UDC 681.32:007.5

DOI: 10.15587/1729-4061.2022.268368

DEVELOPMENT OF A METHOD FOR ENSURING CONFIDENTIALITY AND AUTHENTICITY IN WIRELESS CHANNELS

The object of the research is the development of a method for ensuring the authenticity and integrity of data in wireless channels based on post-quantum cryptosystems. The development of modern digital technologies ensures the transition to smart technologies and the formation of Next Generation Networks. The formation of smart technologies, as a rule, uses wireless communication channel standards IEEE 802.11X, IEEE 802.15.4, IEEE 802.16, which use only authentication protocols and privacy mechanisms, which are formed on symmetric algorithms. In the conditions of the post-quantum period (the advent of a full-scale quantum computer), the stability of such algorithms is questioned. Such systems, as a rule, are formed on the basis of the synthesis of socio-cyber-physical systems and cloud technologies, which simplifies the conduct of Advanced Persistent Threat attacks, both on the internal circuit of execution systems and on external control systems. The creation of multi-circuit information protection systems allows for an objective assessment of the current state of the system as a whole and the formation of preventive measures to counter cyber threats. The proposed method of providing basic security services: confidentiality, integrity and authenticity based on crypto-code constructions takes into account the level of secrecy of information transmitted over wireless channels and/or stored in databases of socio-cyber-physical systems. The use of post-quantum algorithms – McEliece/Niederreiter crypto-code constructions on elliptic/modified elliptic/lossy/Low-density parity-check code provides the necessary level of stability in the post-quantum crypto-period (crypto-stability at the level of 10^{25}–10^{35} group operations), speed and probability of information (Perr not lower than 10^{-9}–10^{-12}). The proposed method of information exchange using wireless communication channels ensures their practical implementation on resource-limited devices (creating of CCC on the GF field (2^4–2^6)

Keywords: crypto-code constructions of McEliece and Niederreiter, smart technologies, security concept, multi-contour protection systems

Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department*
E-mail: Serhii.Yevseiev@gmail.com

Roman Korolev
PhD, Associate Professor *

Mykhailo Koval
Doctor of military sciences, Head of the University***

Khazail Rzayev
PhD, Associate Professor
Department of Computer Technology and Cybersecurity
Azerbaijan Technical University
G. Javid ave., 25, Baku, Azerbaijan, AZ1073

Oleksandr Voitko
PhD, Deputy Head of Department
Department of Information Technology and Information Security
Institute of Troops (Forces) Support and Information Technologies***

Olena Akhiiezer
PhD, Professor, Head of Department
Department of Computer Mathematics and Data Analysis**

Alla Hrebeniuk
PhD, Senior Researcher
Scientific Laboratory
National Academy of the Security Service of Ukraine
Maksymovycha str., 22, Kyiv, Ukraine, 03022

Stanislav Milevskyi
PhD, Associate Professor *

Elnur Baghirov
Software Developer
Fogito Tech LLC
Babek ave., 11/31, Baku, Azerbaijan, AZ1025

Musa Mammadov
Senior Software Developer
Cybernet LLC
Khojaly ave., 5, Baku, Azerbaijan, AZ1025

*Department of Cyber Security**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049

Received date 15.09.2022
Accepted date 25.11.2022
Published date 30.12.2022

***How to Cite:** Yevseiev, S., Korolev, R., Koval, M., Rzayev, K., Voitko, O., Akhiiezer, O., Hrebeniuk, A., Milevskyi, S., Baghirov, E., Mammadov, M. (2022). Development of a method for ensuring confidentiality and authenticity in wireless channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (120)), 15–27. doi: https://doi.org/10.15587/1729-4061.2022.268368*

1. Introduction

The development of wireless technologies has significantly expanded the range of digital services based on integration, cyber-physical systems with LTE (Long-Term Evolution), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth technologies. Further development of this direction makes it possible to form smart-city digital services based on the synthesis of the Internet of things, mesh networks and smart technologies. The use of wireless communication channels can significantly increase the speed of information transfer and ensure the creation of socio-cyber-physical systems based on the of LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth standards. To provide security services in cyber-physical systems, as a rule, the KNX/EIB (European Installation Bus) standard (ISO/IEC 14543) is used based on the use of virtual private network channels (encryption AES-128, -256) [1–7]. The KNX standard in IP Secure mode allows to provide confidentiality and authenticity services based on the use of an additional mechanism (protective shell) that protects all KNX-net/IP data traffic [8]. KNX Data Secure mode uses a longer KNX frame format based on CCM (Code Block Chain Message Authentication Counter) with 128-bit AES block symmetric cipher encryption to ensure information integrity. However, the security mechanisms of the KNX standard (ISO/IEC 14543) do not provide protection against IP networks channel monitoring, which allows an attacker based on a false server to intercept the traffic of the information flow. In addition, according to experts from the National Institute of Standards and Technology (NIST) of the United States, the use of symmetric algorithms with a key length of 128 bits does not provide the required level of security in the post-quantum period [9–11].

In the wireless channels of LTE technologies, only the 3A authentication service (AAA – authentication, authorization, accounting) is provided based on the Diameter protocol [12–16]. The Diameter protocol has a predefined set of common AVPs (Attribute-Value-Pair) between two Diameter nodes, allowing various combinations of the protocol to be used.

However, the absence of security mechanisms in wireless channels of mobile technologies does not allow confidentiality and integrity services to be provided. 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 [17, 18]. In addition, an attacker can forcibly transfer the subscriber's device to 3G mode (third generation) – and carry out further attacks on the less secure SS7 system (signaling system, Signaling System No. 7) [18]. Table 1 shows the main characteristics of wireless mobile and computer networks and security services based on the KNX standard and the Diameter protocol.

Analysis of the Table 1 shows that in the context of the emergence of a full-scale quantum computer, hybridity and synergy of cyber-attacks, wireless channels partially provide privacy services, which requires new approaches to security based on post-quantum mechanisms.

Thus, a new concept of the security of systems formed on the basis of the synthesis of cyber-physical systems (CPS) and social networks – socio-cyber-physical systems (SCPS) is needed. Such systems are rapidly developing based on smart and Internet-of-things technologies and require a new approach to providing security services for wireless channels based on post-quantum cryptosystems.

Table 1

Wireless Network Specifications Table

Technology	Transmission/ reception range, m	V, bps	topology	Transmission spectrum	Modulation	Security services									
						before PQ					in PQ				
						C	I	A	A_u	B	C	I	A	A_u	B
LTE (4G)	up to 13400	up to 100 Mbps	AIPN	600 MHz до 2,5 GHz	64QAM	–	–	+	+	–	–	–	–	–/+	–
LTE (5G)	500	20 Gbps	Heterogeneous core network	from 30 GHz to 300 GHz	256-QAM	–	–	+	+	–	–	–	–	–/+	–
IEEE 802.11 ac (WiFi 5)	500	up to 7 Gbps	P2MP	5 GHz	256-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.11ax, Wi-Fi 6	–	9607 Mbps	P2MP	5 GHz	1024-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16	5000	32 Mbps 134 Mbps	mesh	10–66 GHz	64QAM O-QPSK	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16m (WiMAX2)	6000	90 Mbps 179 Mbps	mesh	11 GHz	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.1 Bluetooth 5	200	2–6 Mbps	mesh	2,4–2,485 GHz	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.4	1000	250 kbps	P2P Cluster tree	2,4–2,483 GHz	BPSK O-QPSK	+	+	+	+	–	–	–	–	–/+	–

Note: C – confidentiality; I – integrity; A – availability; Au – authenticity, B – involvement; AIPN – All IP Network, P2MP – point-to-multipoint, P2P – peer-to-peer, QAM – Quadrature Amplitude Modulation, O-QPSK – quadrature phase shift keying, BPSK – binary phase shift keying

2. Literature data analysis and problem statement

To provide security services and expand the range of digital services based on smart technologies, various approaches are proposed, based on classical symmetric and asymmetric mechanisms, and blockchain technologies. Thus, in [19] an analysis of threats to cyber-physical systems is carried out, and it is also proposed to use the modeling of information protection systems (IPS). Based on the business process models notation (BPMN), it is intuitively possible to describe various approaches to building information security systems. The proposed concept of building security systems allows taking into account the physical components of the CPS, as well as the control flows of the control system to the physical elements of the CPS. However, this does not take into account the actual separation of the physical and control subsystems of the CPS, which does not allow to objectively take into account the current state of security of the system as a whole. In [20], modeling approaches based on a multi-domain language for component-oriented modeling of CPS Modelica are proposed. This approach accurately captures the interaction between the physical and cyber components within the CPS. However, such models do not take into account the need to build multicontour information security systems. With this approach, the inner and outer contours provide not only an objective assessment of the current state of the system, but also allow to form the necessary tuple of IPS elements to provide security services. In [21], the authors proposed an authentication protocol, which, in their opinion, provides the required indicators of reliability and security and can be used in 5G technology. The proposed authentication approach is based on the use of smart cards for authentication using elliptic curve random number generators. However, the use of firmware authentication is subject to scream attacks and does not provide confidentiality and integrity services over wireless communication channels. To ensure the security of key data transmission, [22] presents a protocol based on an improved multi-server key agreement scheme with hash-based authentication and a standalone registration server (standalone RS). This approach ensures the use of a closed channel for the transmission of key data, but does not provide confidentiality and data integrity services. The work [23] presents an analysis of threats on CPS, as well as an analysis of the use of OTP passwords in various authentication schemes. However, it is proposed to use protocols and mechanisms to ensure the authenticity and integrity of classical computer networks as countermeasures for threats. This approach does not take into account the multicontour architecture of CPS, as well as the hybridity and synergy of APT attacks. The paper [24] presents an analysis of the 2-pass authentication and key agreement (AKA) protocol for 5G mobile communications (5G-AKA), which provides data confidentiality and authenticity based on the use of the A5 stream cipher [25, 26]. The scheme of two-factor authentication and key agreement (AKA) for 5G mobile communications is analyzed. 5G-AKA has been proven to be vulnerable to Linkability of AKA Failure Messages (LFM) attacks, which does not allow for confidentiality. A modification of the AKA scheme is proposed, however, the use of a stream cipher for confidentiality will not allow providing the required level of security in the post-quantum period, taking into account the proposals in [27]. In [28, 29], it is proposed to use post-quantum algorithms for providing security services – crypto-code constructs (CCC) McEliece and Niederreiter on algebrogeometric codes. The papers [29, 30] present practical ways to reduce energy and computational costs, which makes it possible to use wireless CCC channels in the information security system to provide the required level of security services.

Thus, the analysis showed that the rapid growth of computing resources and mobile technologies determined the development vector of wireless channels of systems based on smart technologies. This approach makes it possible to integrate and form both CPS and SCPS, which significantly expands the range of digital services. Expanding the range of capabilities of wireless technologies makes it possible to form a smart-city system with functionality in various areas, on the one hand, on the other hand, the inability to resist APT attacks in the context of the emergence of a full-scale quantum computer significantly reduces the security level of such systems [31]. The lack of mechanisms for ensuring confidentiality and integrity services in 4G-6G technologies does not allow for their widespread implementation in the Next Generation Network and smart systems. A promising direction in the construction of IPS is the use of post-quantum algorithms – CCC on algebrogeometric codes and the formation of multicontour IPS.

3. The aim and objectives of the study

The aim of the study is to develop a method for ensuring confidentiality and authenticity in wireless channels. This approach will make it possible to form a dual-contour security system based on mobile and Internet technologies using wireless channels, and provide security services based on post-quantum algorithms.

To achieve the aim of the study, it is necessary to solve the following objectives:

– to develop the conceptual foundations of the CPS dual-contour security system based on post-quantum algorithms;

– to develop a mathematical model of a method for ensuring confidentiality and authenticity in wireless channels;

– to develop an algorithm for the practical implementation of confidentiality and authenticity in wireless channels.

4. Research materials and methods

The object of research is the process of providing security services in wireless channels, which makes it possible to ensure the construction of multicontour security systems in the conditions of the post-quantum period.

The provision of security services in wireless channels is associated with a contradiction between the speed indicators of wireless channels and the need to use cryptographic algorithms to provide confidentiality and integrity services. In addition, in the post-quantum cryptoperiod, the requirements for symmetric cryptography algorithms increase significantly, which casts doubt on the possibility of providing a compromise between the amount of key data and the amount of memory of switching devices. Also, the possibility of offline encryption of various information flows based on symmetric cryptography.

To provide security services, it is proposed to use post-quantum algorithms – crypto-code constructions of McEliece and Niederreiter on algebrogeometric codes [28, 29, 31]. Both crypto-code constructions are based on the principle of using the theory of error-correcting coding and the orthogonality of the matrices G, the generating matrix of the linear code, and H, the check matrix of the linear code. Taking into account the orthogonality of matrices G and H ($G\times H^T=0$), these cryptosystems have almost the same energy costs for encryption.

Concealment matrices are used as a key sequence in both crypto-code constructions:

– X – masking nondegenerate randomly equiprobable $k\times k$ matrix formed by the source of keys with elements from $GF(q)$;

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

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

– G – $k\times n$ generating matrix (McEliece CCC);

– H – check matrix with dimension $r\times n$. In addition, a distinctive feature of Niederreiter's *CCC* is the preliminary use of equilibrium coding, which makes it possible to provide a practically relative coding rate equal to one.

Table 2 shows the main characteristics of elliptic (EC) modified elliptic (MEC) codes. Notations: $GF(q)$ – *Galois* finite field, X – smooth projective algebraic curve in a projective space P^n over $GF(q)$, $g=g(X)$ – kind of curve, $X(GF(q))$ – the set of its points over a finite field, $N=X(GF(q))$ – their number. C – divisor class on X power $\alpha>g-1$, C defines the mapping $\varphi:X\to P^{k-1}$, where $k\geq\alpha-g+1$. The set $y_i=\varphi(x_i)$ specifies the code. Number of points in intersection $\varphi(X)$ with the hyperplane is equal to α, i. e. $n-d\leq\alpha$. This construction allows building codes with parameters $k+d\geq n-g+1$, length n of which is less than or equal to the number of points on the curve X.

Table 2

EC, MEC main characteristics (*n*, k, d)

(*n*, k, d) parameters of the code that is built through of the view $\varphi:X\to P^{k-1}$	$n=2\sqrt{q}+q+1$, $k\geq\alpha$, $d\geq n-\alpha$, $\alpha=3\times degF$, $k+d\geq n$	
(*n*, k, d) parameters of the code that is built through of the view $\varphi:X\to P^{r-1}$	$n=2\sqrt{q}+q+1$, $k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times degF$, $k+d\geq n$	
Characteristics	Shortened MEC	Extended MEC
(*n*, k, d) parameters of the code that is built through mapping of the view $\varphi:X\to P^{k-1}$	$n=2\sqrt{q}+q+1-x$, $k\geq\alpha-x$, $d\geq n-\alpha$, $\alpha=3\times degF$, $k+d\geq n$	$n=2\sqrt{q}+q+1-x+x_1$, $k\geq\alpha-x+x_1$, $d\geq n-\alpha$, $\alpha=3\times degF$
(*n*, k, d) parameters of the code that is built through of the view $\varphi:X\to P^{r-1}$	$n=2\sqrt{q}+q+1-x$, $k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times degF$, $k+d\geq n$	$n=2\sqrt{q}+q+1-x+x_1$, $k\geq n-\alpha$, $d\geq\alpha$, $\alpha=3\times degF$

Table 3 shows the main parameters of the McEliece cryptosystem.

The paper [31] presents the results of studies of the energy consumption of crypto transformations and cryptographic strength. The obtained results confirm the possibility of practical implementation and use of post-quantum algorithms (McEliece and Niederreiter CCC) in wireless channels in offline mode.

Table 3

The main parameters of McEliece's CCC on EC, MEC

Parameter		CCC EC
private key size		$l_{K+}=n^2\times k^2\times m$
information vector size		$l_I=k\times m$
cryptogram dimension		$l_s=n\times m$
relative transfer rate		$R=l_I/l_s={}^{k\times m}\!/_{n\times m}$
Parameter	CCC on shortened MEC	CCC on extended MEC
private key size	$l_{K+}=x\times\left\lceil\log_2\left(2\sqrt{q}+q+1\right)\right\rceil$	$l_{K+}=(x-x_1)\times\log_2\left(2\sqrt{q}+q+1\right)$
information vector size	$l_I=(\alpha-x)\times m$	$l_I=(\alpha-x+x_1)\times m$
cryptogram dimension	$l_S=\left(2\sqrt{q}+q+1-x\right)\times m$	$l_S=\left(2\sqrt{q}+q+1-x+x_1\right)\times m$
relative transfer rate	$R=(\alpha-x)/\left(2\sqrt{q}+q+1-x\right)$	$R=(\alpha-x+x_1)/\left(2\sqrt{q}+q+1-x+x_1\right)$

5. Results of the development of a method for ensuring confidentiality and authenticity in wireless channels

5. 1. Development of the conceptual foundations of the two-contour CPS security system based on post-quantum algorithms

When developing the conceptual foundations of the two-contour CPS security system based on post-quantum algorithms, the approach proposed in [31] was used. It is based on the concept of double-contour security based on crypto-code constructions. At the same time, it is proposed to use integrated solutions for the use of certain codes in crypto-code systems based on the gradation of the information secrecy degree in socio-cyber-physical systems. Table 4 shows the ratio of time and the degree of information secrecy.

Table 4

The ratio of time and the degree of information secrecy

The degree of information secrecy	Time	Suggested codes for *CCC*
critical	up to 1 year	*MEC*, flawed codes
high	up to 1 month	*MEC*
medium	up to 1 hour	*EC*
low	up to 10 minutes	*EC*
very low	up to 1 minute	LDPC

Fig. 1 shows a block diagram of the conceptual foundations of a dual-contour security system. For a formal description of the Concept, the approach in [31] will be used: to ensure the security of the entire protection system, it is necessary to take into account the threats of the internal and external contours for each of the platforms:

1) threats of the internal contour, taking into account the hybridity and synergy of threats for the CPS platform:

$$W^{CPS\ ISL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CPS platform}}} = \\ = W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{C} \bigcap W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{I} \bigcap W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{Au}, \tag{1}$$

where $W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{C}$ – synergy of threats on privacy service, $W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{I}$ – synergy of threats on integrity service, $W^{CPS\ ISL}_{synerg_{\text{CPS platform}}}{}^{Au}$ – synergy of threats on authenticity service;

2) threats of the internal contour, taking into account the hybridity and synergy of threats for the cyberspace platform (CbS):

$$W^{CbS\ ISL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CbS platform}}} = \\ = W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{C} \bigcap W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{I} \bigcap W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{Au}, \tag{2}$$

where $W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{C}$ – synergy of threats on privacy service, $W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{I}$ – synergy of threats on integrity service, $W^{CbS\ ISL}_{synerg_{\text{CbS platform}}}{}^{Au}$ – synergy of threats on authenticity service.

Overall threat assessment of the inner loop, taking into account CPS technologies:

$$W^{CPS}_{ISL} = W^{CPS\ ISL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CPSplatform}}} \bigcup W^{CbS\ ISL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CbSplatform}}}. \tag{3}$$

General assessment of threats of the internal contour, taking into account the form of ownership of the elements and technologies of the cyber-physical system (Fig. 1):

$$W^{CPS}_{ISL_{\text{general}}} = W^{CPS}_{ISL_{\text{private.}}} \bigcup W^{CPS}_{ISL_{\text{state}}} \bigcup W^{CPS}_{ISL_{\text{corporativ}}}, \tag{4}$$

$W^{CPS}_{ISL_{\text{private.}}}$ – overall assessment of internal contour threats to the personal property system;

$W^{CPS}_{ISL_{\text{state}}}$ – overall assessment of threats of the internal contour for the state property system;

$W^{CPS}_{ISL_{\text{corporativ}}}$ – overall assessment of internal contour threats to the corporate property system;

3) threats of the external contour, taking into account the hybridity and synergy of threats for the CPS platform:

$$W^{CPS\ ESL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CPS platform}}} = \\ = W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{C} \bigcap W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{I} \bigcap W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{Au}, \tag{5}$$

where $W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{C}$ – synergy of threats on privacy service,

$W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{I}$ – synergy of threats on integrity service,

$W^{CPS\ ESL}_{synerg_{\text{CPS platform}}}{}^{Au}$ – synergy of threats on authenticity service;

4) threats of the external contour, taking into account the hybridity and synergy of threats for the cyberspace platform (CbS):

$$W^{CbS\ ESL}_{\text{hybrid}\ C,I,Au\ synerg_{\text{CbS platform}}} = \\ = W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{C} \bigcap W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{I} \bigcap W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{Au}, \tag{6}$$

where $W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{C}$ – synergy of threats on privacy service, $W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{I}$ – synergy of threats on integrity service, $W^{CbS\ ESL}_{synerg_{\text{CbS platform}}}{}^{Au}$ – synergy of threats on authenticity service.

General assessment of threats of the external contour, taking into account CPS technologies:

$$W^{CPS}_{ESL} = W^{CPS\ ESL}_{\text{hydrid}\ C,I,Au\ synerg_{CPS_{\text{platform}}}} \bigcup W^{CbS\ ESL}_{\text{hydrid}\ C,I,Au\ synerg_{CbS_{\text{platform}}}}. \tag{7}$$

Overall assessment of threats of the internal contour, taking into account the form of ownership of the elements and technologies of the cyber-physical system (Fig. 1):

$$W^{CPS}_{ESL_{\text{general}}} = W^{CPS}_{ESL_{\text{private.}}} \bigcup W^{CPS}_{ESL_{\text{state}}} \bigcup W^{CPS}_{ESL_{\text{corporativ}}}, \tag{8}$$

$W^{CPS}_{ESL_{\text{private.}}}$ – overall assessment of internal contour threats to the personal property system; $W^{CPS}_{ESL_{\text{state}}}$ – overall assessment of threats of the internal contour for the state property system; $W^{CPS}_{ESL_{\text{corporativ}}}$ – overall assessment of internal contour threats to the corporate property system.

Based on expressions (3), (7), an assessment of threats in cyber-physical systems in the internal and external CPS security contours is formed, and on the basis of expressions (4), (8) – taking into account forms of ownership (separately). To provide a generalized assessment of a multicontour security system, the formula was used:

$$W^{CPS}_{\text{final}} = W^{CPS}_{ISL_{\text{general}}} \bigcup W^{CPS}_{ESL_{\text{general}}}. \tag{9}$$

Required information resource security services $I_{A_i} \in \{I_A\}$ can be described by a tuple $I_{A_i} = \left(Type_i, A_i^C, A_i^I, A_i^{Au}, \beta_i\right)$. T*ype$_i$* – information asset type, described by a set of basic values: T*ype$_i$*={*CI$_i$*, *PD$_i$*, *CD$_i$*, *TS$_i$*, *StR$_i$*, *PubI$_i$*, *ContI$_i$*, *PI$_i$*}, where C*I$_i$* – confidential information, *PD$_i$* – payment documents, *CD$_i$* – loan documents, *TS$_i$* – commercial secret, *StR$_i$* – statistical reports, *PubI$_i$* – public information, *ContI$_i$* – control information, *PI$_i$* – personal data, β_i – a metric of the ratio of time and degree of information confidentiality 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 cyber-physical systems based on wireless mobile technologies is described by the expression:

– for additive convolution:

$$L_{W^{CPS}_{\text{security}}} = L_{ISL} \sum_{j=1}^{2} \sum_{i=1}^{8} \left(I_{A_{ij}} \times \beta_{ij} \right) + L_{ESL} \sum_{j=1}^{2} \sum_{i=1}^{8} \left(I_{A_{ij}} \times \beta_{ij} \right); \tag{10}$$

– for multiplicative convolution:

$$L_{W^{CPSS}_{\text{security}}} = 1 - \left[1 - L_{ISL} \sum_{j=1}^{2} \sum_{i=1}^{8} \left(I_{A_{ij}} \times \beta_{ij} \right) \right] \times \\ \times \left[1 - L_{ESL} \sum_{j=1}^{2} \sum_{i=1}^{8} \left(I_{A_{ij}} \times \beta_{ij} \right) \right]. \tag{13}$$

Such an approach will allow to provide the required level of security in a timely manner, taking into account the degree of information secrecy and/or the security time that is necessary to provide confidentiality, integrity and authenticity services. To ensure the required security level, it is possible to combine various codes and CCC, both McEliece and Niederreiter.

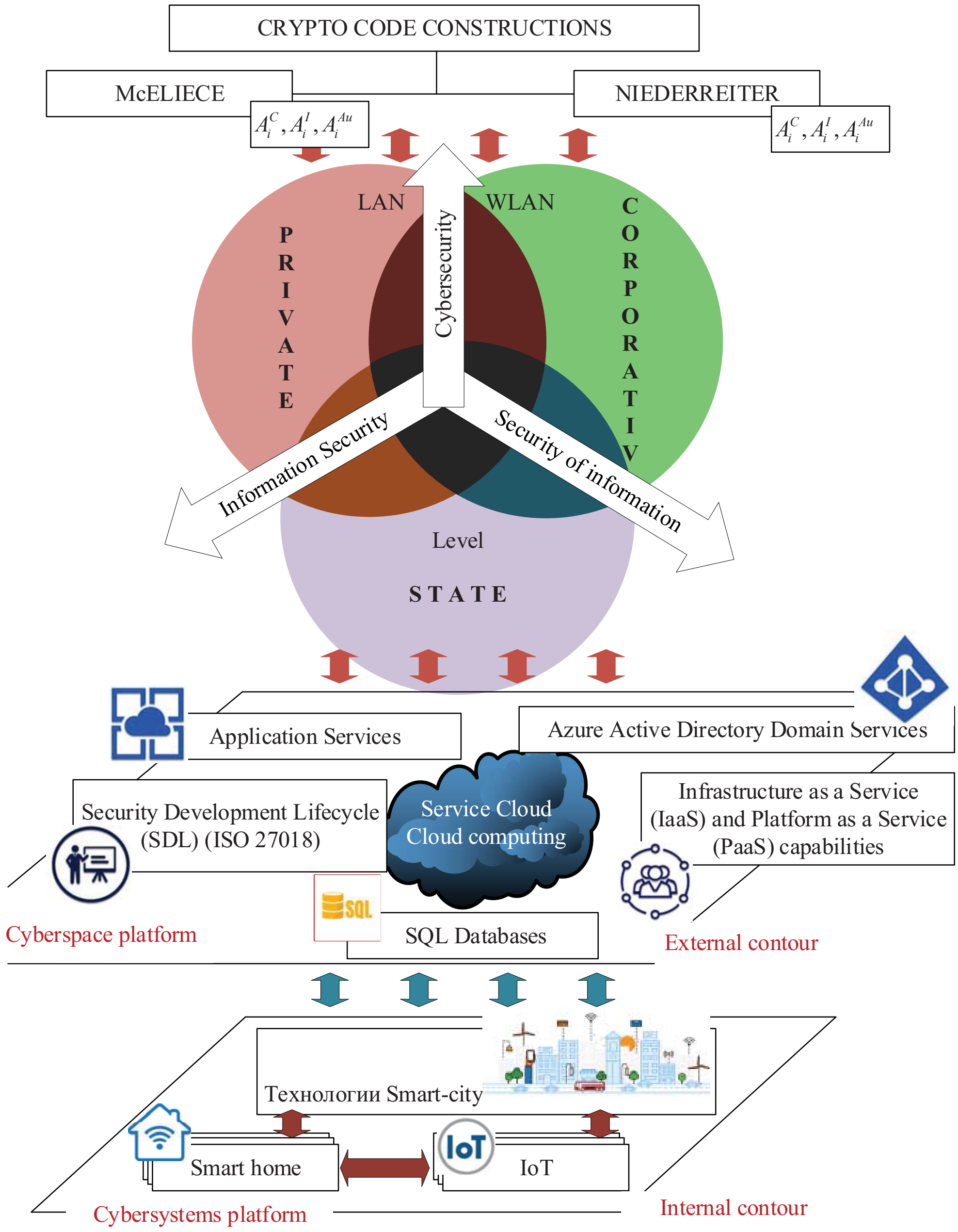

Fig. 1. Structural diagram of the conceptual foundations of a double-contour security system

5. 2. Development of a mathematical model of a method for ensuring confidentiality and authenticity in wireless channels

The formation of a method for ensuring the confidentiality and authenticity of information based on a two-contour security system is proposed to be implemented at the CCC. The use of various error-correcting codes, defective and LDPC codes in McEliece and Niederreiter CCC allows to form various combinations, taking into account the level of secrecy (confidentiality), as well as the required time of information cryptographic strength. Fig. 2 shows a block diagram of the proposed approach. The main elements of the internal contour are various physical control devices (sensors, counters, tracking sensors, video cameras, etc.), as well as the server for dispatching and controlling the physical mechanisms of the CPS. The elements of the outer contour include a server for generating key sequences and storing long-term keys, as well as mobile applications (if necessary) for CPS users.

To provide security services, it is proposed to install McEliece CCC software and hardware encoders on the elements of the internal contour. In this case, on the basis of complexing and the level of circulating information secrecy, various noise-immune codes are established and used. The dependence of time and the degree of information secrecy is given in Table 4.

The relationship between the internal and external contours of the security system on the basis of the proposed method is provided by Niederreiter CCC, the relative coding rate is close to 1. At the same time, the use of two CCCs increases the security level by at least 2 times, and the use of various error-correcting codes integrated provides an increase in the error reliability. Long-term keys are formed in the external contour, the use of which allows to reset the CPS security system (in case of loss of gadgets control, compromise, etc.). As well as the formation of private keys for use in the CPS in the internal contour. To ensure security, long-term keys are stored in encrypted form by McEliece or Niederreiter CCC.

This approach ensures the closure of all channels of information transmission both in the internal contour – the cyber-physical system, and in the external contour, as well as communication channels between the contours. In this case, post-quantum cryptosystems are used, which makes it possible to use this approach with the prospect of a full-scale quantum computer.

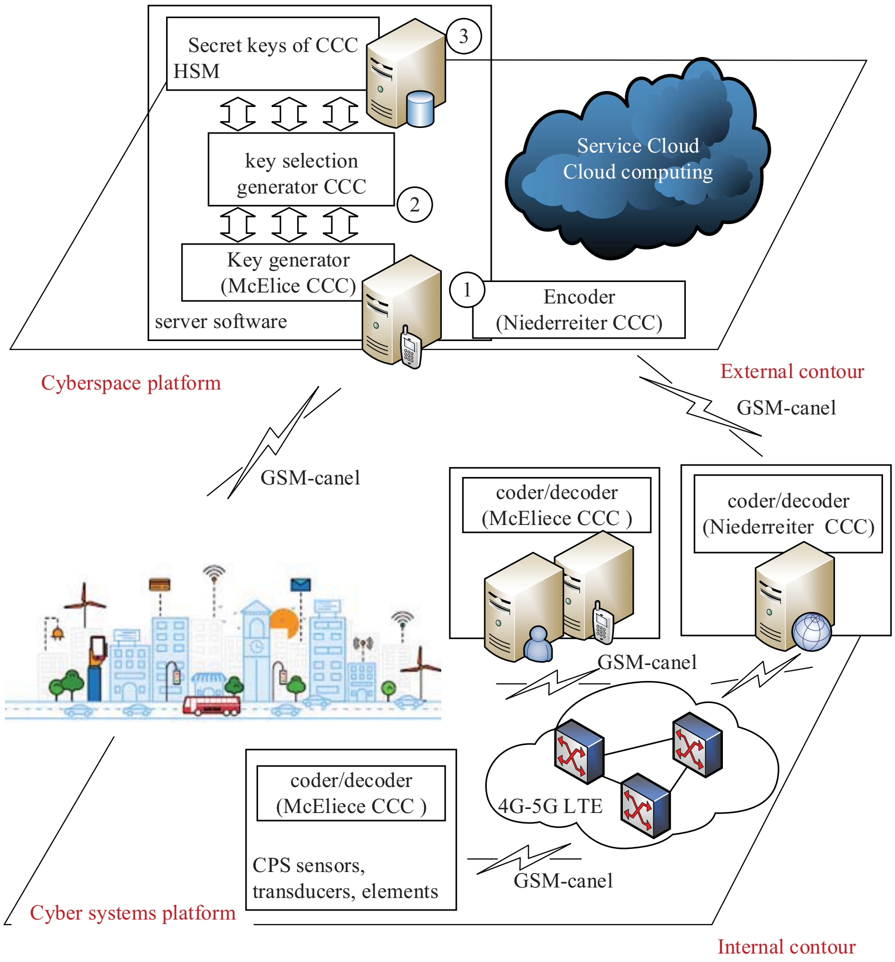

Fig. 2. Structural diagram of the formation of a method for ensuring confidentiality and data integrity

To form a mathematical model of the method for ensuring confidentiality and authenticity in wireless channels, the approaches of the works [29–31] will be used.

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

– set of open texts for McEliece CCC $M=\left\{M_1,M_{2,}\ldots M_{q^k}\right\}$, where $M_i=\{I_0,I_{h_1},\ldots I_{h_j},I_{k\text{-}1}\},\forall I_i\in GF(q)$, h_j – information characters equal to zero, $|h|=\frac{1}{2}k$, i. e. $I_i=0$, $\forall I_i\in h$; for Niederreiter CCC $M_i=\left\{e_0,e_{h_1,}\ldots e_{h_k},e_{e-1}\right\}$, $\forall e_e\in GF(q)$, h_e – error vector characters that are equal to zero, $|h|=\frac{1}{2}e$, that is $e_i=0$, $\forall e_i\in h$. Based on the equilibrium coding algorithm, the plaintext is converted into an error vector;

– set of closed texts (codegrams) for McEliece CCC

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

where $C_i=(c^*_{X_0},c^*_{h_1},\ldots,c^*_{h_j},c^*_{X_{n-1}})$, $\forall c^*_{X_j}\in GF(q)$; for Niederreiter CCC $S=\left\{S_0,S_1,\ldots S_{q^r}\right\}$, where $S_i=\left\{S^*_{X_0},S^*_{h_1},\ldots S^*_{h_j},S^*_{X_r}\right\}$, $\forall S_{X_r}\in GF(q)$;

– a set of direct mappings (based on the use of a public key – generating/checking matrix of error-correcting codes (error-correcting code – *ECC*) (algebrogeometric codes: *EC*, *MEC*; *LDPC*; flawed codes):

1) for McEliece CCC

$$\phi=(\phi_1, \phi_2, \ldots, \phi_s),$$

where $\phi_i : M\rightarrow C_{k-h_j}$, $i=1, 2,\ldots, s$;

2) for Niederreiter CCC

$$\varphi=(\varphi_1, \varphi_2, \ldots, \varphi_r),$$

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

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

1) for McEliece CCC

$$\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},\ldots,\phi_s^{-1}\},$$

where $\phi_i^{-1} : C_{k-h_j}\rightarrow M$, $i=1,2,\ldots,s$;

2) for Niederreiter CCC

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

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

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

1) for McEliece CCC

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

where $G_{X_{a_i}}^{LDPC_i}$ – generating $n\times k$ matrix disguised as a random code. The matrix is determined from the orthogonality of the generator and check matrices;

2) for Niederreiter CCC – $KU_i=\{KU_1, KU_2, \ldots, KU_r\}=\{H_1, H_2, \ldots, H_r\}$, where $H_{X_{a_i}}^{ECC_i}$ – erification $(N-K)\times N$ matrix determines $(N-K)$ checking symbols $P_1, P_2, \ldots, P_{N\text{-}K}$ as a linear combination of information symbols d_k, $k=1, 2, \ldots, K$;

– set of personal (private) keys of users:

$$KR=\left\{KR_1,KR_2,\ldots,KR_r\right\}=\left\{\begin{matrix}\{X,P,D\}_1, & \\ \{X\ P\ D\}_2 & \{X\ P\ D\}_r\end{matrix}\right\},$$

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

where X^i – masking non-degenerate randomly equally probable generated by the key source $k\times k$ matrix with elements from $GF(q)$; P^i – permutable randomly equiprobably formed by the source of the keys $n\times n$ matrix with elements from $GF(q)$; D^i – diagonal formed by the source of the keys $n\times n$ matrix 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/checking matrices:

– forMcElieceCCC– $G_{X_{a_i}}^{ECCu} = X^u \times G^{ECCu} \times P^u, u \in \{1,2,...,s\};$

– for Niederreiter – $H_{X_{a_i}}^{ECCu} = X^u \times H^{ECCu} \times P^u, u \in \{1,2,...,r\}.$

The communication channel receives:

– for McEliece CCC – codeword: $C_j = M_i \times G_{X_{a_i}}^{ECCu^T} + e,$ where e – additional session key of each information package;

– for Niederreiter CCC – syndromic sequence:

$$S^* = (e_n) \times H_{X_{a_i}}^{ECC^T}.$$

On the receiving side, an authorized user who knows the concealment matrices uses a fast decoding algorithm:

– for McEliece CCC:

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

To recover the plaintext, the authorized user adds null information characters $C_j^* = C_j + C_{k-h_j},$ from the restored private text C_j removes the action of the secret permutation and diagonal matrices P^u and D^u.

$$C \ = C_j^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \left(M_i \times \left(G_{X_{a_i}}^{ECCu}\right)^T + e \right) \times$$

$$\times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = \left(M_i \times \begin{pmatrix} X^u \times G_{X_{a_i}}^{ECCu} \times \\ \times P^u \times D^u \end{pmatrix}^T + e \right) \times$$

$$\times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} = M_i \times \left(X^u\right)^T \times \left(G_{X_{a_i}}^{ECCu}\right)^T \times \left(P^u\right)^T \times$$

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

$$= M_i \times \left(X^u\right)^T \times \left(G_{X_{a_i}}^{ECCu}\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$$

decodes the resulting vector using the Berlekamp-Massey algorithm [32]:

$$C = M_i \times \left(X^u\right)^T \times \left(G_{X_{a_i}}^{ECCu}\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$$

i. e., gets rid of the second term and the factor $\left(G_{X_{a_i}}^{ECCu}\right)^T$ in the first term on the right side of the equality, after which it removes the effect of the masking matrix X^u. To do this, the result of decoding $M_i \times (X^u)^T$ should be multiplied by $(X^u)^{-1}$: $(M_i \times (X^u))^T \times (X^u)^-1 = M_i$. The resulting solution is the essence of plain text M_i;

– for Niederreiter CCC.

Next, an authorized user, using a set of matrices $\{X,P,D\}_\mathrm{u} = \{X^u, P^u, D^u\}$ formsavextor: $\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1},$ thus unmasks the code sequence $c_{X_i}^*$.

After substitution, getting the equality:

$$\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} =$$

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

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

An authorized user who has generated a vector has the ability to apply a fast (polynomial complexity) noise-correcting decoding algorithm and thus generate a vector $\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}$ and vector $M_i^u = M_i \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}$.

To restore the information equilibrium sequence M_i it is enough again to multiply vector M_i^u by masking matrices P^u and D^u, in reverse sequence:

$$M_i \ \aleph\aleph M_i^u \aleph\ \aleph P^u \quad D^u \quad M_i \quad \left(D^u\right)^{-1} \quad \left(P^u\right)^{-1} \quad P^u \quad D^u \quad M_i.$$

Thus, the presented mathematical model makes it possible to use McEliece and Niederreiter CCC to provide confidentiality, integrity, and authenticity services and to practically implement the proposed method. Fig. 3 presents the main elements of the proposed method for providing basic security services in cyber-physical systems based on wireless communication channels.

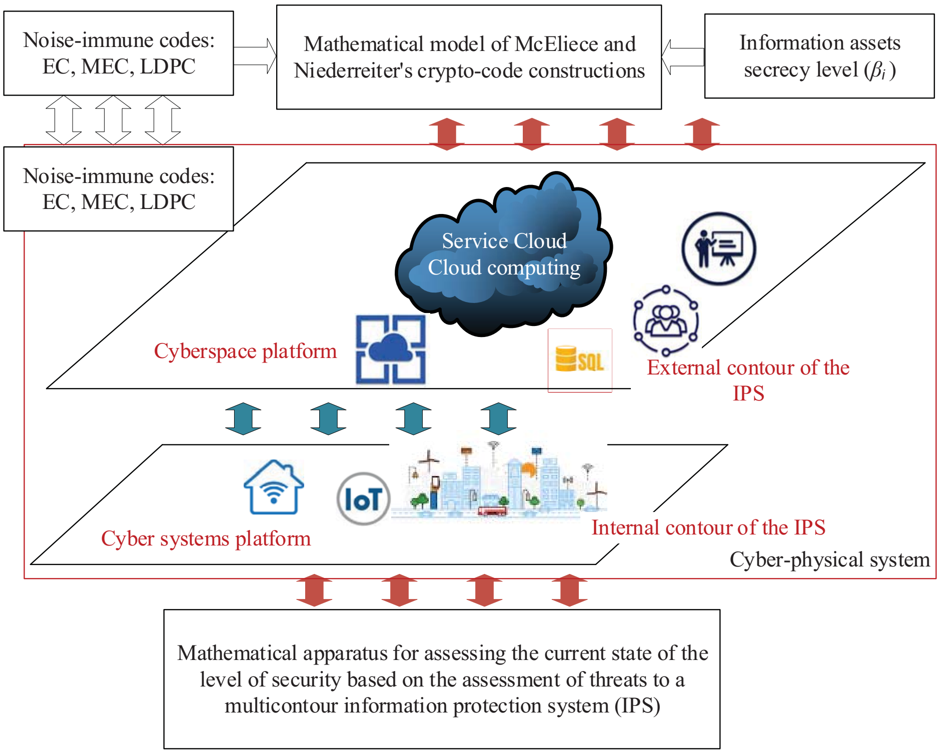
Noise-immune codes: EC, MEC, LDPC
Mathematical model of McEliece and Niederreiter's crypto-code constructions
Information assets secrecy level (β_i)
Noise-immune codes: EC, MEC, LDPC
Service Cloud
Cloud computing
Cyberspace platform
SQL
External contour of the IPS
IoT
Cyber systems platform
Internal contour of the IPS
Cyber-physical system
Mathematical apparatus for assessing the current state of the level of security based on the assessment of threats to a multicontour information protection system (IPS)

Fig. 3. Block diagram of the proposed method for providing security services in wireless channels based on crypto-code constructions

The main difference from the known approaches is, while maintaining the level of bandwidth of the wireless channel, to provide the required level of security (cryptostrength) of the channel in an integrated way (cryptosecurity based on post-quantum algorithms at the level of 10^{25}–10^{35} group operations), (P_{err} not less than 10^{-9}–10^{-12}) [31].

The use of post-quantum algorithms – crypto-code structures on the MEC allows the formation of cryptosystems over the field GF (2^6), and when using defective codes, the formation of hybrid cryptosystems over the field GF (2^4), which allows their practical implementation on resource-limited chipsets. The conducted experimental studies have shown that the use of CCC in cyber-physical systems based on wireless channels requires the presence of a mobile Internet channel (broadband channel). This limitation is based on the existing multi-contour CPS model, where, as a rule, the control system is deployed in cloud technologies.

Thus, the proposed model for the use of McEliece and Niederreiter CCC is the basic component of the proposed method for the formation of cryptosystems to provide basic security services. Such an approach, taking into account the multi-contour CPS and an objective assessment of the current state of security, makes it possible to form a reliable information protection system in the post-quantum period, taking into account possible APT attacks with signs of hybridity and synergy.

5. 3. Development of an algorithm for the practical implementation of confidentiality and authenticity in wireless channels

One of the variants of the proposed method for ensuring confidentiality and authenticity in outbred channels is the use of command transmission security based on two-way communication channels. For example, the connection between the key fob and the car's on-board computer. To form a "dialogue coding" that requires a two-way communication channel (the presence of a receiver and a transmitter, both in the main module and in the key fob), let's use McEliece CCC. In this case, the internal security contour is formed on the basis of encryption of the key fob authentication information package and information packages for the execution of various commands (unlocking the car, opening the driver's door, opening the trunk, etc.). The external contour (cyberspace platform) stores a long-term secret key that allows to reset the key sequences of the CCC and, at the request of the user, generates private keys and public keys of the CCC.

To ensure the service of authenticity – the authenticity of sending a command from the key fob of an authorized user, it is proposed to use a random number that is generated at each "appearance" by the on-board computer of the car, it generates a random number (session key) with a length of 76 bits.

As a pseudo-random number generator of length 76, it is proposed to use a pseudo-random number generator based on a linear recurrent feedback shift register (LFSR) modulo an irreducible polynomial of 76 degrees. These pseudo-random number generators generate sequences of the maximum period and are easily implemented both in hardware and software [33]. The general structural diagram of the LFSR is shown in Fig. 4.

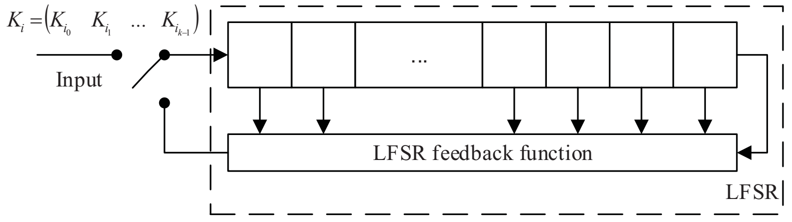

Fig. 4. General block diagram of a recurrent shift register with feedback

LFSR during the first k time counts, the key (switch) is in the upper position, and the shift register is filled with the key sequence $K_i=(K_{i0}, K_{i1}, ..., K_{ik-1})$. During the following q^k-1 time readings, the key (switch) is in the lower position and the values stored in the cells of the shift register are fed to the output of the device. At each time interval, it is in the lower position and the values stored in the cells of the shift register are fed to the output of the device. At each time interval, the information stored in the shift register moves one cell to the right, and the value stored in the rightmost cell is fed through the LRFSR feedback loop. The feedback function specifies a specific type of feedback circuit switching and ensures the formation of a pseudo-random sequence of the maximum period.

The resulting number of 76 bits is converted into an information sequence $I_{1\times19}$ with elements from the field GF (2^4), due to the use of multiplexers according to the scheme presented in Fig. 5.

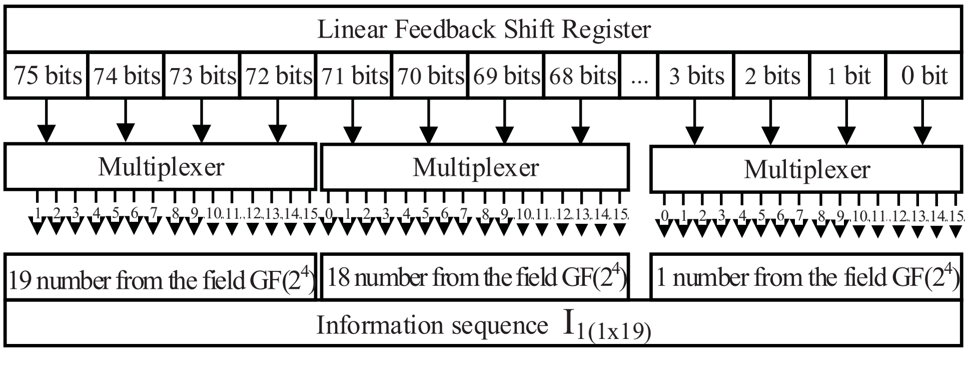

Fig. 5. Scheme for converting a random number into an information sequence $I_{1\times19}$ with elements from the field GF (2^4)

Let's consider the algorithm for ensuring the authenticity and confidentiality of the formation of "dialogue coding" based on McEliece CCC:

Car key fob software:

1. Sends a request to execute a command.
2. Receive over an open channel $I_{2(1\times19)}$.
3. Removing masking matrices and receiving $I_{1\times19}$:

$$I_{1(1\times19)}=I_{2(1\times19)} \times P^{-1}{}_{1(1\times19)}\times D^{-1}{}_{1(1\times19)}.$$

4. Generation of an additional session key – *e* (error vector) – corresponding to some action) (number from 0 to 24). To form the error location, it is proposed to transform the sequence $I_{1\times19}$ into a binary sequence and take the corresponding number in decimal number modulo 25.

5. Formation of a cryptogram. To do this, it is proposed to use the CCC on *EC* (*MEC*) (25,19,3)-code:

$$c_{1(1\times19)} = I_{1(1\times19)} \times G^{ECC}_{1(1\times19)} + e,$$

where $G^{ECC}_{1(1\times19)} = X_{1(1\times19)} \times G_{1(1\times19)} \times P_{1(1\times19)} \times D_{1(1\times19)}$, masking matrices $X_{1(1\times19)}$, $P_{1(1\times19)}$ and $D_{1(1\times19)}$ are long-term keys of the key fob and on-board computer of the car.

6. $c_{1(1\times19)}$ enters the communication channel and is transmitted to the on-board computer of the car.

Vehicle on-board computer software:

1. At the request of the car key software, a random number of 76 bits is generated.

2. Converted to information sequence I_{1x19} with elements from the field $GF\,(2^4)$.

3. Transformation of the information sequence $I_{1\times19}$ based on the use of McEliece CCC masking matrices $P_{1(1\times19)}$ and diagonal matrix $D_{1(1\times19)}$:

$$I_{2(1\times19)}=I_{1(1\times19)}\times P_{1(1\times19)}\times D_{1(1\times19)}.$$

4. Transmission $I_{2(1\times19)}$ on a key fob.

5. Upon receipt $c_{1(1\times19)}$ based on the fast Berlekamp-Massey decoding algorithm, the error vector is found, which determines the command that came from the key fob.

Table 5 presents the results of the analysis of the provision of security services: confidentiality, integrity and authenticity using various wireless channels.

Table 5

Comparative characteristics of wireless channels

Technology	Providing security services			Degree of information secrecy (β_i)				
	A_i^C	A_i^I	A_i^{Au}	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	–/+	–/+	–/+	–	–	–	+	+
IEEE802.16 m (WiMAX2)	–/+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1, Bluetooth 5+KNX	–/+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	–/+	–	–	–	+	+
LTE+*CCC* on *ECC* (*EC*)	+	+	+	+	+	+	+	+
LTE+*CCC* on *ECC* (*MEC*)	+	+	+	+	+	+	+	+

Analysis of the Table 4 shows that the use of symmetric cryptosystems based on block and stream ciphers (used in the KNX standard) do not provide full confidentiality and integrity services in the post-quantum period.

Thus, the proposed algorithm ensures the closing of the wireless channel using a software and hardware complex. The use of a hardware solution for closing (encrypting) the execution command on the on-board computer of the car will counteract almost all threats of intercepting the code execution command and hacking the car's security system as a whole.

6. Discussion of the results of using the McEliece and Niederreiter crypto-code constructions to provide security services

The developed method for ensuring the authenticity and confidentiality of information in wireless channels is based on the use of Grover and Shor, resistant to post-quantum threats, and makes it possible to provide a tunneling mode in open channels. Given in Table 4, the results of security service provision studies confirm that the proposed CCCs on the ECC provide basic security services. Parameters of noise-immune codes given in Table 1, and the parameters of asymmetric cryptosystems based on McEliece and Niederreiter CCCs provide their practical application. Table 6 shows the results of studies of the capacitive characteristic in software implementation on the power of the field.

Table 6

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

McEliece CCC	*GF*(*q*)					
	2^5	2^6	2^7	2^8	2^9	2^{10}
EC	10018042	18048068	32847145	47489784	63215578	82467897
shortened MEC	10007947	17787431	28595014	44079433	61974253	79554764
elongated MEC	11156138	18561228	33210708	48297112	65171690	84051337

The resulting Table 6 shows that the number of group operations of the software implementation of the CCC, depending on the field strength, is 4.5 times less when using the MEC. So, if for the implementation of McEliece's CCC in the field GF(2^{10}) it is needed 82,5×10^6 group operations, then the implementation of the CCC on the MEC in the field GF(2^6) requires 17.7 – 18.6×10^6 group operations.

Table 7 presents the results of studies of the capacitance characteristic in software implementation from the field strength when using defective codes and constructing hybrid crypto-code constructions (HCCC).

When using the HCCC, a significant increase in the speed of systems has been achieved (at least 20 times in terms of the speed of generating a cryptogram), which makes it possible to use resource-limited hardware devices for cryptographic information protection by such systems.

To conduct statistical studies of the stability of the studied cryptosystems, the package NIST STS 822 was used [31]. The research results are presented in Table 8.

Analysis of the Table 8 showed that despite the decrease in the power of the Galois field to *GF* (2^6) for CCC on MEC and *GF* (2^4) for the HCCC, the statistical characteristics of such crypto-code structures turned out to be at least as good as the traditional McEliece CCC on *GF* (2^{10}). All cryptosystems passed 100 % of the NIST tests, and the best result was shown by the HCCC on shortened MECs: 155 out of 189 tests were passed at the level of 0.99, which is 82 % of the total number of tests. At the same time, the traditional McEliece CCC on *GF* (2^{10}) showed 149 tests at the level of 0.99.

Table 7

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

McEliece CCC	*GF*(*q*)						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
shortened MEC	8293075	10007947	17787431	28595014	44079433	61974253	79554764
elongated MEC	8506422	11156138	18561228	33210708	48297112	65171690	84051337
HCCC on elongated MEC	5612316	7900315	14892945	25565274	42279183	58963778	76564173
HCCC on shortened MEC	5942627	7905257	14682411	25595014	42116327	58468143	75474764

Table 8

Statistical security research results

McEliece CCC	Number of tests in which more than 99 % of the sequences passed the test	Number of tests in which more than 96 % of the sequences passed the test	Number of tests where less than 96 % of the sequences passed the test
EC	149 (78,83 %)	189 (100 %)	0 (0 %)
shortened MEC	151 (79,89 %)	189 (100 %)	0 (0 %)
elongated MEC	152 (80,42 %)	189 (100 %)	0 (0 %)
HCCC on elongated MEC	153 (80,95 %)	189 (100 %)	0 (0 %)
HCCC on shortened MEC	155 (82 %)	189 (100 %)	0 (0 %)

This approach confirms that the use of CCC makes it possible to provide basic security services in wireless channels without forming VPN channels, which greatly simplifies practical use in the formation of the architecture of smart-city networks. Thus, the proposed method on CCC with different ECCs makes it possible to provide not only security services, but also to increase the reliability of transmitted information flows in the channels of LTE technologies in an integrated manner. The use of a multi-loop information security system based on CCC also forms an objective assessment of threats, and the current state of security of the system as a whole. The main limitation of the proposed approach for providing security services in wireless communication channels is the use of either a tunnel mode for point-to-point connection, or the use of a mobile broadband Internet channel, in which there are “no” possible filters and limitations of various mobile communication providers. A promising direction for further research is to evaluate the effectiveness of using the proposed method and the Concept of multicontour information protection based on the use of McEliece and Niederreiter CCC with the formation of a control system based on a desktop server.

7. Conclusions

1. The formation of socio-cyber-physical systems based on the integration and synthesis of wireless technologies and mobile Internet technologies, with Internet of things, ensures the further development of digital services. The emergence and development of smart technologies determines not only the vector of further digitalization of services, but also requires a new approach to the formation of an objective assessment of security threats. At the same time, it is necessary to build multicontour information security systems that take into account not only the hardware/software elements of the CPS infrastructure, but also the physical location and form of ownership. In the context of the growth of APT-attacks, the formation of new foundations of the Security Concept is an objective necessity. The use of CCC in wireless channels allows to provide the required level of security, due to the formation of tunnel modes, when connecting point-to-point, or the use of broadband mobile Internet channels based on post-quantum algorithms – crypto-code constructions. The proposed approach allows not only to take into account signs of synergy and hybridity of threats, but also provides an objective assessment of both the threats themselves to critical elements of the CPS infrastructure and the assessment of CPS security as a whole.

2. The proposed mathematical model for constructing asymmetric cryptosystems based on McEliece and Niederreiter CCC makes it possible to provide the required level of confidentiality, integrity and authenticity services and to practically implement the proposed method. This approach provides the required level of protection of security services, and the use of various noise-immune codes allows, taking into account the level of information secrecy, to ensure its reduction in energy consumption and increase the efficiency of information transmission.

3. The proposed algorithm for the implementation of security services based on post-quantum algorithms of McEliece and Niederreiter asymmetric cryptosystems on various algebrogeometric and detrimental codes makes it possible to close the wireless channel and provides the possibility of expanding the range of commands and/or functionality.

Conflict of interests

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was conducted without financial support.

Availability of data

The manuscript has no associated data.

References

1. Merz, H., Hansemann, T., Hübner, C. (2009). Building Automation: Communication systems with EIB/KNX, LON und BACnet. Springer, 282. doi: https://doi.org/10.1007/978-3-540-88829-1
2. KNX Technical Manual. 2CKA001473B8668. 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
3. Technical documentation on KNX devices (2006). ABB.
4. KNX Handbook Version 1.1 Revision 1 (2004). Konnex Association.
5. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual. Busch-Watchdog Sky KNX (2016). Busch-Jaeger Elektro GmbH, 648.
6. 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
7. Manual for KNX Planning (2017). Siemens Switzerland Ltd, 100.
8. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation (2010). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 116.
9. Guide for Cybersecurity Event Recovery. NIST. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf
10. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
11. Guide to LTE Security. NIST Special Publication (SP) 800-187. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-187/draft/documents/sp800_187_draft.pdf
12. 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
13. 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
14. 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/wp-content/uploads/papers/v1i6/F0320121611.pdf
15. 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
16. Tschofenig, H. (2019). Diameter: new generation AAA protocol – design, practice, and applications. John Wiley & Sons, Ltd. doi: https://doi.org/10.1002/9781118875889
17. Ugrozy bezopasnosti yadra paketnoy seti 4G. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
18. Uyazvimosti protokola Diameter v setyakh 4G. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
19. Ashibani, Y., Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. Computers & Security, 68, 81–97. doi: https://doi.org/10.1016/j.cose.2017.04.005
20. Graja, I., Kallel, S., Guermouche, N., Cheikhrouhou, S., Hadj Kacem, A. (2018). A comprehensive survey on modeling of cyber-physical systems. Concurrency and Computation: Practice and Experience, 32 (15). doi: https://doi.org/10.1002/cpe.4850
21. Minahil, Ayub, M. F., Mahmood, K., Kumari, S., Sangaiah, A. K. (2021). Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. Digital Communications and Networks, 7 (2), 235–244. doi: https://doi.org/10.1016/j.dcan.2020.06.003
22. Inam ul haq, Wang, J., Zhu, Y., Maqbool, S. (2021). An efficient hash-based authenticated key agreement scheme for multi-server architecture resilient to key compromise impersonation. Digital Communications and Networks, 7 (1), 140–150. doi: https://doi.org/10.1016/j.dcan.2020.05.001
23. Darem, A., Alhashmi, A. A., Jemal, H. A. (2022). Cybersecurity Threats and Countermeasures of the Smart Home. Ecosystem. International Journal of Computer Science and Network Security, 22 (3), 303–311. doi: https://doi.org/10.22937/IJCSNS.2022.22.3.39
24. Munilla, J., Burmester, M., Barco, R. (2021). An enhanced symmetric-key based 5G-AKA protocol. Computer Networks, 198, 108373. doi: https://doi.org/10.1016/j.comnet.2021.108373
25. Generic authentication architecture (GAA); generic bootstrapping architecture (GBA). TS 33.220. 3GPP. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2280
26. HMAC: Keyed-Hashing for Message Authentication. Available at: https://www.ietf.org/rfc/rfc2104.txt

27. 3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation. TR 35.909. 3GPP. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2405
28. 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
29. 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. doi: https://doi.org/10.15587/1729-4061.2016.75250
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: http://doi.org/10.15587/978-617-7319-31-2
32. Bleykhut, R. (1986). Teoriya i praktika kodov, kontroliruyuschikh oshibki. Moscow: Mir, 576.
33. Naim, M., Ali-Pacha, H., Ali-Pacha, A., Hadj-Said, N. (2021). Lengthening the period of a Linear Feedback Shift Register. Journal of Engineering Technology and Applied Sciences. doi: https://doi.org/10.30931/jetas.778792