

– approach 1: causing damage to the original text followed by encryption of the damaged text and/or its damage;

– approach 2: damaging the ciphertext;

– approach 3: damaging the plaintext and the ciphertext of the damaged text.

The analysis of the use of the MV2 algorithm (damage algorithm) showed that the best result is achieved when performing the following sequences – starting with encryption in the Rao-Nam CCC, then damage to the ciphertext (approach 3). Fig. 8, 9 show the information exchange protocols in a hybrid symmetric cryptosystem based on the CCC, (modified CCC) Rao-Nam on the MEC (shortened codes).

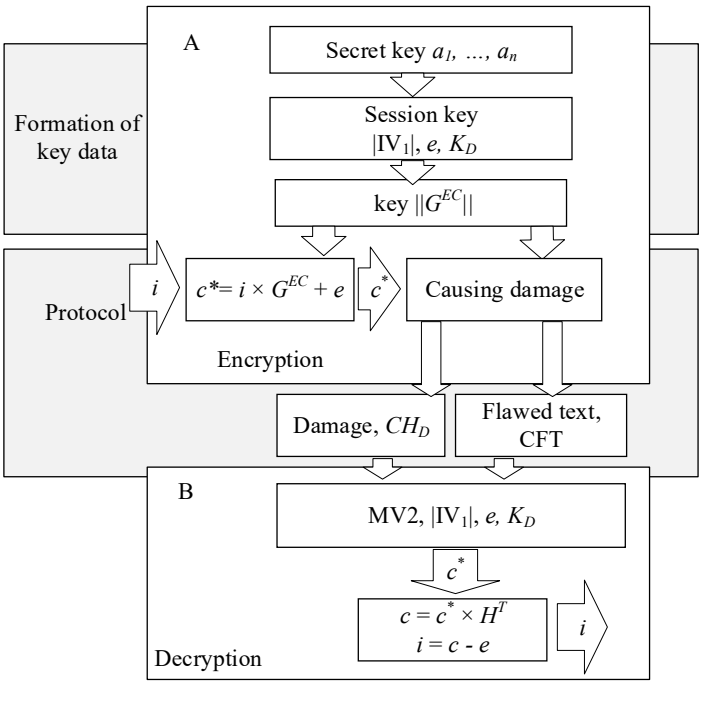

Fig. 8. Information exchange protocol in a hybrid symmetric cryptosystem based on the Rao-Nam crypto-code construction on elliptic codes (*shortened codes*)

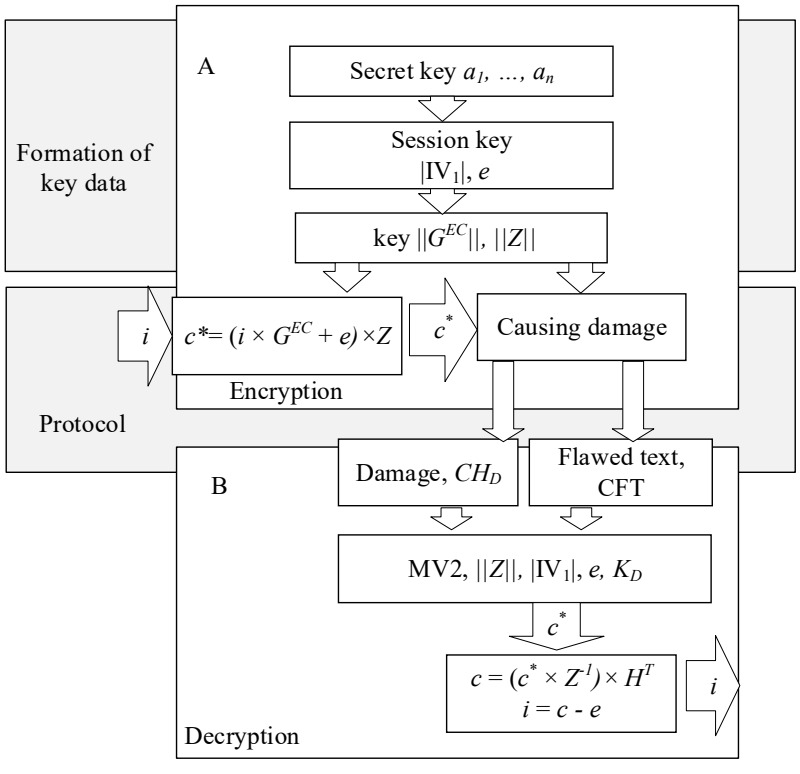

Fig. 9. Information exchange protocol in a hybrid symmetric cryptosystem based on the Rao-Nam crypto-code construction on modified elliptic codes (*shortened codes*)

The proposed approach provides the necessary level of stability (due to multi-channel cryptography on flawed codes), reliability, and significantly reduces the volume of key data. In addition, to reduce key data and increase the level of security of key data, it is possible to exchange only the coefficients of the elliptic curve equation between protocol participants. This approach ensures the transfer of not the entire tuple of key data vectors, which also reduces the total volume of key information.

5. 3. Evaluation of the main parameters of the proposed Rao-Nam crypto-code constructions

For experimental study of the proposed symmetric cryptosystems based on Rao-Nam CCC on *EC*(*MEC*), hybrid symmetric cryptosystems, corresponding software layouts were implemented. The results of comparative studies of Rao-Nam CCC are given in Tables 1, 2. Tables 1, 2 show the abbreviations: shortening (sh) – CCC on shortened *MEC*, elongation (el) – CCC on lengthened MES, shh – hybrid symmetric cryptosystems with shortened *MEC*, elh – hybrid symmetric cryptosystems with lengthened *MEC*. The parameters of symmetric (hybrid symmetric) cryptosystems were studied over Galois fields: for Rao-Nam CCC on *EC* – *GF* (2^{10}); with shortened/lengthened *MEC* – *GF* (2^6); for hybrid cryptosystems – *GF* (2^4):

The complexity of breaking the Rao-Nam CCC on the EC is given by the expressions [24, 28]:

– on *EC:*

$$O_{K+}=N_{cov}\times n\times r,$$

where:

$$N_{\text{cov}} \geq \frac{C_n^{\rho \cdot t}}{C_{n-k}^{\rho \cdot t}} = \frac{n(n-1)\ldots(n-\rho \cdot t-1)}{(n-k)(n-k-1)\ldots(n-k-\rho \cdot t-1)},$$

$$t=(d-1)/2, \quad (9)$$

– on shortened codes:

$$O_{K+} = N_{\text{cov}} \times \left(2\sqrt{q}+q+1-1/2k\right)\times r; \quad (10)$$

– on lengthened codes:

$$O_{K+} = N_{\text{cov}} \times \left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times r; \quad (11)$$

– on shortened *MEC* with damage:

$$O_{K+} = N_{\text{cov}} \times \left(2\sqrt{q}+q+1-1/2k\right)\times r + N_{F\text{ or}}\left(N_K\right), \quad (12)$$

where $N_F \approx \frac{K_C^{\ z}}{2^{1-K_C^{\ z+1}}}\times|F|$; K_C=97/128; $|F|$ – total length of the output flags (damages) (bits) – with the attacker knowing the remainder (damaged text) and the given flags (losses), with the unknown key: $N_K \approx 2^{1190\times z}$; z=16;

– on shortened *MEC* with damage:

$$O_{K+} = N_{\text{cov}} \times \left(\begin{matrix}2\sqrt{q}+q+1-\\-1/2k+1/2k\end{matrix}\right)\times r + N_{F\text{ or}}\left(N_K\right). \quad (13)$$

Analysis of Tables 1, 2 showed that the use of HCCC on flawed codes provides ≈12 times reduction in the number of elementary group operations when forming a cryptogram. When spreading – about 20 times the number of elementary group operations at the receiving side.

Tables 3, 4 present the results of studies of the dependence of the capacitive characteristic on the power of the Galois field for software implementation.

To assess the stability of the cryptosystem, the NIST STS 822 package was used, which determines the probability of randomness of the initial sequence [39, 40].

Table 5 presents the results of research into the statistical properties of the proposed methods based on the *NIST STS* 822 package.

Table 5 shows that for a symmetric system based on the Rao-Nam CCC and a hybrid symmetric cryptosystem, the statistical characteristics are not worse than the indicators of the asymmetric McEliece CCC on *EC*. All symmetric cryptosystems on the Rao-Nam scheme passed 100 % of the tests. The best result was shown by the symmetric cryptosystem on the Rao-Nam scheme on shortened *MEC* with flawed codes: 153 out of 189 tests were passed at the level of 0.99, which is 80% of the total number of tests.

Thus, the proposed methods provide basic security services, the necessary level of resilience, and increased reliability in systems based on smart and mobile technologies.

Table 1

Break difficulty results for *EC (MEC)*

Relative encoding speed, *R*	$lg(l_s)$									
	1	2	3	4	5	6	7	8	9	10
0.5	4.75	10.52	18.22	21.42	38.77	54.13	82.14	165.84	358.33	672.37
0.75	12.1	21.76	33.17	51.75	61.09	78.37	83.72	179.13	371.09	684.94
0.5(el)	15.6	32.47	43.75	59.43	68.26	101.72	156.75	223.64	421.97	716.41
0.75(el)	18.23	35.67	51.61	72.81	87.32	112.46	164.72	231.57	428.63	722.26
0.5(sh)	19.12	38.63	56.88	78.92	94.91	120.83	182.39	276.27	459.81	783.46
0.75(sh)	19.82	39.18	58.03	80.52	104.56	128.79	189.74	287.33	476.52	794.28

Table 2

Break difficulty results for *MEC(MEC+DC)*

Relative encoding speed, *R*	$lg(l_s)$					
	1	2	3	4	5	6
0.5(el)	15.6	32.47	43.75	59.43	68.26	101.72
0.75(el)	18.23	35.67	51.61	72.81	87.32	112.46
0.5(sh)	19.12	38.63	56.88	78.92	94.91	120.83
0.75(sh)	19.82	39.18	58.03	80.52	104.56	128.79
0.5(elh)	7.21	21.46	31.68	41.72	56.63	72.32
0.75(elh)	9.17	23.72	33.83	42.27	58.91	74.79
0.5(shh)	12.54	27.48	37.38	47.48	62.86	89.5
0.75(shh)	14.56	29.82	38.43	58.23	66.53	97.71

Table 3

Dependence of the software implementation speed on the field strength (number of group operations)

Cryptosystems	$GF(q^m)$					
	2^5	2^6	2^7	2^8	2^9	2^{10}
Rao-Nam CCC on *EC*	2,003,608	3,609,614	6,569,429	9,497,957	12,643,116	16,493,579
Rao-Nam CCC on shortened *MEC*	2,001,589	3,557,486	5,719,003	8,815,887	12,394,851	15,910,953
Rao-Nam CCC on lengthened *MEC*	2,231,228	3,712,246	6,642,142	9,659,422	13,034,338	16,810,267

Table 4

Dependence of the software implementation speed on the field strength (number of group operations)

Cryptosystems	$GF(2^4)$	$GF(2^5)$	$GF(2^6)$	$GF(2^7)$	$GF(2^8)$	$GF(2^9)$	$GF(2^{10})$
Rao-Nam CCC on shortened *MEC*	1,658,615	2,001,589	3,557,486	5,719,003	8,815,887	12,394,851	15,910,953
Rao-Nam CCC on lengthened *MEC*	1,701,284	2,231,228	3,712,246	6,642,142	9,659,422	13,034,338	16,810,267
Rao-Nam CCC on lengthened *MEC+ flawed codes*	1,122,463	1,580,063	2,978,589	5,113,055	8,455,837	11,792,756	15,312,835
Rao-Nam CCC on shortened *MEC+ flawed codes*	1,188,525	1,581,051	2,936,482	5,119,003	8,423,265	11,693,629	15,094,953

Table 5

Statistical safety research results

Cryptosystems	Number of tests in which more than 99 % of sequences passed the test	Number of tests in which more than 96 % of sequences passed the test	Number of tests in which less than 96 % of sequences passed the test
McEliece CCC on *EC*	149 (78.3 %)	189 (100 %)	0 (0 %)
Rao-Nam CCC on shortened *MEC*	149 (78.8 %)	189 (100 %)	0 (0 %)
Rao-Nam CCC on lengthened *MEC*	150 (79.3 %)	189 (100 %)	0 (0 %)
Rao-Nam CCC on lengthened *MEC+ flawed codes*	151 (79.9 %)	189 (100 %)	0 (0 %)
Rao-Nam CCC on shortened *MEC+ flawed codes*	153 (80 %)	189 (100 %)	0 (0 %)

5. 4. Development of a structural diagram for building an intelligent information protection system using crypto-code constructions

To provide security services at critical infrastructure facilities based on smart and mobile technologies, it is proposed to create an intelligent information protection system. An intelligent information protection system is an interconnected set of organizational and engineering and technical measures, means and methods of information protection using artificial intelligence systems. The structural diagram of the intelligent information protection system is shown in Fig. 10.

To ensure the classification of threats, a threat classifier is used, which provides not only the formation of a threat tuple, but also allows for the formation of a statistical analysis of threats, the criticality of elements of the infrastructure of protected objects, and also determines the flow level of security [41]. In [42], a classification of attackers is proposed, which provides the ability to assess their computational and financial capabilities. Formally, the mathematical model of the attackers' "capabilities" is defined by the expression:

$$\lambda_i^{cyber} = \left(\omega_i^{cyber}\right) \times p_i \times \psi_{motiv}, \quad (14)$$

where $A_i^{cyber} \in \left\{A_i^{cyber}\right\}$ – attacker category; ω_i^{cyber} – attacker opportunity coefficient CPS; T – time of threat realization; p_i – probability of at least one threat being implemented; ψ_{motiv} – probability of the attacker's motivation to carry out the threat.

In [43], the foundations of building multi-contour protection systems are defined, taking into account not only the structure of the network, but also the possibility of considering it taking into account the physical location (platform). This approach makes it possible to create models not only of cyber-physical systems, but also of their alternative – socio-cyber-physical systems.

This approach ensures the construction of both an external and internal protection contour for each network infrastructure platform, which ensures an increased level of objectivity in assessing threats, their integration with social engineering methods, and active terrorist actions.

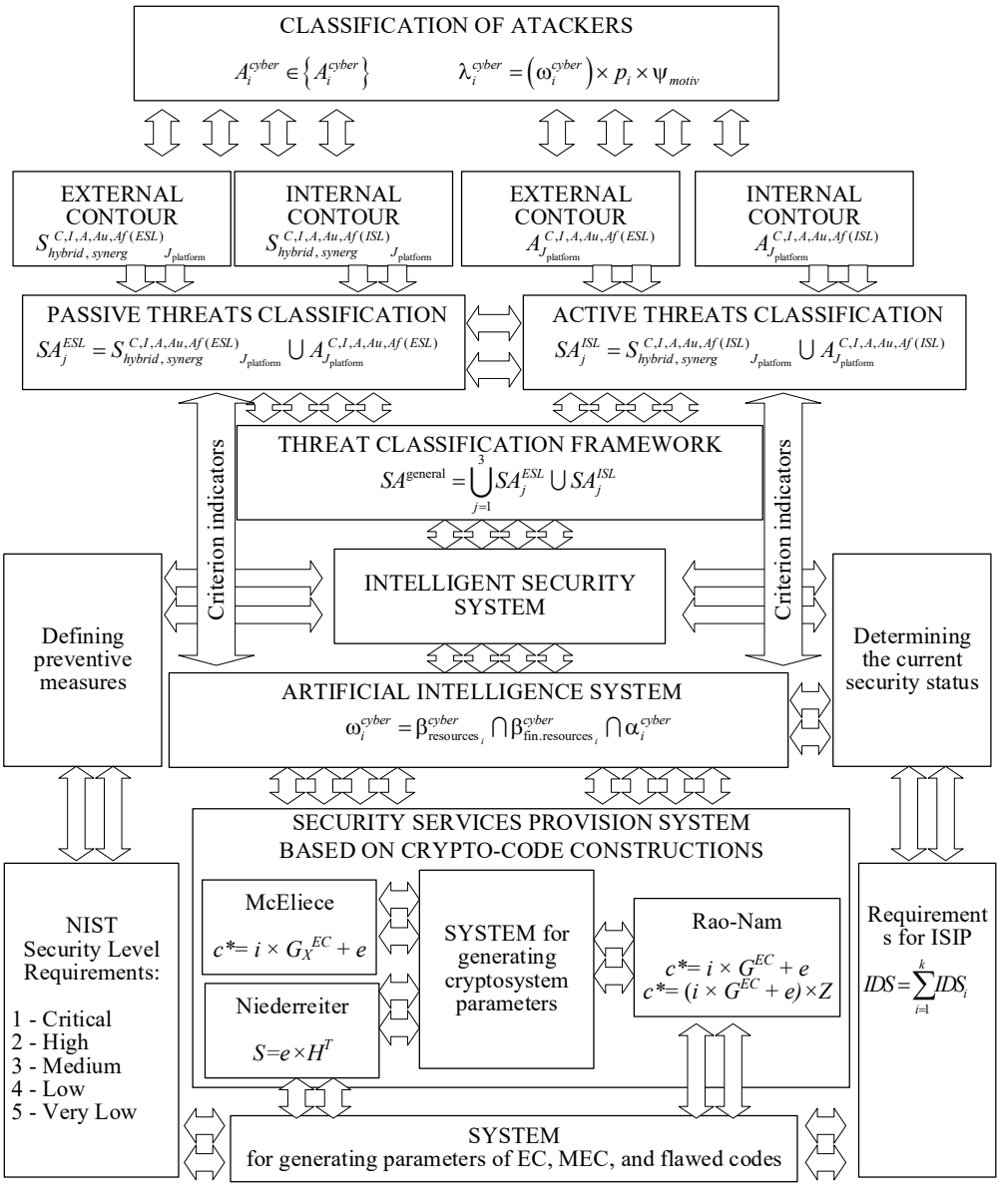

Fig. 10. Structural diagram of an intelligent information protection system

The overall threat assessment of the implementation of internal circuit threats will be defined as:

$$SA_j^{ESL} = S_{hybrid,\ synerg\ \ J_{platform}}^{\tilde{N},I,A,Au,Af(ESL)} \bigcup A_{J_{platform}}^{\tilde{N},I,A,Au,Af(ESL)}, \quad (15)$$

where SA_j^{ESL} – general threat taking into account the "combination" of passive (technogenic) and anthropogenic threats from attackers (terrorists) to the internal contour of the infrastructure of the protected object; $S_{hybrid,\ synerg\ \ J_{platform}}^{\tilde{N},I,A,Au,Af(ESL)}$ – a general threat to the main security services (C – confidentiality; I – integrity; A – availability; Au – authenticity, Af – involvement), with signs of hybridity and synergy. The sign of synergy is considered as the possibility of maximum impact of the threat on all services of one security component (cybersecurity, information security, information security). Hybridity – the possibility of a threat to inject (crack) one of the security services into all its components. $A_{J_{platform}}^{\tilde{N},I,A,Au,Af(ESL)}$ – overall active threat to core security services.

The assessment of the overall threat of the implementation of external contour threats will be defined as:

$$SA_j^{ISL} = S_{hybrid,\ synerg\ \ J_{platform}}^{\tilde{N},I,A,Au,Af(ISL)} \bigcup A_{J_{platform}}^{\tilde{N},I,A,Au,Af(ISL)}. \quad (16)$$

Thus, the threat classification framework provides a generalization of expert assessments of threats, taking into account their integration and unification:

$$SA^{\text{general}} = \bigcup_{j=1}^{3} SA_j^{ESL} \bigcup SA_j^{ISL}, \quad (17)$$

where $SA^{general}$ – general threat to the infrastructure platforms of the protected object.

To take into account the level of protection, the attacker's capabilities, and the probability of implementation, an indicator of the attacker's "capabilities" will be defined as:

$$\omega_i^{cyber} = \beta_{\text{resources}_i}^{cyber} \bigcap \beta_{\text{fin.resources}_i}^{cyber} \bigcap \alpha_i^{cyber}, \quad (18)$$

$\beta_{\text{resources}_i}^{cyber} \in$ {1 – unlimited computing resources of cyberterrorists, 0.75 – computing resources of the state (special services), 0.5 – computing resources of cybercriminals, 0.25 – computing resources of criminals, competitors, hackers, 0.001 – computing resources of vandals }; $\alpha_i^{cyber} \in$ {1 – frequency of threat implementation daily, 0.75 – frequency of threat implementation every week, 0.5 – monthly threat implementation frequency, 0.25 – frequency of threat realization each year, 0.001 – unlimited time }; $\beta_{\text{fin.resources}_i}^{cyber} \in$ {1 – unlimited financial resources of cyberterrorists, 0.75 – financial resources of the state (special services), 0.5 – financial resources of cybercriminals, 0.25 – financial resources of criminals, competitors, hackers, 0.001 – financial resources of vandals}. Table 6 shows the generalized indicators taking into account the level of security.

The analysis of Table 6 showed that the relevant cyber groups (with the support of the state/special services) have both financial and computational capabilities to carry out both terrorist attacks and targeted attacks on the infrastructure elements of the protected object.

Neural networks play an important role in cybersecurity, providing powerful tools for threat detection, anomaly analysis, and system protection. Different types of networks are suitable for different tasks: CNNs are excellent at processing images and network traffic, RNNs cope with temporal data, and GANs help test security systems. Table 7 lists the main applications of neural networks in cybersecurity [44–49].

Table 6

Initial data of criteria and indicators of expert assessment of the attacker's "danger" weight coefficient

Category	Weighting coefficient evaluation indicators				
	ω_i^{cyber}			p_i	ψ_{motiv}
	$\beta_{\text{resources}}^{cyber}$	α_i^{cyber}	$\beta_{\text{fin.resources}_i}^{cyber}$		
Critical	1	1	1	1	1
High	0.75	0.75	0.75	0.75	0.75
Medium	0.5	0.5	0.5	0.5	0.5
Low	0.25	0.25	0.25	0.25	0.25
Too low	0.001	0.001	0.001	0.001	0.001

Table 7

Main applications of neural networks in cybersecurity

Network type	Application	Example problem
FCNN	Log analysis and attack classification	DDoS attack classification
CNN	Image and network traffic analysis	Detecting malware through binaries
RNN (LSTM, GRU)	Time series and sequence analysis	User behavior analysis
GAN	Data generation and robustness testing	Creating synthetic attack data
Autoencoders	Anomaly detection and data compression	Detecting traffic anomalies
Transformers	Text data analysis	Detecting phishing emails
GNN	Graph and network analysis	Botnet detection
Hybrid networks	Combined analysis	Combine multiple architectures to solve complex problems

The analysis of Table 7 showed that Fully Connected Neural Networks (FCNN) will provide analysis of logs and anomalies, detection of anomalies and threats in data based on security system logs; threat detection: data classification (malicious/intact traffic).

Convolutional Neural Networks (CNN) provide network traffic analysis; phishing site detection: analysis of web page screenshots; malware recognition: analysis of binary files through visualization of their structures.

Thus, the use of appropriate networks will ensure timely assessment of the current state of the facility's infrastructure protection system and determination of the attacker's "capabilities".

To provide security services, it is proposed to use post-quantum symmetric and asymmetric cryptosystems based on appropriate crypto-code constructions, taking into account the "volume" of secrecy of the relevant confidential information.

Based on the identification of threats (targeted attacks), the formation of constant control over the current state of the security system, and the assessment of compliance with the requirements of international regulators, an objective assessment of the current state of the security of the infrastructure elements of the protected object is created. The use of post-quantum algorithms within the infrastructure of the information protection system allows for a timely "response" to changes not only in key data, but also in the CCC itself and their parameters (jamming and flawed codes).

6. Discussion of the results of developing a structural diagram for building an intelligent information protection system

The analysis of a proposed cybersecurity system should begin first of all with the identification of features that significantly distinguish the proposed system from similar ones proposed and described by other researchers. There are several such features.

It is important to focus on the fact that the use of neural network technologies in the form of neural networks is fully integrated into the security system. The implementation of neural network technologies is based on the use of the proposed classifiers, which are significantly different from those used traditionally, for example [42]. First of all, the existing classifier introduces financial indicators of attacks, such as the cost of implementing a particular attack. This allows to significantly reduce the efforts to counter cyberattacks. By rejecting cyber threats that cannot be implemented, and based on the possible resources of cybercriminals, as well as identifying classes of attacks that cannot be resisted, based on the resources available to the security system [43].

To implement such functionality, an attacker classifier was developed and introduced into the security system. Although today there are classifications of cybercriminals, for example [43–47], the possibilities of implementing cyberm attacks are quite general, based more on their level of professionalism than on resource capabilities.

The proposed threat classifier and attacker classifier are not independent and function together in the proposed system, providing not only the classification of implemented attacks, but also the class of attackers who can carry out the corresponding attacks.

These classifiers define the general requirements for a neural network for classifying and predicting attacks. The classifier specifies the number of different attacks, which determines the number of outputs of the neural network. The additional output reflects the fact that the obtained network performance indicators may correspond to the normal mode of network operation without any attacks. The number of inputs of a neural network operating in the current state classification mode corresponds to the number of different parameters recorded by IDS/IPS. This approach is traditional when using neural networks for classifying cyberattacks and anomalies in networks [2–5, 7–11]. The starting set of factors, which corresponds to the inputs of the neural network, is determined by different sets of test data on which the neural network is trained, for example, CUP KDD99. There can be up to 50 such parameters according to different test data sets [49]. In contrast to existing approaches, it is proposed to reduce the number of inputs that occurs during training of the neural network. In the process of training a neural network to solve attack classification problems, it may turn out that some indicators have such a small input weight that these parameters can be neglected and not taken into account in further work. In this case, the number of inputs can be reduced, which will lead to a simplification of the structure of the neural network and, as a result, an increase in the performance of the neural network in the classification process. It should also be taken into account that when considering the implementation of threats for systems of a specific purpose, it may turn out that some of the threats reflected in the classifier will never be implemented for this system.

In this case, it is also possible to reduce the number of outputs of the neural network. Let's denote the input parameter vector used for classification as $X=\{x_1, x_2, ..., x_n\}$, where x_i – parameter used to classify the attack, retained after training the neural network, and n – number of such parameters.

The output vector of the neural network is denoted as $Y=\{y_0, y_1, ..., y_m\}$, where y_i – i-th output that corresponds to i-th class of threats, y_0 – output corresponding to the normal state in the absence of attacks, m – number of different classes of attacks. After classifying the threat, each is assigned a corresponding source of such an attack, which is represented in the classifier of attackers. For further consideration, let's denote the set of attackers represented in the classifier, $A_i^{cyber} \in \left\{A_i^{cyber}\right\}, \forall A_i^{cyber} \in 1,...k,$ where A_i^{cyber} – type of attacker, k – number of different classes of attackers. Such a comparison is necessary to predict the further implementation of such an attack (determining the probability of repetition of the analyzed attack in the future). To determine the probabilistic characteristics of the attack, the classifiers must be expanded by adding financial indicators of the attack implementation (f_{ri}), protection against attack (fp_i) and the attacker's capabilities to carry out a particular attack (fa_i). If the attack and its source are identified, it is possible to estimate the costs of its implementation and the possibility of implementing the analyzed attack by the relevant attacker.

If the threat records in the classifier are sorted by their financial indicators, then a boundary can be obtained that cuts off those attacks that cannot be implemented by a particular class of attackers. Using this approach, it is possible to identify a set of attacks that can be expected to be implemented in the future.

The disadvantage of the proposed scheme may be the need to obtain information about the resources that are spent on implementing a particular attack, and on preventing the implementation of such an attack. This may require expert assessment in the case when all or part of the data is not known. Another limitation is that the classifier contains previously known attacks for which there are corresponding statistics in the data sets used to train the neural network. The appearance of a new attack will require its inclusion in the classifier and the collection of the necessary statistics for the data set for training. If this needs to be done in real time, this may determine the limitations of using such a system for known attacks, or for cases when retraining the neural networks in the system will not lead to losses.

Another improvement proposed for the security system is a classifier of crypto-code structures, which aligns certain crypto-code structures as an effective post-quantum mechanism for providing security services at a security facility. Formally, such a classifier can be represented as ($C=\{ccc_i\}$), where CCC_i – i-th crypto-code construction, which is the most effective mean of protection against the intended type of attack, the source of which is an attacker of the corresponding type. In addition, there is an integrated ability to reduce both the computational costs of using the corresponding CCC on certain jamming-resistant codes (symmetric or asymmetric CCC).

Thus, the combined use of modified and developed classifiers, which reflect the above-mentioned financial and computational indicators, corresponding to different classes/sets of attacks, and attackers of different classes. This approach allows not only to highlight the range of attacks, the implementation of which should be expected in the future, but also to suggest the most appropriate crypto-code design

as an effective tool for preventing losses from a certain class of attacks. In addition, it allows to highlight a set of classes of attacks that should be expected in the future.

To ensure the security services of the intelligent information protection system, it is proposed to use post-quantum symmetric Rao-Nam CCCs on *MEC* and HCCCs on flawed codes. Their use provides a reduction of ≈12 times in the number of operations when forming a cryptogram. As well as about 20 times in the number of elementary group operations during decoding, which is confirmed by the data in Tables 1, 2. When the power of the Galois field in which the CCCs are built is reduced, additional mechanisms are usually required to ensure the required level of stability. Such mechanisms in the proposed Rao-Nam CCCs are initialization vectors – for shortened and extended elliptic codes, as well as splitting the cryptogram into loss and damaged text, which is confirmed by the results in Table 5. The main limitations of using CCCs are the creation of a CCC parameter generation server and the need to use additional chipsets (W/LW) at intermediate and end points of the infrastructure of the intelligent protection system.

Thus, the combination of post-quantum algorithms (symmetric cryptosystems) with elements of artificial intelligence provides the possibility of timely formation of a "portrait" of the attacker (its financial and computational capabilities to implement threats). In addition, sets of possible threats are generalized, which makes it possible to timely use the necessary CCCs on the corresponding codes.

7. Conclusions

1. The proposed symmetric cryptosystem based on the Rao-Nam scheme on algebrogeometric codes (elliptic and modified elliptic codes) provides the required level of security. To reduce the volume of key data, it is proposed to use a modification of algebrogeometric codes, which provides for a reduction in the volume of key data with given cryptographic stability parameters. The cryptosystem is formed over the Galois field $GF(2^{6-8})$. Stability is ensured by using additional session initialization vectors. When using shortened elliptic codes, the initialization vector determines the "places of origin" of the codeword symbols (cryptograms). When using lengthened ones, an additional session initialization vector is added, which determines the "places of addition" of the plaintext symbols to the cryptogram.

2. The proposed algorithm for further reduction of key data based on multi-channel cryptography on flawed codes. By using the MV2 algorithm (damage), cryptogram formation is divided into two mechanisms – cryptogram formation in the symmetric Rao-Nam cryptosystem on shortened elliptic codes with subsequent damage.

3. The conducted stability studies using the NIST package showed that despite the reduction in the power of the Galois field, all cryptosystems passed 100 % of the tests. The best result was shown by the Rao-Nam CCC on shortened *MEC*: 155 out of 189 tests were passed at the level of 0.99, which is 82 % of the total number of tests. The use of flawed codes and a further reduction in the power of the Galois field leads to a significant reduction in the complexity of the formation (≈12 times) and decoding of the cryptogram (≈20 times).

4. The proposed structural scheme of the intelligent information protection system is based on the combined multi-platform protection system based on post-quantum algorithms – crypto-code constructions with an artificial intelligence system. This approach provides integration with the threat classification framework and provides a timely assessment of the "capabilities" of attackers. This allows for the definition of preventive countermeasures and reduction (minimization) of funding for the provision of security services.

Conflict of interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, that could influence the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Using artificial intelligence tools

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207
2. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. https://doi.org/10.15587/1729-4061.2021.233533
3. Petrivskyi, V., Shevchenko, V., Yevseiev, S., Milov, O., Laptiev, O., Bychkov, O. et al. (2022). Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. Eastern-European Journal of Enterprise Technologies, 1 (9 (115)), 15–23. https://doi.org/10.15587/1729-4061.2022.252988
4. Yevseiev, S., Milevskyi, S., Bortnik, L., Alexey, V., Bondarenko, K., Pohasii, S. (2022). Socio-Cyber-Physical Systems Security Concept. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 1–8. https://doi.org/10.1109/hora55278.2022.9799957

5. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. Post-Quantum Cryptography, 1–14. https://doi.org/10.1007/978-3-540-88702-7_1
6. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's Algorithm to AES: Quantum Resource Estimates. Post-Quantum Cryptography, 29–43. https://doi.org/10.1007/978-3-319-29360-8_3
7. Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J. (2017). Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3. Selected Areas in Cryptography – SAC 2016, 317–337. https://doi.org/10.1007/978-3-319-69453-5_18
8. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8105
9. Mariantoni, M. (2014). Building a Superconducting Quantum Computer. Available at: https://www.youtube.com/watch?v=wWHAs--HA1c
10. Xu, N., Zhu, J., Lu, D., Zhou, X., Peng, X., Du, J. (2012). Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System. Physical Review Letters, 108 (13). https://doi.org/10.1103/physrevlett.108.130501
11. Dattani, N. S., Bryans, N. (2014). Quantum factorization of 56153 with only 4 qubits. arXiv. https://doi.org/10.48550/arXiv.1411.6758
12. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. DSN progress report 42-44, 114–116. Available at: https://ipnpr.jpl.nasa.gov/progress_report/42-44/44N.PDF
13. Niederreiter, H. (1986). Knapsack-Type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory, 15 (2), 19–34.
14. Rao, T. R. N., Nam, K.-H. (1987). Private-Key Algebraic-Coded Cryptosystems. Advances in Cryptology – CRYPTO' 86, 35–48. https://doi.org/10.1007/3-540-47721-7_3
15. Struik, R., van Tilburg, J. (1988). The Rao-Nam Scheme is Insecure Against a Chosen-Plaintext Attack. Advances in Cryptology – CRYPTO '87, 445–457. https://doi.org/10.1007/3-540-48184-2_40
16. Cheng, Y. C., Lu, E. H., Wu, S. W. (1998). A modified version of the Rao-Nam algebraic-code encryption scheme. Information Processing Letters, 68 (4), 215–217. https://doi.org/10.1016/s0020-0190(98)00156-2
17. Li, Y. X., Deng, R. H., Wang, X. M. (1994). On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions on Information Theory, 40 (1), 271–273. https://doi.org/10.1109/18.272496
18. Bernstein, D. J. (2010). Grover vs. McEliece. Post-Quantum Cryptography, 73–80. https://doi.org/10.1007/978-3-642-12929-2_6
19. Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed-Muller codes. Discrete Mathematics and Applications, 4 (3). https://doi.org/10.1515/dma.1994.4.3.191
20. Minder, L., Shokrollahi, A. (2007). Cryptanalysis of the Sidelnikov Cryptosystem. Advances in Cryptology - EUROCRYPT 2007, 347–360. https://doi.org/10.1007/978-3-540-72540-4_20
21. Baldi, M., Chiaraluce, F. (2007). Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes. 2007 IEEE International Symposium on Information Theory, 2591–2595. https://doi.org/10.1109/isit.2007.4557609
22. Liu, J., Tong, X., Wang, Z., Ma, J., Yi, L. (2019). An Improved Rao–Nam Cryptosystem Based on Fractional Order Hyperchaotic System and EDF–QC–LDPC. International Journal of Bifurcation and Chaos, 29 (09), 1950122. https://doi.org/10.1142/s0218127419501220
23. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18–26. https://doi.org/10.15587/1729-4061.2016.75250
24. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. https://doi.org/10.15587/1729-4061.2018.150903
25. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. https://doi.org/10.15587/1729-4061.2016.86175
26. Couvreur, A., Otmani, A., Tillich, J. (2014). Polynomial Time Attack on Wild McEliece over Quadratic Extensions. Advances in Cryptology – EUROCRYPT 2014, 17–39. https://doi.org/10.1007/978-3-642-55220-5_2
27. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. https://doi.org/10.15587/1729-4061.2017.108461
28. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. https://doi.org/10.15587/1729-4061.2019.156620
29. Zhang, G., Cai, S. (2017). Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes. Cluster Computing, 22 (S2), 2599–2610. https://doi.org/10.1007/s10586-017-1354-x
30. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D. (2014). Enhanced Public Key Security for the McEliece Cryptosystem. Journal of Cryptology, 29 (1), 1–27. https://doi.org/10.1007/s00145-014-9187-8
31. Moufek, H., Guenda, K. (2017). A New variant of the McEliece cryptosystem based on the Smith form of convolutional codes. Cryptologia, 42 (3), 227–239. https://doi.org/10.1080/01611194.2017.1362061
32. Dinh, H., Moore, C., Russell, A. (2011). McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. Advances in Cryptology – CRYPTO 2011, 761–779. https://doi.org/10.1007/978-3-642-22792-9_43

33. Tsyhanenko, O., Rzayev, K., Mammadova, T. (2018). Mathematical model of the modified niederreiter crypto-code structures. Advanced Information Systems, 2 (4), 37–44. https://doi.org/10.20998/2522-9052.2018.4.06
34. Massey, J. L. (1986). Theory and practice of error control codes. Proceedings of the IEEE, 74 (9), 1293–1294. https://doi.org/10.1109/proc.1986.13626
35. Mishenko, V. A., Vilanskiy, Yu. V. (2007). Usherbnye teksty i mnogokanalnaya kriptografiya. Minsk: Enciklopediks.
36. Mishenko, V. A., Vilanskiy, Yu. V., Lepin, V. V (2007). Kriptograficheskiy algoritm MV2. Minsk: Enciklopediks.
37. Yevseiev, S. (2017). The use of damaged codes in crypto code systems. Systemy obrobky informatsiyi, 5, 109–121. Available at: http://nbuv.gov.ua/UJRN/soi_2017_5_17
38. Voronin, A., Akhiiezer, O., Galuza, A., Lebedeva, I., Zaitsev, Y., Lebedev, S. (2023). Modeling Competitive Interaction “Predator-Prey” on the Example of Two Innovative Processes. 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), 131–134. https://doi.org/10.1109/acit58437.2023.10275538
39. Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S. et al. (2000). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology. NIST Special Publication 800-22. https://doi.org/10.6028/nist.sp.800-22
40. Potij, O. V. (2004). Metodika statistichnogo testuvannja NIST STS ta matematichne obґruntuvannja testiv. Tehnichnij zvit IIT – 001-2004. Kharkiv, 62.
41. Класифікатор кібербезпеки. Available at: https://skl.khpi.edu.ua/
42. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. https://doi.org/10.15587/1729-4061.2020.205702
43. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. https://doi.org/10.15587/978-617-7319-72-5
44. Avinash, S. V. (2017). Understanding Activation Functions in Neural Networks. The Theory Of Everything. Available at: https://medium.com/the-theory-of-everything/understanding-activation- functions-in-neural-networks-9491262884e0
45. AutoDraw. Available at: https://www.autodraw.com/
46. Kreutz, D., Ramos, F. M. V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103 (1), 14–76. https://doi.org/10.1109/jproc.2014.2371999
47. Geetha, R., Thilagam, T. (2020). A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. Archives of Computational Methods in Engineering, 28 (4), 2861–2879. https://doi.org/10.1007/s11831-020-09478-2
48. Salvakkam, D. B., Saravanan, V., Jain, P. K., Pamula, R. (2023). Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning. Cognitive Computation, 15 (5), 1593–1612. https://doi.org/10.1007/s12559-023-10139-2
49. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6. https://doi.org/10.1109/cisda.2009.5356528