The results of developing post-quantum algorithms of McEliece and Niederreiter crypto-code constructs based on LDPC (Low-Density Parity-Check) codes are presented. With the rapid growth of computing capabilities of mobile technologies and the creation of wireless mesh and sensor networks, Internet of Things technologies, and smart technologies on their basis, information security is becoming an urgent problem. At the same time, there is a need to consider security in two circuits, internal (directly within the network infrastructure) and external (cloud technologies). In such conditions, it is necessary to integrate threats to both the internal and external security circuits. This allows you to take into account not only the hybridity and synergy of modern targeted threats, but also the level of significance (degree of secrecy) of information flows and information circulating in both the internal and external security circuits. The concept of building security based on two circuits is proposed. To ensure the security of wireless mobile channels, it is proposed to use McEliece and Niederreiter crypto-code constructs based on LDPC codes, which allows integration into the credibility technology of IEEE 802.15.4, IEEE 802.16 standards. This approach provides the required level of security services (confidentiality, integrity, authenticity) in a full-scale quantum computer. Practical security technologies based on the proposed crypto-code constructs, online IP telephony and the Smart Home system based on the use of an internal server are considered

Keywords: crypto-code constructs, low-density parity-check codes, security concept

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2022.254545

DEVELOPMENT OF CRYPTO-CODE CONSTRUCTS BASED ON LDPC CODES

Serhii Pohasii
PhD, Associate Professor*
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department *
E-mail: Serhii.Yevseiev@gmail.com
Oleksandr Zhuchenko
PhD, Associate Professor**
Oleksandr Milov
Doctor of Technical Sciences, Professor*
Volodymyr Lysechko
PhD, Associate Professor**
Oleksandr Kovalenko
Doctor of Technical Sciences, Associate Professor
Department of Cybersecurity and Software
Central Ukrainian National Technical University
Universytetskyi ave., 8, Kropyvnytskyi, Ukraine, 25006
Maryna Kostiak
PhD, Senior Lecturer
Department of Information Security
Institute of Computer Technologies, Automation and Metrology
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
Andrii Volkov***
Aleksandr Lezik
PhD, Associate Professor***
Vitalii Susukailo
Postgraduate Student
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
*Department of Cyber Security
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
**Department of Transport Communications
Ukrainian State University of Railway Transport
Feierbakha sq., 7, Kharkiv, Ukraine, 61050
***Department of Tactics of Air Defense Force of Land Force
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023

Received date 01.03.2022
Accepted date 04.04.2022
Published date 29.04.2022

How to Cite: *Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O., Kostiak, M., Volkov, A., Lezik, A., Susukailo, V. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. doi: https://doi.org/10.15587/1729-4061.2022.254545*

1. Introduction

The creation of modern synthesized networks is based on the hybridization of technologies of wireless mobile and socio-cyberphysical systems based on the Internet of things. Classical computer systems and technologies integrate elements of the Internet of things and form fundamentally new directions for the development of the IT industry, smart

technologies that combine all the achievements of mobile, wireless and socio-cyberphysical systems. However, the rapid expansion of mesh and sensor networks using wireless channel standards: LTE (Long-Term Evolution), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth mobile technologies does not ensure the security of information flows. In pursuit of super speeds, these channels do not provide confidentiality and integrity services. The Diameter protocol provides interaction between clients for authentication, authorization and accounting of various security services, but it has significant drawbacks in terms of modern cyber attacks. To ensure security in cyberphysical systems based on the Internet of things, the KNX standard (ISO/IEC 14543) is applied based on the use of VPN channels (AES–128, –256 encryption). However, all security mechanisms will not provide the required level of security in the post-quantum period (the emergence of a full-scale quantum computer). USA NIST experts raise doubts about the strength of modern symmetric and asymmetric cryptosystems (including elliptic curve algorithms) based on Grover and Shor quantum algorithms. Under such conditions, post-quantum cryptographic algorithms based on the synthesis of theories of error-correcting coding and information protection – crypto-code constructs (CCC) can be considered as an alternative security mechanism. Such constructs are hybrids, since the formation of an asymmetric cryptosystem (cryptographic security is not based on a complexity-theoretic problem of random code decoding) is based on the use of algebraic codes. According to USA NIST experts, to ensure cryptographic strength, the formation of noise-resistant codes is necessary over the Galois field (GF 2^{10}–2^{13}), which is a rather difficult issue even with modern computing resources. The use in wireless cyberphysical systems requires a significant field reduction, which, on the one hand, reduces energy consumption, and on the other hand, requires a certain level of cryptographic strength. Thus, for cyberphysical systems based on wireless mobile technologies, cryptosystems are needed that will provide the necessary level of cryptographic strength in the post-quantum period, energy intensity that will allow them to be used in smart technologies, and also provide a full range of security services.

In addition, there is a need to consider the concept of two security loops (internal – the network infrastructure itself, and external – cloud platforms – cyberphysical systems management servers) in the context of integration of networks and cloud technologies.

2. Literature review and problem statement

Code-based cryptosystems have been recognized as promising alternatives to asymmetric cryptography. This is because they provide security based on well-known NP-hard problems and still demonstrate high performance on a wide range of computing platforms. The main drawback of code-based schemes, including the popular proposals of McEliece and Niederreiter, are large keys whose size is inherently determined by the underlying code. The McEliece cryptosystem is one of the oldest public-key cryptosystems that cannot be cracked. Its simplicity and efficiency make it a very interesting candidate for the post-quantum era, as it is supposed to be immune to quantum computer attacks.

In [1], the McEliece cryptosystem is analyzed, its foundations, advantages and disadvantages are considered, some basic concepts of coding theory necessary to understand the McEliece cryptosystem are presented. The focus of the work is on the code-based encryption protocol. It is assumed that the cryptosystem is resistant to polynomial-time quantum attacks. It is noted that the McEliece cryptosystem has a problem with the key size [2] and decryption time. Therefore, attempts have been made to reduce its key size, but increase protection against known attacks and reduce the encryption and decryption time.

A McEliece-based cryptosystem is proposed that uses Goppa codes, the family used in the original McEliece, and LDPC (Low-Density Parity-Check) codes, a graph-based code family that allows fast hardware decoding. The new construct provides fast encryption and decryption, both software and hardware, and is scaled very well for large messages, solving the above problem. In addition, with this construct, the key size can be reduced by more than ten times compared to the original McEliece. As a further direction of work, it is proposed to find ways to further reduce the key size of the McEliece cryptosystem, which is of great importance if current cryptographic protocols are expected to be replaced by quantum-resistant ones.

In [3], it is proposed to use quasi-cyclic MDPC (Moderate-Density Parity-Check) codes, which provide a very compact representation of keys. In [4], new implementations of the McEliece scheme using QC-MDPC (Quasi-cyclic MDPC) codes adapted for embedded devices are investigated, various approaches to decoding QC-MDPC codes are evaluated and improved. Therefore, current research is aimed at alternative codes that provide a more compact representation of keys, but still retain the security properties of the cryptosystem. In particular, it is proposed to use QC-MDPC codes as an alternative.

Almost all known asymmetric cryptosystems rely on two classes of fundamental problems, namely the factorization problem and the discrete logarithm problem (elliptic curve). Thanks to Shor's efficient algorithm, which solves both problems on quantum computers, it became clear that a greater variety of public-key primitives need to be prepared for using quantum computers. In [5], the possibilities of using a quantum computer to solve coding and encryption problems are presented. The drawback is the instability of the stored and processed information, as well as the limited time of its existence.

The most promising alternatives fall into code-based cryptography and hash-based cryptography. The main disadvantage of many proposed cryptosystems in these classes is low efficiency and practicality due to large key sizes or complex calculations compared to classical cryptosystems. This is especially true for small and embedded systems where memory and processing power are scarce resources. Code-based cryptosystems, such as the well-established proposals of McEliece and Niederreiter, have been shown to significantly outperform classical asymmetric cryptosystems on embedded systems. The work [6] explored the implementation of the McEliece scheme in embedded systems, which was considered a problem due to the need to store large keys. The paper [7] describes methods for the systematic design of an embedded coprocessor for a McEliece post-quantum secure cryptosystem. The joint development of hardware and software aims to put McEliece into practice on low-cost embedded platforms. Optimization of the construct occurs when selecting system parameters, transforming algorithms, choosing architecture and arithmetic primitives.

It is noted in [8] that most of the commonly implemented public-key cryptosystems have proved their security based

on the assumed complexity of two mathematical problems: factoring the product of two large primes and computing discrete logarithms. Both problems are believed to be computationally unsolvable on a conventional computer. However, a quantum computer capable of performing calculations on several thousand qubits could solve both problems using Shor's algorithm. It is argued that the main disadvantage of the McEliece public-key cryptosystem is a very large public key consisting of several hundred thousand bits. Another drawback of the McEliece scheme, like many other ones, is that it is not semantically secure. An implementation of a public-key cryptosystem is proposed, which is semantically secure and uses a 40 times smaller public key and a five times smaller private key than earlier implementations. This superiority comes at the cost of very long keys (often more than 50 kB).

Although code-based encryption schemes were proposed over 30 years ago, they are hardly found in any (cost-driven) real-world applications due to their large private and public keys. Robert McEliece's original proposal for a code-based encryption scheme was to use binary Goppa codes, but in general any other linear code could be used. While other types of codes may have advantages such as a more compact representation, most proposals using other codes have proven to be less secure. In [9], a cryptosystem construct based on generalized Srivastava codes, a large class that includes Goppa codes as a special case, is presented. This approach allows the use of relatively short public keys without being vulnerable to known structural attacks.

In [10], various derivatives of the McEliece cryptosystem are investigated and their structural flaws are studied. An efficient structural attack on the McEliece cryptosystem based on algebrogeometric codes defined on elliptic curves is designed. This attack is based on the Sidelnikov and Shestakov algorithm, which solves the corresponding problem for Reed-Solomon codes. The presented algorithm is heuristic with polynomial time. The Sidelnikov cryptosystem based on Reed-Mahler binary codes is shown to be unreliable. The main idea of the proposed attack is to exploit the fact that the minimum weight words in the Reed-Mahler code have very specific properties. This attack is based on the ability to find minimum weight words in the code, which in this particular case is much easier than normal decoding. The attack has a sub-exponential execution time if the code order is kept fixed, and cracks large keys, as Sidelnikov suggested, in less than an hour on a standard PC.

The Niederreiter cryptosystem is an independently developed version of the McEliece's proposal, which has proved its equivalence in terms of security [11]. Many proposals have already tried to solve the problem of large keys by replacing the originally used binary Goppa codes with (secure) codes that allow more compact representations. So, in [12], new parameters are proposed for McEliece and Niederreiter cryptosystems, which provide standard protection against all known attacks. The new parameters take into account an improved attack, the introduction of list decoding for binary Goppa codes and the ability to select a code length that is not a power of two. The resulting public key sizes are significantly smaller than previous options for the same security level. In [13], efficient implementations of McEliece versions using quasi-dyadic codes are presented. Of note is the presentation of secure parameters for the classical McEliece encryption scheme based on quasi-dyadic generalized Srivastava codes and the sequential conversion of the scheme into a secure protocol by applying the Fujisaki-Okamoto transformation.

Despite the claims that many attempts have failed, and for the few remaining there are practically no publicly available implementations [14], a number of publications refute this statement. The paper [15] proposes a new approach to investigating the security of the McEliece cryptosystem using error-correcting codes. It is noted that since its invention, no effective attack has been developed that would allow recovering the private key. It is proved that the private key of the cryptosystem satisfies a system of bihomogeneous polynomial equations. This property is due to a special class of considered codes, which are alternative codes. It is stated that the implementation of the described algebraic attack in the Magma computer algebra system allows you to find a secret key in a short time for almost all proposed problems. In [16], a new general method for reducing the size of a public key using quasi-cyclic codes was proposed. A method of hiding the structure of a secret generator matrix is considered by first selecting the subcode of the subfield of a quasi-cyclic code defined in a large alphabet, and then by randomly reducing the selected subcode. The security of the proposed option is related to the difficulty of decoding a random quasi-cyclic code.

In [17], an algorithm based on "families of random differences" is proposed, which allows one to build very large sets of equivalent codes. Extensive cryptoanalysis has been developed to test the level of security achievable by the selected system parameters. The proposed scheme provides satisfactory system reliability with a reduced key size and increased transmission rate. Moreover, it was found that the new cryptosystem can be rather fast to justify its adoption as an alternative to widespread solutions such as RSA. [18] considers possible incorporation of quasi-cyclic low-density parity-check codes into the McEliece cryptosystem to test the combined security/error control performance, which can potentially be achieved by this scheme. As the linearity of converting a private key to a public key exposes the system to a full crack attack, suitable conditions adapted to this class of codes are presented and discussed. In [19], the authors come to a conclusion that some families of QC-LDPC codes (Quasi-cyclic LDPC) based on cyclic permutation matrices are inapplicable due to security problems. However, other codes based on the "difference families" approach can provide a good level of intrusion protection.

The results obtained led to the conclusion that McEliece based on LDPC codes is not considered a good choice [20].

In [21], two versions of the McEliece cryptosystem are proposed. The first option is based on moderate-density parity-check (MDPC) codes, and the other one – on quasi-cyclic MDPC codes. MDPC codes are the LDPC codes with higher density than those commonly used for telecommunication applications. As a rule, this leads to a deterioration in the error-correcting ability. However, the main thing in code-based cryptography is not necessarily the correction of many errors. Instead, only the number that provides an adequate level of security is important, a condition that MDPC codes satisfy. This approach has many advantages. Under a reasonable assumption, MDPC codes reduce the McEliece key recognition problem to the problem of decoding linear codes. Since message attacks on the McEliece scheme also come down to this problem, the security of our scheme has the advantage that it relies on a well-studied coding theory problem.

All cryptosystems based on the complexity of factorization or discrete logarithming can be attacked for polynomial time using a quantum computer [22]. This threatens most if not all public-key cryptosystems deployed in practice, such as RSA or DSA. Code-based cryptography is considered quantum-resistant and therefore seen as a viable replacement for these schemes in future applications. However, regardless of their so-called "post-quantum" nature, code-based cryptosystems offer other benefits even for modern applications. These benefits are due to superior algorithmic efficiency, which is several orders of magnitude higher than that of traditional schemes.

The McEliece cryptosystem is a code cryptosystem originally proposed using Goppa codes. Its security is based on two assumptions: the indistinguishability of the code family and the difficulty of decoding the general linear code [23]. The decoding problem is a well-studied NP-complete problem that is still considered difficult. On the other hand, the indistinguishability problem is usually the weakest one and depends heavily on the choice of code family. As an example of such fragility, [24] presents a recognizer for high-speed Goppa codes (similar to those originally proposed for digital signature [25] and some realistic security parameters of McEliece cryptosystems). Although this does not constitute a practical attack, it is expected that Goppa codes will not prove to be an optimal choice for code-based cryptography.

MDPC codes seem very convenient for cryptographic purposes. Under the reasonable assumption that distinguishing a (quasi-cyclic) MDPC code from a (quasi-cyclic) random linear code is equivalent to establishing the existence of low-weight codewords in its binary code, we show that these codes reduce the length of the McEliece key. Thus, the security of the McEliece version proposed in [21] depends on only one well-studied coding theory problem. This is a strong argument in favor of the proposed scheme, and it should be compared with the scenario for Goppa codes. Distinguishing Goppa codes is not necessarily a complex problem. Although this does not necessarily lead to a practical attack, it shows that algebraic codes are not the optimal choice for cryptography.

In [26], decoding optimization methods for MDPC codes are proposed and several efficient implementations of the McEliece QC-MDPC cryptosystem are considered. These include high-speed and lightweight architectures for reconfigurable hardware, efficient coding styles for the ARM Cortex-M4 microcontroller, and new high-performance software implementations that make full use of vector instructions. Based on the data presented in the publication, it can be concluded that McEliece encryption, in combination with QC-MDPC codes, not only provides high-performance implementations, but also allows you to create lightweight constructs on a wide range of different platforms.

In the context of public-key cryptography, the McEliece cryptosystem is a very reasonable solution based on the complexity of the decoding problem, which is believed to be able to resist with the advent of quantum computers. Despite this, the original McEliece cryptosystem based on Goppa codes aroused limited interest in practical applications, partly due to some restrictions imposed by this very special class of codes.

In [27], the latter proposal is developed by introducing bit-reversal decoding for QC-LDPC codes, which leads to a significant reduction in decoding complexity due to moderate losses in terms of error correction performance. The performance of bit-reversal decoding can be easily predicted with theoretical arguments, and this helps determine the size of the system without the need for lengthy numerical simulations. The most effective attack procedures known to date are also considered and their performance is analytically estimated. Thus, tools are provided that allow the developer to easily find the best set of system parameters to optimize the trade-off between security and complexity. The proposed modification is aimed at overcoming the main shortcomings of the original system, while providing a satisfactory security level.

It is argued in [28] that the most effective way to overcome the shortcomings of the McEliece cryptosystem would be to replace the Goppa codes with other code families, which would provide a more compact representation of their characteristic matrices and increase the coding rate. Unfortunately, although there are several code families with these characteristics, only in very few cases Goppa codes can be replaced without incurring serious security flaws.

In [29], it is proposed to use an additional key data parameter – the initialization vector (a set of invalid position vectors of the error vector). To counter Sidelnikov's attacks, it is proposed to use MEC modified (shortened) algebrogeometric (elliptic) codes. To do this, you need to use a second additional initialization vector (a set of positions to reduce the error vector). Based on the modification of the classical Niederreiter scheme on non-binary codes, applied algorithms are proposed for generating and decrypting a cryptogram in a modified Niederreiter crypto-code system based on modified (shortened) elliptic codes and software. In [30], security mechanisms based on modified Niederreiter and McEliece crypto-code systems are proposed, which provide the reliability (using error-correcting elliptic codes) and security of transmitted data.

The work [31] presents McEliece and Niederreiter hybrid crypto-code constructs (HCCC) on flawed codes, which use algorithms for causing damage and generating flawed text and damage. This approach reduces the energy consumption in the implementation, but requires an additional damage transmission channel.

In [32], to ensure the security of critical infrastructure systems, it is proposed to use hybrid crypto-code constructs based on modified asymmetric McEliece crypto-code systems based on flawed codes. This allows you to get the maximum number of emergent properties with minimum resources spent for initiation into a systemic synergistic security effect. The main difference from known approaches to constructing hybrid cryptosystems is the use of modified asymmetric crypto-code systems instead of symmetric cryptosystems. To enhance the strength and "reduce" the power of the alphabet (the dimension of the GF (2^6–2^8) field) for constructing modified McEliece crypto-code constructs (CCC), systems based on flawed codes are used.

Thus, the analysis of post-quantum algorithms showed that, depending on the degree of information secrecy, the efficiency of data transmission and its relevance for providing security services, CCC based on LDPC codes can be used. In addition, McEliece and Niederreiter CCC based on MEC (modified (shortened) algebrogeometric (elliptic) codes) can be used in smart, mesh, sensor networks to provide privacy and integrity services only in the internal security loop. This approach does not fully provide the required level of post-quantum cryptographic strength, energy intensity, as well as efficiency, and does not require additional costs for implementation.

3. The aim and objectives of the study

The aim of the study is to develop McEliece and Niederreiter crypto-code constructs based on low-density parity-check codes. This approach allows forming a dual-loop network security system based on mobile technologies and provides security services both in the internal and external loop of the security system based on post-quantum algorithms.

To achieve the aim, the following objectives were accomplished:

– to develop a concept of wireless network security based on mobile technologies;

– to develop mathematical models for building McEliece and Niederreiter crypto-code constructs based on LDPC codes;

– to develop methods for the practical implementation of McEliece and Niederreiter crypto-code constructs.

4. Materials and methods of research

To ensure security in the post-quantum period – the emergence of a full-scale quantum computer, NIST experts propose to use post-quantum algorithms. Such algorithms require an increase in key sequences to 512 bits for symmetric cryptosystems (this provides a safe time of about 60 years), or the use of post-quantum asymmetric cryptosystems (PQAS). Among the contestants of the third round of the competition, algorithms based on the integration of the theory of error-correcting coding and cryptography stand out. Fig. 1 shows the block diagrams of McEliece and Niederreiter crypto-code constructs based on algebrogeometric codes (elliptic codes over the GF (2^8) field, which provide protection against the Sidelnikov attack and reduce energy consumption. In addition, they provide an integrated error correction in the information sequence [33]. Both crypto-code constructs are based on the principle of using error-correcting coding theory and orthogonality of the matrices G – the generator matrix of the linear code, and H – the parity-check matrix of the linear code. As a key sequence in both crypto-code constructs, the masking matrices are used:

– X – masking nonsingular $k\times k$ matrix randomly equiprobably formed by a key source with elements from $GF(q)$;

– P – permutation $n\times n$ matrix randomly equiprobably formed by a key source with elements from $GF(q)$;

– D – diagonal $n\times n$ matrix formed by a key source with elements from $GF(q)$;

– G – generator matrix of dimension $k\times n$ (McEliece *CCC*);

– H – parity-check matrix of dimension $r\times n$. In addition, a distinctive feature of Niederreiter *CCC* is the preliminary use of equilibrium coding, which allows for an almost relative coding rate equal to one.

However, the McEliece *CCC* provides an integrated (by one mechanism) error correction. The Hamming weight (the number of non-zero elements of the error vector e) does not exceed the correcting ability of the algebraic block code used $\left(0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor\right)$. The use of *MEC* in crypto-code constructs provides the required level of cryptographic strength by using initialization vectors (IV_i, where i is the number of shortening or lengthening symbols), and also allows constructing them over GF (2^6). The papers [29, 32] present mathematical models and practical algorithms for their implementation, as well as the results of studies of their cryptographic strength. Hybrid crypto-code constructs based on flawed codes can reduce the level of energy consumption (built over the GF (2^4) field, and provide the required level of cryptographic strength by using two-channel cryptography [30–32]. However, using them in smart technologies and wireless mobile network standards is difficult, due to the need for additional conversion of m-ary code sequences into binary ones and vice versa, which requires additional energy consumption. To solve this issue, it is proposed to use LDPC codes to build crypto-code constructs.

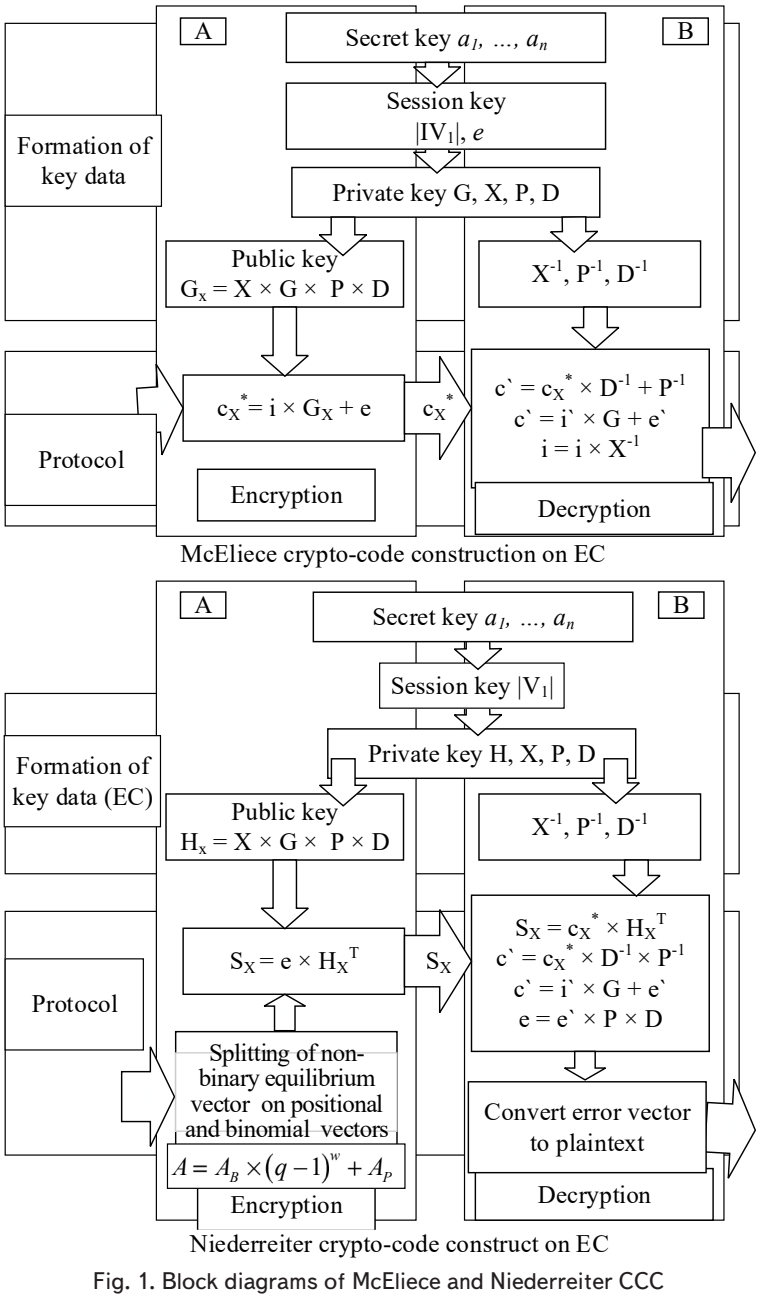

Fig. 1. Block diagrams of McEliece and Niederreiter CCC

LDPC codes are used in modern data transmission standards such as DVB-S2, Gigabit Ethernet, WiMAX, Wi-Fi. This ensures their use in any communication system, for example, in space communications, microwave communication systems, digital satellite television.

The formation of regular LDPC codes is determined by a sequential procedure [34–42]. A regular LDPC code with block length n is generated based on the parity-check matrix H, which is characterized by a constant number of units in the W_r row and a constant number of units in the W_c column. The parity-check matrix H has a low density of units (the density of units is considered low if a specific part of units is less than 50 % of all elements of the parity-check matrix).

Based on the given parameters n, W_r, W_c, the corrective properties of the code (t bit) are changed. The position of units in the parity-check matrix H is formed on the basis of random permutations of the columns of the base submatrix containing only one unit in each column. The rate of a regular LDPC code, depending on the parameters of the parity-check matrix, is determined by the formula:

$$r_k = \frac{n - \left(n \cdot \frac{W_c}{W_r} - (W_c - 1)\right)}{n} = 1 - \frac{W_c}{W_r} + \frac{W_c - 1}{n}, \qquad (1)$$

where n is the length of the code sequence, W_r is the number of units in the row of the parity-check matrix H, W_c is the number of units in the column of the parity-check matrix H; r_k is the coding rate of the regular LDPC code.

At the same time, matrices H of the LDPC code with the same size and parameters can generate codes with different code distance d and correction power t.

The parity-check matrix of the LDPC code can be presented as:

$$H = \begin{bmatrix} H_1 \\ \hline \pi_1(H_1) \\ \hline \vdots \\ \hline \pi_{Wc-1}(H_1) \end{bmatrix}, \qquad (2)$$

where H_1 is the base submatrix, $\pi_1(H_1)$ are the submatrices obtained by random permutation of the columns of the base submatrix H_1, i=1, 2, ..., W_{c1}.

The parity-check matrix H can be reduced to the form:

$$H = [A | I_{n-k}], \qquad (3)$$

where A is some fixed $((n-k)\times k)$ matrix with 0 s and 1 s (which is no longer 1-sparse), I_{n-k} is the identity matrix of size $((n-k)\times(n-k))$.

The codeword generation matrix G has the form:

$$G = [I_k | -A^T]. \qquad (4)$$

If the matrix H is presented as (3), then the matrix G (4) is easily obtained from the matrix H by Gaussian transformations.

Thus, taking into account expressions (1)–(4) and block diagrams of McEliece and Niederreiter *CCC*, it is possible to use post-quantum cryptosystems of provable strength to ensure information security in wireless networks based on mobile technologies [43].

To ensure security in cyberphysical systems and smart technologies, the KNX standard (ISO/IEC 14543) is used, which provides security services such as data confidentiality and integrity [44–51]. Fig. 2, 3 present the basic principles of security according to the KNX standard.

The KNX IP Secure standard allows authentication and encryption of KNX telegrams in IP networks. Tunneling is usually formed, which provides the confidentiality of information. KNX IP Secure mechanisms are an additional security shell that protects all KNXnet/IP data traffic.

However, KNX IP Secure is not so secure, the network can be monitored, sent packets can be recorded and easily repeated, because there are no line connectors with the "Security Proxy" function. In addition, the use of the AES-128 algorithm in the formation of tunneling in the post-quantum period will not provide the required level of protection even for the inner loop.

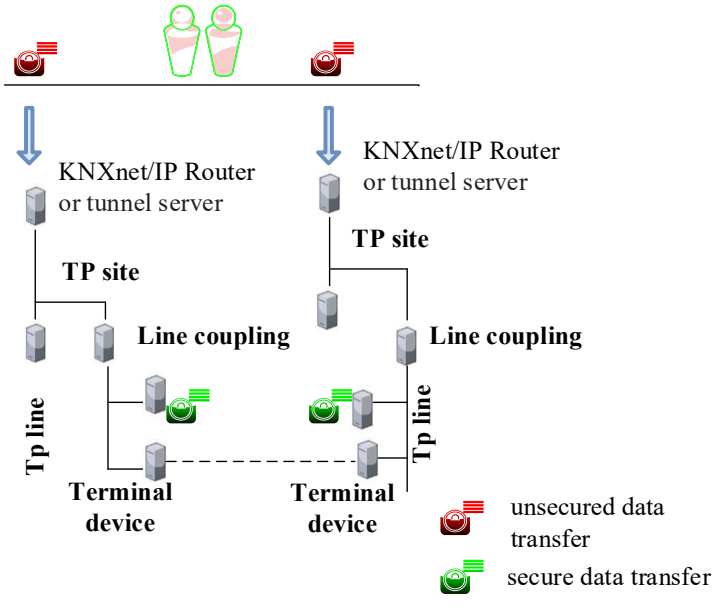

Fig. 2. Security in mobile wireless channels based on KNX

In Fig. 3, the presented interaction protocol based on wireless mobile Internet confirms the possibility of ensuring data confidentiality only in the internal security loop, within the network infrastructure. However, in the external security loop, the standard does not provide services. It is assumed that this is done by security technologies in cloud platforms, which, given the availability of intelligence services of developed countries, casts doubt on the provision of security services. Thus, the control system that is hosted and implemented on the basis of cloud technologies (external security loop) is not fully secure. With the advent of quantum computers, the possibility of secure performance of the full range of functions is called into question.

KNX Data Secure protects user data from unauthorized access and manipulations using encryption and authentication mechanisms. KNX Data Secure devices use a longer KNX telegram format (extended frames) than conventional devices to transmit authenticated and encrypted data.

KNX Data Secure uses the CCM (Cipher Chain Message Authentication Code Counter) mode with 128-bit AES encryption to ensure information integrity. However, the proposed options for using the KNX standard provide only integrity and do not provide confidentiality of information, which significantly reduces the overall security of information flows in wireless mobile networks.

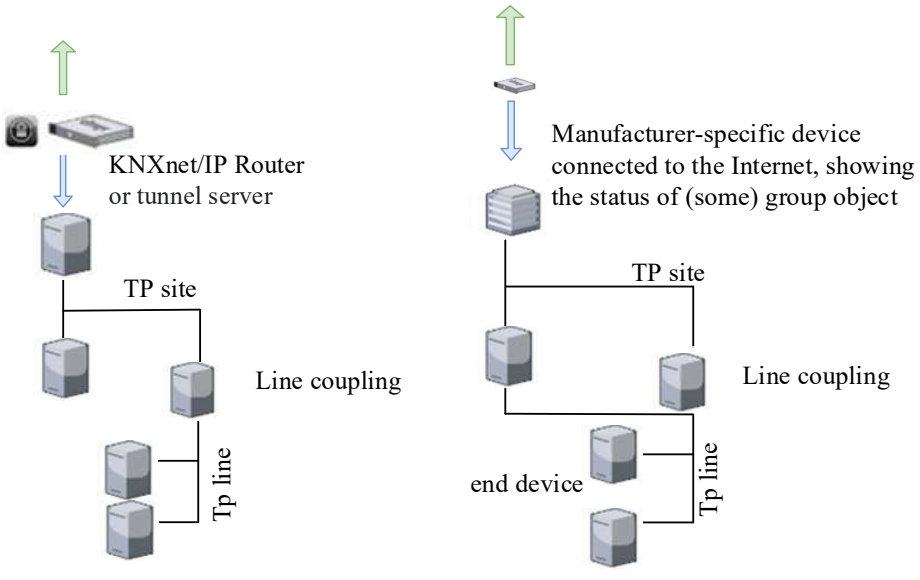

Fig. 3. KNX Data Secure: *a* – KNX IP Secure; *b* – KNX Data Secure

To ensure authenticity in mobile wireless technologies and networks, the Diameter protocol is used. The Diameter protocol has a predefined set of common attributes and assigns appropriate semantics to each attribute. These AVP (Attribute-Value-Pair) convey AAA (authentication, authorization, accounting) details (such as routing, security, and capabilities) between two Diameter nodes. In addition, each AVP pair is associated with the AVP Data Format defined in the Diameter protocol (e.g., OctetString, Integer32), so the value of each attribute must follow the data format [52–56]. However, the Diameter protocol, like previous mobile network protocols, was not designed with security in mind. Therefore, it has almost all the threats inherent in the "G" technology.

Developers in pursuit of super-speeds do not think that the development of computer technology allows intruders (cyberterrorists) to "expand the range and boundaries" of threats. In other words, to consider the use of this technology for organizing a "window" to corporate networks and/or local user networks.

As practice shows, in networks based on the Diameter protocol, attacks aimed at denial of service, disclosure of information about subscribers and the operator's network, as well as fraud against the operator are possible.

In addition, an attacker can forcefully transfer the subscriber's device to 3G mode and carry out attacks on the less secure SS7 system.

The goals of attacks are listening to voice calls, intercepting SMS, and implementing fraudulent schemes against subscribers [57, 58]. Thus, the lack of cryptographic algorithms to ensure confidentiality and integrity services leads to the identification of the following classes of "classical" attacks (Fig. 4).

At the same time, confidentiality implies protecting data from passive attacks during transmission, integrity – protecting data during storage, and authenticity – the authenticity of the message source.

The analysis of Fig. 4 shows that if mobile wireless technologies have only this protocol, confidentiality and integrity problems are not solved. The use of KNX mechanisms provides these services only within the infrastructure of cyberphysical systems, and does not provide protection in the external security loop – a cloud-based platform. Table 1 shows the main characteristics of wireless mobile and computer networks and security services based on the KNX standard and the Diameter protocol.

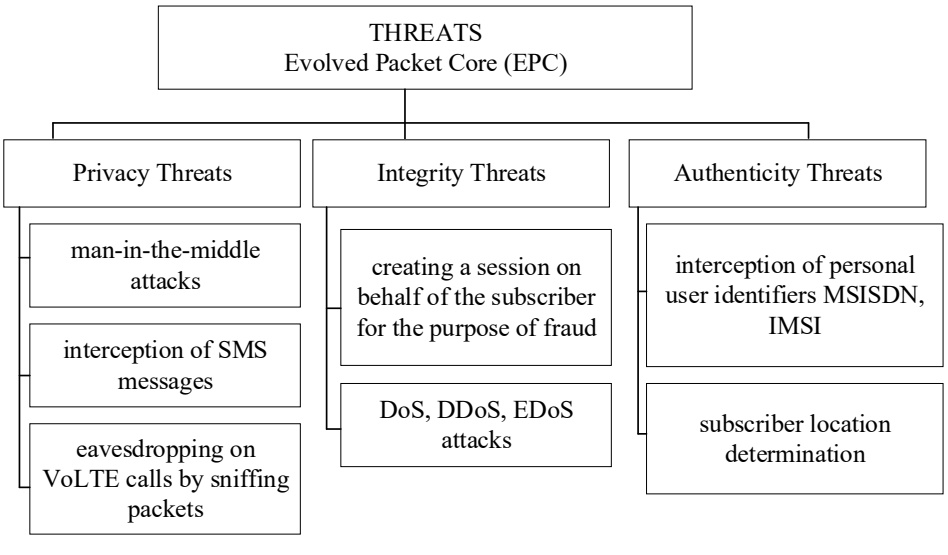

Fig. 4. Main types of attacks on Evolved Packet Core

The analysis of Table 1 shows that with the emergence of a full-scale quantum computer, services in the internal security loop are questioned, due to quantum hacking algorithms of symmetric and asymmetric algorithms. In addition, Diameter-based mobile technologies provide only AAA services. In modern conditions of hybridity and synergy of cyberattacks, this allows you to freely gain unauthorized access to both internal and external security loops and implement targeted attacks on cyberphysical systems.

To ensure the development of mesh and sensor network technologies using wireless channel standards: LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth mobile technologies, new approaches to providing security services are needed. In the context of the emergence of a quantum computer (a possible decrease in "trust" in modern cryptosystems based on symmetric and asymmetric cryptography (including elliptic curve cryptography), it is necessary not only to use post-quantum cryptographic algo-

rithms, but also a new approach to ensuring the security of socio-cyberphysical systems (SCFS) formed on the basis of synthesis, which are rapidly developing based on smart and Internet of things technologies.

To provide security services in the face of modern threats, the concept of dual-loop security based on post-quantum algorithms – McEliece and Niederreiter crypto-code constructs is proposed. At the same time, it is proposed to apply integrated solutions for the use of certain codes in crypto-code systems based on the gradation of the degree of information secrecy in socio-cyberphysical systems. Table 2 shows the ratio of time and information secrecy.

Table 1

Wireless network specifications table

Technology	Transmission reception range, m	*V*, bit/s	topology	Transmission range	Modulation	security services									
						before PQ					in PQ				
						C	*I*	*A*	A_u	*B*	*C*	*I*	*A*	A_u	*B*
LTE (4G)	up to 13,400	up to 100 Mbit/s	AIPN	600 MHz Up to 2.5 GHz	64QAM	–	–	+	+	–	–	–	–	–/+	–
LTE (5G)	500	20 Gbit/s	Heterogeneous backbone	from 30 GHz up to 300 GHz	256-QAM	–	–	+	+	–	–	–	–	–/+	–
IEEE 802.11 ac (WiFi 5)	500	up to 7 Gbit/s	P2MP	5 GHz	256-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.11ax, Wi-Fi 6	–	9,607 Mbit/s	P2MP	5 GHz	1,024-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16	5,000	32 Mbit/s 134 Mbit/s	mesh	1066 GHz	64QAM O-QPSK	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16m (WiMAX2)	6,000	90 Mbit/s 179 Mbit/s	mesh	11 GHz	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.1 Bluetooth 5	200	26 Mbit/s	mesh	2.42.485 GHz	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.4	1,000	250 Kbit/s	P2P Cluster tree	2.42.483 GHz	BPSK O-QPSK	+	+	+	+	–	–	–	–	–/+	–

Note: C – confidentiality; I – integrity; A – availability; Au – authenticity, B – involvement

Table 2

Time and information secrecy ratio

Degree of information secrecy	Time	Proposed codes for CCC
critical	up to 1 year	*MEC*, flawed codes
high	up to 1 month	*MEC*
average	up to 1 hour	*EC*
low	up to 10 minutes	*EC*
very low	up to 1 minute	LDPC

This approach allows timely provision of the required security level, taking into account the degree of information secrecy and/or the safe time to provide confidentiality services.

Thus, there is a need to form a security concept based on two circuits: internal – directly the security of network infrastructure elements and external – a cloud-based management platform.

5. Results of the development of the wireless network security concept based on crypto-code constructs

5. 1. Development of the wireless network security concept based on mobile technologies

To ensure the security of modern wireless networks and systems based on their infrastructure, it is necessary to take into account the integration of the internal infrastructure of network elements (internal loop) and the external management infrastructure based on cloud platforms.

The synthesis of internal and external circuits ensures efficiency, energy intensity and relative safety (each circuit builds security on its own mechanisms and principles), on the one hand. On the other hand, there is no way to control not only the security mechanisms used, but also to assess the current state of security of information flows circulating and stored in the circuit. Fig. 5 shows a block diagram of the dual-loop security concept for socio-cyberphysical systems.

Security systems of socio-cyberphysical systems are mostly focused on critical infrastructure facilities (banking and financial sector, fuel and energy complex, life support networks, telecommunications and communication networks, security and defense complex, etc.). To ensure the security of such systems, two classes of threats must be considered. The first class is threats and their integration with the methods of social engineering of the internal infrastructure (internal security loop). The second class is threats of the external loop (cloud technologies that provide not only the management of socio-cyberphysical systems and networks, but also the storage/duplication of the database). The works [31, 59] propose methodological foundations for building security systems, taking into account the synergy and hybridity of modern targeted attacks on critical infrastructure facilities, which makes it possible to ensure security in the internal loop.

To ensure the safety of the entire security system, it is necessary to take into account the threats of the internal and external circuits:

– threats of the internal loop, taking into account hybridity and synergy [59]:

$$W^{SCPS\ ISL}_{hybrid\ C,I,A,Au,Af\ synerg} = W^{SCPS\ ISLC}_{synerg} \bigcap W^{SCPS\ ISLI}_{synerg} \bigcap$$
$$\bigcap W^{SCPS\ ISLA}_{synerg} \bigcap W^{SCPS\ ISLAu}_{synerg} \bigcap W^{SCPS\ ISLInv}_{synerg}, \quad (5)$$

where $W^{SCPS\ ISLC}_{synerg}$ is the synergy of confidentiality threats, $W^{SCPS\ ISLI}_{synerg}$ is the synergy of integrity threats, $W^{SCPS\ ISLA}_{synerg}$ is the

synergy of availability threats, $W_{synerg}^{SCPS\ ISLAu}$ is the synergy of authenticity threats, $W_{synerg}^{SCPS\ ISLInv}$ is the synergy of involvement threats;

– threats of the external loop, taking into account hybridity and synergy:

$$W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ESL} = W_{synerg}^{SCPS\ ESLC} \cap W_{synerg}^{SCPS\ ESLI} \cap \cap W_{synerg}^{SCPS\ ESLA} \cap W_{synerg}^{SCPS\ ESLAu} \cap W_{synerg}^{SCPS\ ESLInv}, \quad (6)$$

where $W_{synerg}^{SCPS\ ESLC}$ is the synergy of confidentiality threats, $W_{synerg}^{SCPS\ ESLI}$ is the synergy of integrity threats, $W_{synerg}^{SCPS\ ESLA}$ is the synergy of availability threats, $W_{synerg}^{SCPS\ ISLAu}$ is the synergy of authenticity threats, $W_{synerg}^{SCPS\ ESLInv}$ is the synergy of involvement threats.

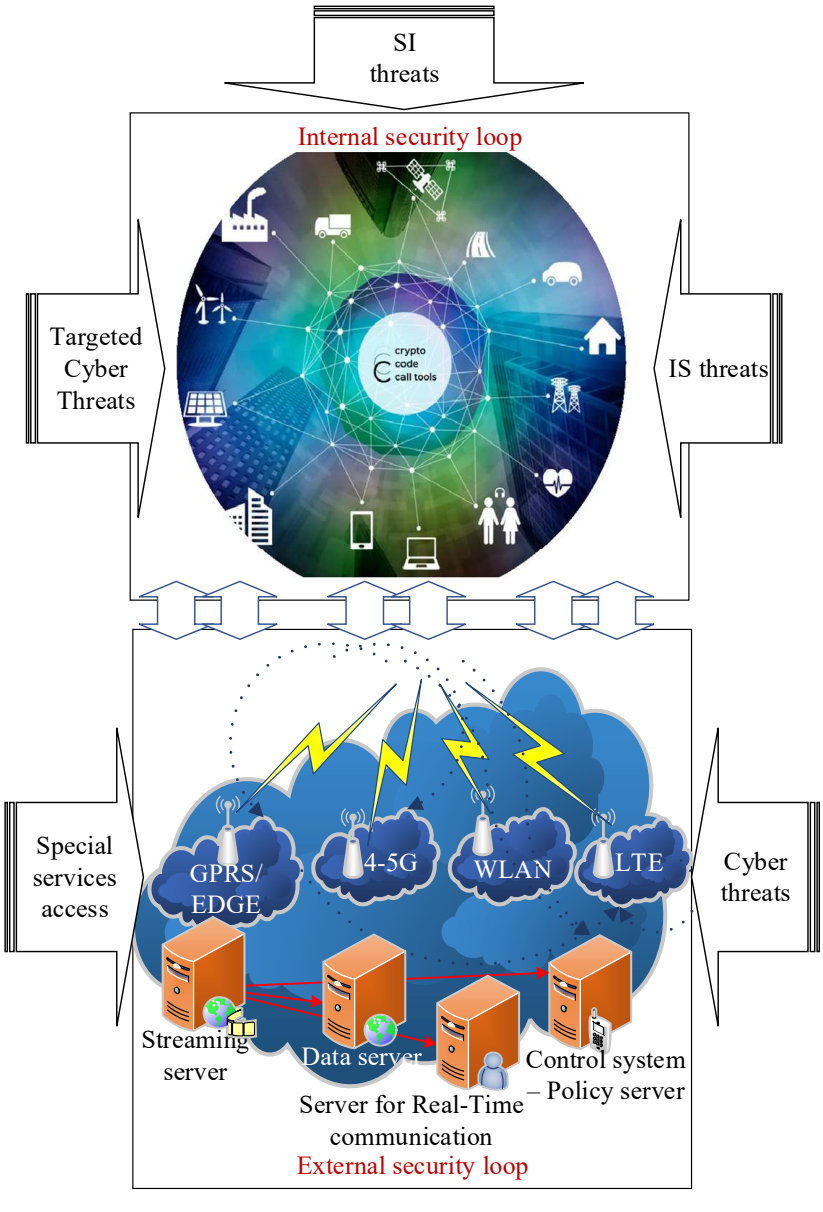

Fig. 5. Block diagram of the concept of dual-loop security of socio-cyberphysical systems

Each element of information resources $I_{A_i} \in \{I_A\}$ can be described by the vector $I_{A_i} = (Type_i, A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i)$. $Type_i$ – type of information asset, described by a set of basic values: $Type_i$={CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i}, where CI_i – confidential information, PD_i – payment documents, CD_i – credit documents, TS_i – trade secret, StR_i – statistical reports, $PubI_i$ – public information, $ContI_i$ – control information, PI_i – personal data. $A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$ – security services (A_i^C – confidentiality, A_i^I – integrity, A_i^A – availability, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i – metric of the time and information secrecy ratio for an asset (critical – 1.0; high – 0.75; medium – 0.5; low – 0.25; very low – 0.01).

Then the general (current) level of security of socio-cyberphysical systems based on wireless mobile technologies is described by the expression:

– for additive convolution

$$L_{W_{\text{security}}^{SCPS}} = \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ISL}} \sum_{i=1}^{8} (I_{A_i} \times \beta_i) + \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ESL}} \sum_{i=1}^{8} (I_{A_i} \times \beta_i); \quad (7)$$

– for multiplicative convolution

$$L_{W_{\text{security}}^{SCPS}} = 1 - \left[1 - \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ISL}} \sum_{i=1}^{8} (I_{A_i} \times \beta_i)\right] \times \left[1 - \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ESL}} \sum_{i=1}^{8} (I_{A_i} \times \beta_i)\right]. \quad (8)$$

In (7), (8) index i refers to the corresponding type of information asset, and external summation is performed for all threats of the internal and external loops.

The proposed concept of two security loops provides integration and takes into account the capabilities of targeted cyber attacks, their synergy, hybridity and the possibility of integration in the face of growing computing resources and expanding the range of smart technologies.

5. 2. Development of mathematical models of McEliece and Niederreiter crypto-to-code constructs based on LDPC codes

To implement crypto-code constructs based on LDPC codes, we use the approaches of [29–31, 60].

The initial data for mathematical models of McEliece and Niederreiter *CCC* are:

– a set of plaintexts for McEliece *CCC*

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

where $M_i = \{I_0, I_{h_1}, \ldots I_{h_j}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j – information symbols equal to zero, $|h| = \frac{1}{2}k$, i.e. I_i=0, $\forall I_i \in h$; for the Niederreiter CCC $M_i = \{e_0, e_{h_1}, \ldots e_{h_k}, e_{e-1}\}$, $\forall e_e \in GF(q)$, h_e – error vector symbols equal to zero $|h| = \frac{1}{2}e$, i.e. e_i=0, $\forall e_i \in h$. Based on the equilibrium coding algorithm, the plaintext is converted into an error vector;

– a set of closed texts (codegrams) for McEliece *CCC*

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

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

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

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

– a set of direct mappings (based on the use of a public key – generator/parity-check matrix of the LDPC code:

1) for McEliece CCC – $\phi=(\phi_1, \phi_2, ..., \phi_s)$, where

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

2) for Niederreiter CCC – $\varphi=(\varphi_1, \varphi_2, ..., \varphi_r)$, where

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

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

1) for McEliece CCC – $\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\}$, where

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

2) for Niederreiter CCC – $\varphi^{-1}=\left\{\varphi_1^{-1},\varphi_2^{-1},...,\varphi_r^{-1}\right\}$, where

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

– a set of keys parameterizing direct mappings (authorized user's public key):

1) for McEliece CCC –

$$KU_i=\left\{KU_1,KU_2,...,KU_S\right\}=\left\{G_1^{LDPC},G_2^{LDPC},...,G_S^{LDPC}\right\},$$

where $G^{LDPC_i}_{X_{a_i}}$ – generator matrix disguised as a random code. The matrix is defined from the orthogonality of the generator and parity-check matrices;

2) for Niederreiter CCC – $KU_i=\{KU_1, KU_2, ..., KU_r\}=\{H_1, H_2, ..., H_r\}$, where $H^{LDPC_i}_{X_{a_i}}$ – $(N\text{-}K)\times N$ parity-check matrix defines $(N–K)$ parity-check symbols $P_1, P_2, ..., P_{N\text{-}K}$ as a linear combination of information symbols d_k, k=1, 2, ..., K;

– a set of private keys of users:

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

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

where X^i is a masking nondegenerate $k\times k$ matrix randomly equiprobably formed by a key source with elements from $GF(q)$; P^i is a permutation $n\times n$ matrix randomly equiprobably formed by a key source with elements from $GF(q)$; D^i is a diagonal $n\times n$ matrix formed by a key source with elements from $GF(q)$. Due to the fact that the diagonal matrix is equal to the identity matrix, the value can be neglected, which reduces the capacity and complexity of the calculation.

The public key is formed by multiplying the masking matrices by the generator/parity-check matrices:

– for McEliece CCC –

$$G^{LDPCu}_{X_{a_i}}=X^u\times G^{LDPCu}\times P^u,\ \ u\in\left\{1,2,...,s\right\};$$

– for Niederreiter CCC –

$$H^{LDPCu}_{X_{a_i}}=X^u\times H^{LDPCu}\times P^u,\ \ u\in\left\{1,2,...,r\right\}.$$

The communication channel receives:

– for McEliece CCC – the codeword:

$$C_j=M_i\times G^{LDPCu^T}_{X_{a_i}}+e,$$

where e is an additional session key of each information package;

– for Niederreiter CCC – syndrome sequence:

$$S^*=\left(e_n\right)\times H^{LDPC^T}_{X_{a_i}}.$$

On the receiving side, an authorized user who knows the masking matrices uses a fast algorithm based on soft decoding.

Fig. 6 shows a block diagram of decoding the received sequence based on soft decoding.

The following designations are introduced on the scheme: *LLR* – log-likelihood ratio; d_k – codeword symbol, $d_{ij}\in\{0, 1\}$, $x_k=(2d_k1)+p_k$, p_k – random variable having a normal distribution with zero mean.

The analysis of Fig. 8 shows that the soft decision is the log-likelihood ratio (posterior LLR). A soft decision can be represented by a set of prior, internal and external information. The hard decision for some symbol is based on posterior LLR. The sign of the log-likelihood ratio determines the hard decision, and the value determines the reliability of this decision.

The parity-check matrix has the dimension of $(N–K)\times N$ and allows expressing $(N–K)$ parity-check symbols $P_1, P_2, ...,$ $P_{N\text{-}K}$ as a linear combination of information symbols d_k, k=1, 2, ..., K, that is, defines the parity-check equations:

$$\begin{cases}P_1=c_{11}d_1\oplus c_{21}d_2\oplus...\oplus c_{k1}d_K,\\ P_2=c_{12}d_1\oplus c_{22}d_2\oplus...\oplus c_{k2}d_K,\\ ...\\ P_{N-K}=c_{1\,N-K}d_1\oplus c_{2\,N-K}d_2\oplus...\oplus c_{K\,N-K}d_K,\end{cases}\qquad(9)$$

where c_{ij} are the elements of the submatrix A, $c_{ij}\in\{0,1\}$. If d_k, k=1, 2, ..., K are statistically independent symbols taking the values 0 and 1 and corresponding, in general, to the information symbols of the block code, and $\beta_k=(2d_k–1)=\pm1$.

With this format, the result of adding symbols β_k modulo two is as follows:

$$\begin{cases}\beta_1\oplus\beta_2=-1, \text{if } \beta_1=\beta_2,\\ \beta_1\oplus\beta_2=+1, \text{if } \beta_1\neq\beta_2.\end{cases}\qquad(10)$$

Then the log-likelihood ratio of the sum modulo two of symbols $\beta_k-LLR(\beta_1\oplus\beta_2\oplus...\oplus\beta_K)$ can be written as follows [60]:

$$LLR(\beta_1\oplus\beta_2...\oplus\beta_k\oplus...\oplus\beta_K)=\ln\left[\frac{\sum\limits_k e^{LLR(\beta_k)}}{1+\prod\limits_k e^{LLR(\beta_k)}}\right].\qquad(11)$$

Expression (11) can be approximated as:

$$LLR(\beta_1\oplus\beta_2...\oplus\beta_k\oplus...\oplus\beta_K)\approx$$
$$\approx-1\cdot\left[\prod_k\text{sign}\left\{LLR(\beta_k)\right\}\right]\left[\min_k\left\{\left|LLR(\beta_k)\right|\right\}\right],\qquad(12)$$

where the sign(•) function returns the sign of its argument.

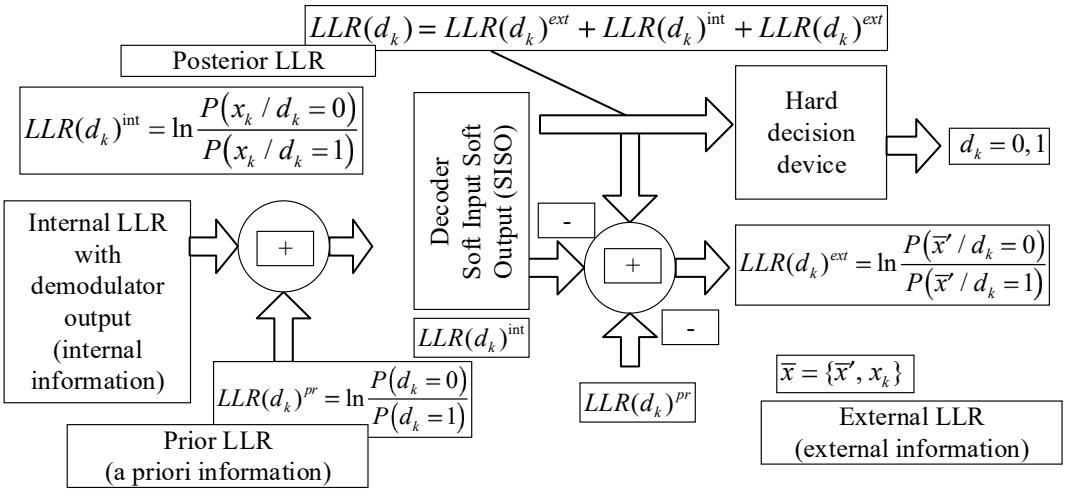

Fig. 6. Soft decision decoding scheme

Each parity-check equation (9) allows you to express one symbol (regardless of whether it is information or parity-check) through the sum modulo two of all other symbols included in this parity-check equation.

The initial data of the algorithm are: a parity-check matrix H of the block (N, K) code, a sequence of soft decisions for information and parity-check symbols from the demodulator output.

LDPC decoding algorithm:

Step 1. Determine the reliability estimate for each code symbol (for each information and parity-check symbol) of the codeword based on soft decisions for the demodulator output by calculating their absolute value (we neglect the sign of soft decisions in the demodulator output sequence).

Step 2. For the row of the parity-check matrix H with the number i, i=1... N–K:

1) find the code symbol corresponding to the non-zero (unit) value of the elements of the row with the number i of the matrix H. This means that the code symbol is part of the parity-check equation determined by the row with the number i, and has the lowest reliability estimate (the least reliable symbol). We fix the column number j, j=1... N of the parity-check matrix H, which corresponds to the least reliable symbol found;

2) transform the parity-check matrix H by linear combination of its rows. Linear combination is performed in order to eliminate the dependence of other parity-check equations (defined by other rows of the parity-check matrix) on the least reliable symbol found. This will be achieved when the column of the matrix H with the number j will have only one unit contained exactly in the considered row with the number i;

3) repeat preliminary procedures 1 and 2 for each of the rows of the parity-check matrix H, and proceed to the next step.

Step 3. Perform hard decoding of K symbols having the highest reliability estimate (the most reliable symbols).

Step 4. For each of the K most reliable symbols:

1) find soft decisions using two trial code sequences (hypotheses). One trial sequence is generated by re-encoding the hard decoding result of the K most reliable symbols obtained in Step 3 (first hypothesis). The other is formed by re-encoding the result of hard decoding of the K most reliable symbols obtained in Step 3, but with an additional inversion of the symbol for which a soft decision is found (second hypothesis);

2) find a hard decision based on the soft decision obtained in the preliminary procedure.

Step 5 (optional). We update the reliability estimate for each code symbol and proceed to Step 1 for the next iteration.

Thus, the presented algorithm ensures the efficiency of decoding and the use of LDPC codes in McEliece and Niederreiter crypto-code constructs. This approach allows you to vary, depending on the degree of information secrecy in the selection of an error-correcting code for crypto-code constructs, and ensure the required level of security.

5. 3. Development of methods for implementing McEliece and Niederreiter crypto-code constructs

An example of the implementation of such systems is the protocol for ensuring the security of voice messages in online mode proposed in [60] based on McEliece and Niederreiter *CCC* on *EC* (*MEC*) shown in Fig. 7. Fig. 8 shows the implementation of the proposed concept and crypto-code constructs based on LDPC codes. The proposed security protocol for cyberphysical systems ("Smart Home") is based on a two-loop security concept and post-quantum algorithms.

So, in Fig. 7, to ensure the security of voice messages, it is proposed to use a hardware-software encoder, which is built into the headset (Bluetooth headphones) and provides encryption of a digital message based on McEliece *CCC*. Then the encrypted message is transmitted via the Bluetooth channel to a mobile gadget. In this case, standard protocols of the GSM mobile Internet channel are used. This allows you to ensure the confidentiality of conversation without taking into account the requirements of the communication channel, requirements of manufacturers of headsets and mobile gadgets, not to take into account modifications of both the Bluetooth channel and mobile Internet technology.

In addition, the use of a hardware-software implementation of the encoder in the form of a chipset can significantly reduce the cost of production and implementation of this approach. To ensure security, only the session password is recorded in the headphones, depending on the role (sender, recipient), which are recorded from the mobile application.

After the end of conversation, they are deleted. In this case, the chipset implements the encoder based on McEliece *CCC*. The security of key data transfer between the mobile application and the server is ensured by Niederreiter *CCC*. To ensure the security of the server part, after generating keys for a conversation and transferring them

to the sender and recipient, the server RAM is reset, which ensures channel tunneling between users. The secret keys of McEliece and Niederreiter crypto-code constructs change at different time intervals and are OTP keys (session keys).

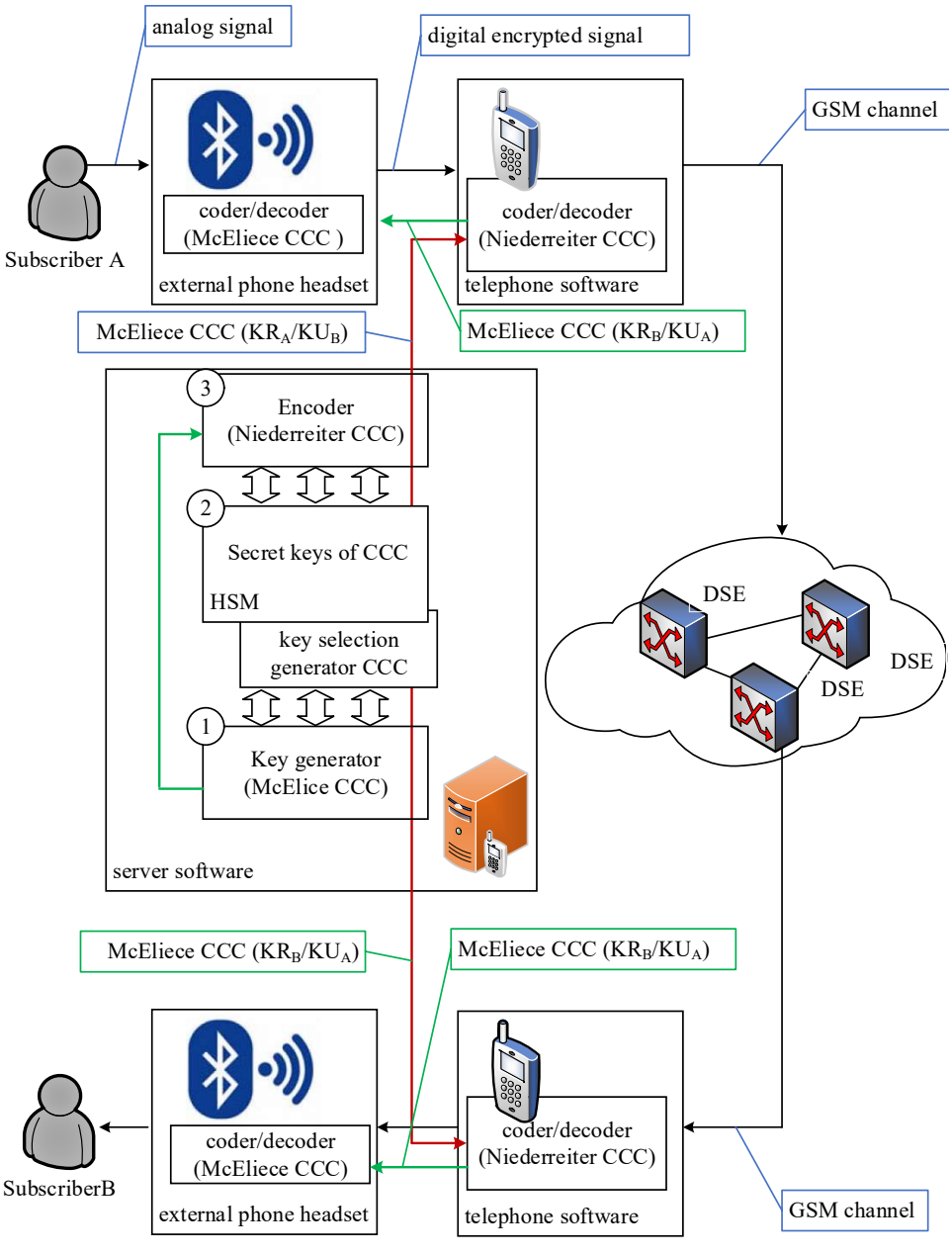

Fig. 7. Block diagram of a two-loop information security system based on CCC to ensure the confidentiality of voice messages

Consider a voice message security protocol based on post-quantum algorithms:

SUBSCRIBER A (call initiator):

1. Opens the phone software and finds the corresponding subscriber (Subscriber B) in the list.

2. Sends a request to subscriber B through the server.

3. Receives a private key on the phone software through a private channel (using encryption based on Niederreiter CCC on *EC*), and a public key of subscriber B.

4. Confirms readiness for conversation. At the same time, the private key KR_A and the public key KU_B are transmitted from the phone software via the Bluetooth channel.

5. The key is recorded in the Bluetooth headphones in the encoder (coder/decoder).

6. After the key is recorded, a signal of readiness is generated.

7. After confirmation of the readiness of subscriber B, a conversation is carried out.

SERVER SOFTWARE:

1. At the request of subscriber A in Secret keys of *CCC* (block 2), the *CCC* Key Selection Generator randomly selects the key parameters and sends them to the key generator (block 1).

2. In the key generator, secret keys are received from GSM (masking matrices – X, P, D, and generator matrix G^{EC}).

3. In the key generator, KR_A (McEliece *CCC* private key of subscriber A) and KU_A (public key of subscriber A) are generated.

4. Based on the response of subscriber B, the public key KU_B is generated and transmitted to subscriber A.

5. In the encoder (block 3), the generated KR_A and KU_A are received from the key generator (block 1), the data is deleted after the keys are transmitted to the key generator.

6. In the encoder, KR_A, KU_A, KU_B are encrypted.

7. From the encoder, KR_A, KU_B are sent to subscriber A (the subscriber who initiates the call), KU_A – to subscriber B (the subscriber who is being called), the data is deleted after the keys are transmitted to the encoder.

SUBSCRIBER B (recipient of the call):

1. Receives a request from the server in the phone software to transfer the public key (KU_A).

2. Confirms the request to the server, sends KR_B.

3. Receives the public key KU_A on the phone software via a private channel (using encryption based on Niederreiter CCC on EC).

4. Confirms readiness for conversation. At the same time, the public key (KU_A) is transmitted from the phone software via the Bluetooth channel.

5. The key is recorded in the Bluetooth headphones in the decoder (coder/decoder).

6. After the key is recorded, a signal of readiness is generated.

7. After confirmation of readiness, subscriber B sends a signal to the server that he is ready for conversation.

Thus, the proposed protocol ensures the closure of the mobile Internet channel using software and hardware. Using a hardware solution for closing (encrypting) a voice message in a headset will counteract almost all threats, and using a key server provides a tunnel mode, which eliminates the possibility of "eavesdropping" of voice messages.

Fig. 8 suggests using McEliece and Niederreiter CCC based on LDPC codes to ensure security in cyberphysical systems.

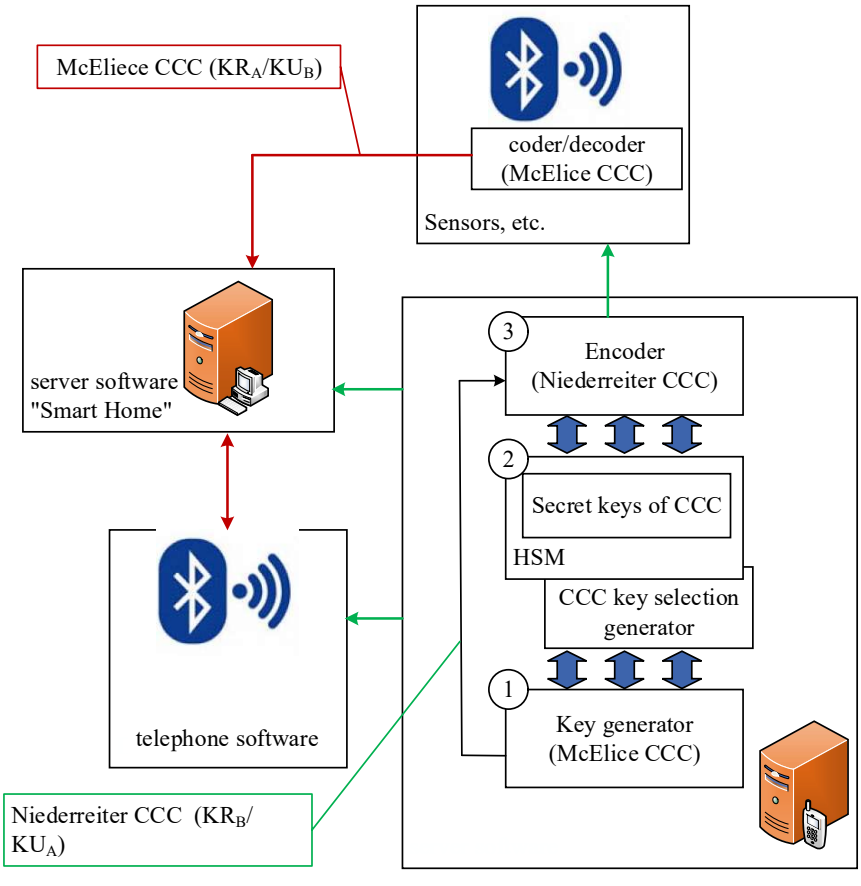

Fig. 8. Block diagram of a two-circuit security system of the "Smart Home" system based on CCC

The use of these post-quantum asymmetric cryptosystems ensures the required level of security when providing security services. The use of LDPC codes allows using mobile wireless technologies based on IEEE802.11ac, IEEE802.11ax, IEEE802.16m, IEEE802.15.1, IEEE802.15.4 standards without significant changes. The smart home system controls a complex of autonomous systems, each of which controls certain devices in the house, connecting them into a common cyberphysical system. However, to ensure the security of the external circuit (control and information storage systems), it is proposed to use the developed server, which is physically located in the house.

Each system sends a data packet to a local server, which allows you to manage your home in the absence of the Internet, being on the same local network (connected to a WI-FI router). Information in the cyberphysical system network is transmitted over open wireless channels with encryption based on McEliece and Niederreiter *CCC* on LDPC codes.

This approach provides security services, and using a local control server, reduces the likelihood of targeted attacks to gain unauthorized access to the Smart Home control system. The approach also provides the required level of security when using mobile control applications, based on the use of McEliece and Niederreiter *CCC* on LDPC codes. To ensure the security of the database, McEliece and Niederreiter *CCC* on *EC* (*MEC*) can be used, which greatly complicates the implementation of R2L class cyber attacks (Remote to Local (user) Attack).

6. Discussion of the results of using McEliece and Niederreiter crypto-code constructs based on LDPC codes

The proposed security approach in *SCFS* is based on the concept of a two-loop security system, post-quantum algorithms – McEliece and Niederreiter crypto-code constructs based on various codes. This approach provides a complex system approach in building two circuits of the information security system, takes into account the signs of synergy and hybridity of targeted attacks, and ensures the full purposeful development of smart technologies and technologies based on wireless mobile systems. Table 2 shows the comparative characteristics of using crypto-code constructs in the post-quantum period, taking into account integration with various standards of wireless and mobile Internet technologies, as well as taking into account the criticality (degree of secrecy) of information.

The analysis of Table 2 shows that classical (symmetric) cryptosystems based on block and stream ciphers (used in the KNX standard) do not provide full confidentiality and integrity services. Application to provide the distribution of key data for symmetric cryptosystems, as well as authenticity and involvement services. In addition, the use of elliptic curve cryptosystems also does not provide the required level of resistance to quantum computing hacking algorithms.

Thus, to ensure security in *SCFS*, it is proposed to use post-quantum algorithms – crypto-code constructs, which, unlike modern security service mechanisms (KNX, IEEE802.11h, IEEE802.16e standards use symmetric encryption algorithms), provide the required level of cryptographic strength. In addition, crypto-code constructs 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 rate of cryptographic transformations, they are compatible with symmetric cryptography algorithms) and the required level of energy intensity. The results of comparative studies on the criteria for cryptographic strength, efficiency, and energy intensity are given in [29–32]. The synthesis of the proposed concept with the proposed technologies based on *CCC* (*HCCC*) not only provide the required level of basic criteria for modern wireless networks, but also fundamentally change the methodological foundations for building security systems in *SCFS*.

Table 3

Comparative characteristics of wireless and mobile Internet technologies

Technology	Security services					Degree of information secrecy (β_i)				
	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* based on *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Mobile technologies+*HCCC* based on *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Mobile technologies+*CCC* based on *LDPC codes*	+	+	+	+	+	–	–	+	+	+

7. Conclusions

1. The development of computing resources, quantum computers and the rapid growth in the use of wireless and mobile technologies allow the formation and development of smart technologies, new network formats based on their synthesis with classical networks. However, in pursuit of super speeds and digitalization, developers do not pay due attention to the security of such systems. The formation of socio-cyberphysical systems based on the integration and synthesis of wireless and mobile Internet technologies with the Internet of things, on the one hand, ensures the development of digital services. On the other hand, they form unprotected critical points used by cybercriminals for malicious purposes. The advent of a full-scale quantum computer only exacerbates the ability to provide the required level of security. In addition, the use of cloud technologies requires a reassessment of approaches to the formation of a security system. Under such conditions, the proposed approach of using a dual-loop security system is relevant and timely. The proposed concept allows you not only to take into account the signs of synergy and hybridity of modern threats, but also provides an objective approach to assessing the current level of security in socio-cyber-physical systems.

2. The use of crypto-code constructs to ensure the security of post-quantum cryptosystems provides a timely transition to post-quantum algorithms. This approach provides the required level of security services, and the use of various codes ensures, taking into account the cost (degree of secrecy) of information, its security when using modern standards of wireless communication channels. At the same time, the cost of security is proposed to be assessed not by a quantitative assessment of damage when it is compromised, but by the time of its relevance, which allows varying the use of error-correcting codes in CCC.

3. Practical methods for implementing post-quantum algorithms provide a solution to a set of problems – ensuring the required level of security (when implementing security services), efficiency and reliability of information flows. The use of both software and hardware-software implementations of McEliece and Niederreiter CCC based on various codes makes it possible to single them out as a separate direction of providing security and reliability services. This approach can significantly simplify security issues in the rapidly developing areas of SCFS, smart and mesh technologies.

References

1. Branco, P. de M. (2017). A new LDPC-based McEliece cryptosystem. Tecnico Lisboa, 79. Available at: https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973967111/Thesis.pdf
2. Engelbert, D., Overbeck, R., Schmidt, A. (2007). A Summary of McEliece-Type Cryptosystems and their Security. Journal of Mathematical Cryptology, 1 (2). doi: https://doi.org/10.1515/jmc.2007.009
3. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2012). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. Available at: https://eprint.iacr.org/2012/409.pdf
4. Baldi, M., Bodrato, M., Chiaraluce, F. (2008). A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes. Security and Cryptography for Networks, 246–262. doi: https://doi.org/10.1007/978-3-540-85855-3_17
5. Chang, K. (2012). I.B.M. Researchers Inch Toward Quantum Computer. The New York Times. Available at: http://www.nytimes.com/2012/02/28/technology/ibm-inch-closer-on-quantum-computer.html?_r=1&hpw
6. Eisenbarth, T., Güneysu, T., Heyse, S., Paar, C. (2009). MicroEliece: McEliece for Embedded Devices. Cryptographic Hardware and Embedded Systems - CHES 2009, 49–64. doi: https://doi.org/10.1007/978-3-642-04138-9_4
7. Ghosh, S., Delvaux, J., Uhsadel, L., Verbauwhede, I. (2012). A Speed Area Optimized Embedded Co-processor for McEliece Cryptosystem. 2012 IEEE 23rd International Conference on Application-Specific Systems, Architectures and Processors. doi: https://doi.org/10.1109/asap.2012.16
8. Heyse, S. (2011). Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices. Lecture Notes in Computer Science, 143–162. doi: https://doi.org/10.1007/978-3-642-25405-5_10

9. Persichetti, E. (2012). Compact McEliece keys based on quasi-dyadic Srivastava codes. Journal of Mathematical Cryptology, 6 (2). doi: https://doi.org/10.1515/jmc-2011-0099
10. Minder, L. (2007). Cryptography Based on Error Correcting Codes. Lausanne. doi: https://doi.org/10.5075/epfl-thesis-3846
11. Overbeck, R., Sendrier, N. (2009). Code-based cryptography. Post-Quantum Cryptography, 95–145. doi: https://doi.org/10.1007/978-3-540-88702-7_4
12. Bernstein, D. J., Lange, T., Peters, C. (2008). Attacking and Defending the McEliece Cryptosystem. Lecture Notes in Computer Science, 31–46. doi: https://doi.org/10.1007/978-3-540-88403-3_3
13. Cayrel, P.-L., Hoffmann, G., Persichetti, E. (2012). Efficient Implementation of a CCA2-Secure Variant of McEliece Using Generalized Srivastava Codes. Lecture Notes in Computer Science, 138–155. doi: https://doi.org/10.1007/978-3-642-30057-8_9
14. Misoczki, R., Barreto, P. S. L. M. (2009). Compact McEliece Keys from Goppa Codes. Lecture Notes in Computer Science, 376–392. doi: https://doi.org/10.1007/978-3-642-05445-7_24
15. Faugère, J.-C., Otmani, A., Perret, L., Tillich, J.-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. Lecture Notes in Computer Science, 279–298. doi: https://doi.org/10.1007/978-3-642-13190-5_14
16. Berger, T. P., Cayrel, P.-L., Gaborit, P., Otmani, A. (2009). Reducing Key Length of the McEliece Cryptosystem. Lecture Notes in Computer Science, 77–97. doi: https://doi.org/10.1007/978-3-642-02384-2_6
17. 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. doi: https://doi.org/10.1109/isit.2007.4557609
18. Baldi, M., Chiaraluce, F., Garello, R. (2006). On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2006 First International Conference on Communications and Electronics. doi: https://doi.org/10.1109/cce.2006.350824
19. Baldi, M., Chiaraluce, F., Garello, R., Mininni, F. (2007). Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2007 IEEE International Conference on Communications. doi: https://doi.org/10.1109/icc.2007.161
20. Monico, C., Rosenthal, J., Shokrollahi, A. (2000). Using low density parity check codes in the McEliece cryptosystem. 2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060). doi: https://doi.org/10.1109/isit.2000.866513
21. Otmani, A., Tillich, J.-P., Dallot, L. (2010). Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 3 (2), 129–140. doi: https://doi.org/10.1007/s11786-009-0015-8
22. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. 2013 IEEE International Symposium on Information Theory. doi: https://doi.org/10.1109/isit.2013.6620590
23. Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.) (2009). Post-Quantum Cryptography. Springer, 246. doi: https://doi.org/10.1007/978-3-540-88702-7
24. Courtois, N. T., Finiasz, M., Sendrier, N. (2001). How to Achieve a McEliece-Based Digital Signature Scheme. Lecture Notes in Computer Science, 157–174. doi: https://doi.org/10.1007/3-540-45682-1_10
25. Faugere, J.-C., Gauthier-Umana, V., Otmani, A., Perret, L., Tillich, J.-P. (2011). A distinguisher for high rate McEliece cryptosystems. 2011 IEEE Information Theory Workshop. doi: https://doi.org/10.1109/itw.2011.6089437
26. Gaborit, P. (2005). Shorter keys for code based cryptography. In International Workshop on Coding and Cryptography – WCC'2005, 81–91.
27. Heyse, S., von Maurich, I., Güneysu, T. (2013). Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices. Lecture Notes in Computer Science, 273–292. doi: https://doi.org/10.1007/978-3-642-40349-1_16
28. Baldi, M., Bianchi, M., Chiaraluce, F. (2013). Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Information Security, 7 (3), 212–220. doi: https://doi.org/10.1049/iet-ifs.2012.0127
29. 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. doi: https://doi.org/10.15587/1729-4061.2018.150903
30. 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. doi: https://doi.org/10.15587/1729-4061.2016.86175
31. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2
32. 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. doi: https://doi.org/10.15587/1729-4061.2017.108461
33. Sidel'nikov, V. M. (2002). Kriptografiya i teoriya kodirovaniya. Materialy konferentsii: Moskovskiy universitet i razvitie kriptografii v Rossii. Moscow: MGU.
34. Ranjitha, C. R., Thomas, J., Chithra, K. R. (2016). A brief study on LDPC codes. International Journal of Engineering Research and General Science, 4 (2), 612–618. Available at: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf
35. Broul´ım, J. (2018). LDPC codes - new methodologies. University of West Bohemia, 127. Available at: https://cds.cern.ch/record/2730008/files/CERN-THESIS-2018-479.pdf
36. Zhu, H., Pu, L., Xu, H., Zhang, B. (2018). Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic. Wireless Communications and Mobile Computing, 2018, 1–9. doi: https://doi.org/10.1155/2018/5264724

37. Singh, H. (2020). Code based Cryptography: Classic McEliece. arxiv.org. doi: https://doi.org/10.48550/arXiv.1907.12754
38. Chen, P.-J., Chou, T., Deshpande, S., Lahr, N., Niederhagen, R., Szefer, J., Wang, W. (2022). Complete and Improved FPGA Implementation of Classic McEliece. Cryptology ePrint Archive: Report 2022/412. URL: https://eprint.iacr.org/2022/412
39. Liva, G., Song, S., Lan, L., Zhang, Y., Lin, S., Ryan, W. E. (2017). Design of LDPC Codes: A Survey and New Results. Journal of Communications Software and Systems, 2 (3), 191. doi: https://doi.org/10.24138/jcomss.v2i3.283
40. Richardson, T. J., Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 47 (2), 638–656. doi: https://doi.org/10.1109/18.910579
41. Chandrasetty, V. A., Aziz, S. M. (2011). FPGA Implementation of a LDPC Decoder using a Reduced Complexity Message Passing Algorithm. Journal of Networks, 6 (1). doi: https://doi.org/10.4304/jnw.6.1.36-45
42. Wang, Y. (2008). Generalized constructions, decoding and implementation of LDPC codes. University of Hawaii at Manoa. Available at: https://scholarspace.manoa.hawaii.edu/bitstream/10125/20577/Ph.D._AC1.H3_5085_r.pdf
43. Sarvaghad-Moghaddam, M., Ullah, W., Jayakody, D. N. K., Affes, S. (2020). A New Construction of High Performance LDPC Matrices for Mobile Networks. Sensors, 20 (8), 2300. doi: https://doi.org/10.3390/s20082300
44. Hübner, C., Merz, H., Hansemann, T. (2009). Gebäudeautomation. Kommunikationssysteme mit EIB/KNX, LON und BACnet. Hanser. doi: https://doi.org/10.3139/9783446422636
45. 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX / Busch-Watchdog Sky KNX (2017). Busch-Jaeger Elektro GmbH, 198. Available at: https://library.e.abb.com/public/ddedcbf7ab704705affb179ca91e0fa2/2CKA001473B8668_Prasenzmelder_6131_03_ABB_EN.pdf
46. Technical documentation on KNX devices (2006). ABB.
47. KNX Handbook Version 1.1 Revision 1 (2004). Konnex Association.
48. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual. Busch-Watchdog Sky KNX (2016). Busch-Jaeger Elektro GmbH, 648.
49. ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products (2016). ABB, 86. Available at: https://library.e.abb.com/public/d26bd890d3ef476fbc3a59a2fdca6116/Webinar%20ABB%20i-bus%20KNX%20-%20KNX%20Basics%20and%20Products.pdf
50. Manual for KNX Planning (2017). Siemens Switzerland Ltd, 100.
51. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation (2010). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 116.
52. Kottapalli, N. (2011). Diameter and LTE Evolved Packet System. Corporate Headquarters, 10. Available at: http://go.radisys.com/rs/radisys/images/paper-lte-diameter-eps.pdf
53. Ventura, H. (2002). Diameter - Next generation's AAA protocol. Institutionen för Systemteknik, 66. Available at: https://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf
54. Vinay Kumar, S. B., Harihar, M. N. (2012). Diameter-Based Protocol in the IP Multimedia Subsystem. International Journal of Soft Computing and Engineering (IJSCE), 1 (6), 266–269. Available at: https://www.ijsce.org/portfolio-item/F0320121611/
55. Qanbari, S., Mahdizadeh, S., Rahimzadeh, R., Behinaein, N., Dustdar, S. (2016). Diameter of Things (DoT): A Protocol for Real-Time Telemetry of IoT Applications. Lecture Notes in Computer Science, 207–222. doi: https://doi.org/10.1007/978-3-319-43177-2_14
56. Tschofenig, H. (2019). Diameter: new generation AAA protocol – design, practice, and applications. John Wiley & Sons, Inc. doi: https://doi.org/10.1002/9781118875889
57. Ugrozy bezopasnosti yadra paketnoy seti 4G (2017). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
58. Uyazvimosti protokola Diameter v setyakh 4G (2018). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
59. 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. doi: https://doi.org/10.15587/1729-4061.2021.233533
60. Yevseiev, S., Pohasii, S., Khvostenko, V. (2021). Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Information Processing Systems, 3 (166), 35–40. doi: https://doi.org/10.30748/soi.2021.166.03