UDC 004.056.5:004.272:621.391 **doi:** https://doi.org/10.20998/3083-6298.2025.02.03

Sergii Dunaiev[1]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

AN INTEGRATED APPROACH TO DATA CONFIDENTIALITY IN 5G/6G BASED ON LDPC CODES AND POST-QUANTUM CRYPTOGRAPHY

Abstract. Relevance of the research. In the current conditions of the development of next-generation wireless networks (5G/6G), there is a growing need to ensure a high level of secrecy and data protection in the face of complex cyberthreats and the prospect of quantum attacks. The use of LDPC codes in combination with post-quantum cryptography methods creates the possibility of a comprehensive approach that allows simultaneously increasing the reliability of coding and resistance to cryptanalytic attacks, while maintaining high network throughput. **Subject of the research.** Methods and models of data secrecy in 5G/6G mobile networks based on LDPC codes integrated with post-quantum cryptography algorithms, as well as the principles of their combination to achieve increased resistance to attacks. **Purpose of the research.** Development and justification of an integrated data secrecy model that provides an optimal combination of coding and cryptography mechanisms to increase the level of security and efficiency of information processing in high-speed 5G/6G networks. **The following results** were obtained. A comprehensive analysis of authentication and coding methods in 5G and 6G networks was conducted. A comparative table of authentication and coding mechanisms, including post-quantum cryptographic algorithms (PQC), was developed. The advantages and limitations of existing 5G authentication methods were identified and the integration of PQC was proposed to improve security in 6G networks. The principles of LDPC codes were analyzed and their effectiveness in improving data confidentiality was demonstrated. An integrated data hiding model was proposed that combines LDPC coding with post-quantum cryptography to ensure both high-speed communication and resistance to quantum attacks. The presented models allow formalizing the processes of authentication, data transmission, and increasing confidentiality in next-generation networks, as well as their real-time adaptation to various network conditions and threat levels. **Conclusions.** An integrated approach to data secrecy based on LDPC codes and post-quantum cryptography allows for significantly increasing the resilience of 5G/6G communication systems to current and future threats, ensuring a balance between speed, reliability, and cryptographic robustness.

Keywords: 5G/6G; LDPC codes; post-quantum cryptography; data secrecy; information protection; integrated model; quantum attacks.

Introduction

Problem relevance. In modern 5G/6G wireless networks, the growth in the volume of transmitted information and the active implementation of smart technologies create new challenges in the field of ensuring data confidentiality and integrity. Traditional protection methods, which involve the separate use of noise-resistant coding and cryptography, are not effective enough in the face of the threat of quantum computing and high dynamics of network environments.

Literature review. By the early 2020s, fifth-generation (5G) mobile networks had been deployed in most countries around the world, offering key capabilities such as massive device connectivity (mMTC), ultra-high reliability link capacity (uRLLC), and consistently low latency [1]. However, it is already clear that 5G will not be able to fully meet the demands that will arise after 2030, especially given the increase in the number of connected devices, the volume of data processed, and increased security requirements.

Sixth-generation (6G) networks are designed to provide higher levels of energy efficiency, spectral efficiency, and scalability of communication solutions. Particular attention will be paid to enhancing security, which in 6G will have fundamentally new characteristics due to the introduction of data concealment methods that are absent in 5G technology.

The 6G architecture will integrate terrestrial and above-ground segments into a single communication environment spanning air, land, space, and sea [2,3]. This necessitates adaptive, context-aware security solutions that can dynamically change the level of protection depending on the conditions of information transmission.

Additionally, the use of new frequency bands (millimeter waves, terahertz (THz), and optical spectrum) will significantly increase network throughput, but at the same time will complicate the task of encryption and stealth due to increased risks of interception and interference.

Thus, 6G will not only develop the capabilities of 5G, but will also define new standards of protection and reliability necessary for the stable operation of intelligent infrastructures, telemedicine, autonomous transportation systems, and large-scale distributed IoT platforms. Comparative characteristics of 5G and 6G in key parameters, such as data transfer rate, reliability, latency, and localization accuracy, are given in Table 1. [4].

Table 1 – **Comparison of 5G and 6G characteristics**

№	Parameter	5G	6G
1	Data transfer speed	From 0,1 Gb/s to 20 Gb/s	From 1 Gb/s to 1 Tb/s
2	Reliability	Error probability $< 10^{-5}$	Error probability $< 10^{-9}$
3	Delay	Less than 5 ms	Less than 100 ns
4	Localization accuracy	Less than 10 cm in two dimensions	Less than 1 cm in three dimensions
5	Cryptography	TLS/SSL	TLS/SSL +

№	Parameter	5G	6G
	support		new models шифрування
6	Coding mechanisms	Turbo, LDPC	LDPC, Polar, Post-Quantum Coding
7	AI support	Limited	Built-in (AI-native)

As shown in Table 1, sixth-generation (6G) networks demonstrate a significant increase in key technical indicators compared to 5G. In particular, the data transfer rate in 6G can reach 1 Tbit/s, which is tens of times higher than the capabilities of 5G and opens up prospects for processing large amounts of information in real time. Reliability increases by 10,000 times, which is crucial for critical areas such as medicine, autonomous transport systems, and defense technologies.

Another breakthrough is the sharp reduction in latency from the millisecond level in 5G to nanoseconds in 6G. This makes it possible to implement ultra-reliable low-latency communication (URLLC) scenarios, in particular for telesurgery or remote control of unmanned aerial vehicles in real time.

The accuracy of location determination is also significantly increased - from centimeter in 5G to millimeter in three-dimensional space in 6G. This opens up new opportunities for the development of "smart" cities, robotic systems, augmented reality technologies and high-precision monitoring.

Thus, 6G not only significantly surpasses 5G in all key parameters, but also creates new challenges in the field of cybersecurity. To effectively ensure secrecy, integrity and rapid detection of threats, solutions are needed that go beyond the capabilities of classical protocols such as TLS/SSL. This necessitates the implementation of innovative methods of secure data transmission, in particular, noise-resistant coding technologies, machine learning algorithms and analysis of behavioral characteristics of traffic.

A review of the literature and modern solutions in the field of data secrecy [5,6] showed that classical coding methods (Reed–Solomon codes, turbo codes) are inferior to LDPC codes in terms of efficiency in high-speed networks. LDPC codes provide low error rates and are suitable for high transmission rates. In addition, post-quantum cryptography is aimed at countering future quantum attacks (algorithms on lattices, codes, multidimensional structures). [7-9] However, it must be noted that the separate use of cryptography or coding does not guarantee a sufficient level of stability, which is a weak point in protection.

Thus, protecting the authenticity and integrity of data in 5G and 6G wireless networks is implemented using a comprehensive approach that combines cryptographic mechanisms with error detection and correction codes. This approach allows not only to confirm the authenticity of the user or device, but also to prevent falsification of information during its transmission.

This research proposes an integrated approach that combines LDPC codes with modern cryptographic and post-quantum algorithms, providing multi-level information protection at the physical and channel levels. Such synergy allows not only to increase data secrecy, but also to optimize the use of network resources, ensuring resilience to a wide range of current and future cyber threats.

The **purpose of the research** is to develop and substantiate an integrated data secrecy model that provides an optimal combination of coding and cryptographic mechanisms to increase the level of security and efficiency of information processing in high-speed 5G/6G networks.

2. The main part of the study

In the context of the stated goal, it is necessary to create a single protective mechanism that combines:

coding (LDPC codes), which reduces the probability of errors, increases the reliability of data transmission and simultaneously creates a "mask" of the message structure;

cryptography (post-quantum algorithms), which protects data from interception even in the event of the emergence of quantum computers capable of cracking classical methods.

In combination, this provides a double line of defense: even when attempting to crack the cipher, an additional level of LDPC coding complicates analysis and increases secrecy.

2.1. Authentication models in 5G and 6G networks. Modern 5G wireless networks use a multi-layered authentication model that combines several security mechanisms, including Primary Authentication (based on the SIM card and SUPI identifier), Secondary Authentication (e.g., via EAP protocols), and 5G-AKA with the resynchronization mechanism and SEAF as the central element of trust. Verification of the authenticity of transmitted data in 5G is reinforced by means at the physical layer - from CRC for frame integrity control to LDPC and Polar codes, which perform both the role of error correction and indirect authentication.

In 6G technologies, the approach to authentication becomes more context-oriented and includes integration with post-quantum cryptographic algorithms (in particular, CRYSTALS-Kyber and Dilithium) to ensure resistance to attacks using quantum computing. Zero Trust Architecture guarantees authentication at every node in the network, and blockchain is used for decentralized identification of users and devices. Coding technologies such as LDPC, Reed-Solomon, and PUF in 6G not only increase the reliability of data transmission, but also directly integrate with cryptographic modules, creating a unified system for verifying the source of information and protecting against counterfeiting even under the threat of quantum attacks.

Table 2 compares authentication and encryption tools for 5G and 6G networks.

Table 1 – **Comparison table of means of authentication and coding**

Parameter	5G	6G
Authentication protocols	5G-AKA, EAP	Context-aware, Post-Quantum, Zero Trust
Basic codes	Polar, LDPC, CRC	LDPC, RS, PUF
Trust architecture	SEAF, HSS	Blockchain, AI-based identity graphs
Additional means	USIM, AKA keys	AI biometrics, multi-factor authentication
Approach to source verification	Syntactic/control	Noise + contextual behavioral testing

The analysis of authentication and encryption tools in 5G and 6G networks (Table 2) demonstrates a clear evolution from classic centralized mechanisms to more flexible, intelligent, and post-quantum threat-resistant solutions.

In 5G, two-factor authentication based on SIM/USIM, 5G-AKA and EAP protocols, as well as centralized trust infrastructure (SEAF, HSS) play a key role. In 6G, this approach is transformed into dynamic context-aware models integrated with post-quantum cryptography algorithms (CRYSTALS-Kyber, Dilithium) and Zero Trust architecture, where authentication is performed at every node in the network.

Data integrity tools in 5G are based on LDPC and Polar codes, which are optimal for stable channels. In 6G, this set is supplemented by Reed-Solomon codes and Physically Unclonable Functions (PUF), which allows implementing a hardware level of device identification and protection, especially in environments with a large number of IoT nodes.

While in 5G, source verification is mostly based on checksums and syntax checking, 6G uses noise-based concealment methods, behavioral pattern analysis, and real-time risk assessment. In this case, noise-resistant coding (LDPC, RS) in 6G performs a dual function. – not only protection against interference, but also the role of an authenticity indicator.

Thus, 6G forms a new level of security, where the combination of noise-resistant coding, post-quantum cryptographic algorithms, behavioral analytics and decentralized architectures creates multi-layered protection with minimal delay in responding to threats, which is especially important for intelligent systems, critical infrastructure and URLLC scenarios.

For clarity, we present a generalized comparison of authentication and encryption mechanisms in 5G and 6G networks, taking into account the integration of post-quantum cryptographic algorithms (Table 3).

Table 3 – **Comparison of authentication and encryption tools in 5G and 6G networks taking into account post-quantum algorithms (PQC)**

Parameter / Technology	*5G*	*6G (including PQC)*
Authentication model	Multilevel: Primary (SIM, SUPI), Secondary (EAP), 5G-AKA with resynchronization, SEAF as a trust center	Context-based authentication, Zero Trust Architecture, integration with PQC (CRYSTALS-Kyber, Dilithium), blockchain identity
Basic protocols	5G-AKA, EAP	PQC-extended authentication protocols, hybrid schemes (classical cryptography + PQC)
Integrity checking mechanisms	Frame-level CRC	CRC + PQC-based MAC codes and digital signatures
Code technologies for authenticity	LDPC (at the physical layer), Polar Codes for control channel (URLLC)	Deep integration of LDPC, RS codes for source verification, PUF codes for hardware identification, PQC-based code schemes
The role of coding	Indirect authentication through successful decoding	Combined function – protection, source verification, resistance to quantum attacks

The data in Table 3 demonstrate that in 6G, authentication and encryption evolve from the classic multi-layered identification schemes of 5G to context-oriented and post-quantum mechanisms capable of providing protection against future quantum threats. While in 5G encryption is used mainly for integrity verification and as an auxiliary authentication tool, in 6G it is integrated directly into cryptographic mechanisms, combining LDPC, RS codes, PUF and PQC solutions to create a multifunctional, attack-resistant system.

Therefore, an integrated approach based on LDPC codes in combination with modern cryptographic and post-quantum algorithms will provide a significant increase in data secrecy and noise immunity in 5G/6G wireless networks. Unlike traditional solutions, where protection at the physical and channel levels is implemented separately, the integration of mechanisms will allow achieving multi-level protection with simultaneous optimization of bandwidth and network resource utilization, which is critically important for future generations of mobile communications.

2.2. Using LDPC codes to enhance data secrecy. As mobile networks evolved, each successive generation of communications sought not only to increase data transfer speeds but also to strengthen information security. Starting with 1G in the 1980s, which provided only analog voice transmission without encryption, users remained vulnerable to eavesdropping and data interception. [10] 2G introduced the first digital security mechanisms, including authentication, encryption, and temporary access identifiers. However, due to one-way authentication and incomplete encryption, the network remained potentially open to attack. [10,11]

3G significantly improved security through two-way authentication and radio interface encryption. However, with the growth of Internet services, new

threats have emerged, including attacks on IP protocols and leaks of personal data. [11] 4G and 5G have expanded network functionality: cloud services, NFV, and SDN have appeared, which has increased flexibility and scalability, but at the same time created additional risks, including vulnerabilities at the access point level, potential DDoS attacks, data leaks due to weak service isolation, and the possibility of eavesdropping in MIMO architectures. [12-14] The emergence of 6G, focused on mass device integration, artificial intelligence, holographic communications a and the terahertz spectrum, poses new challenges in the field of information security, especially with regard to protecting data privacy. [15-18] Ensuring the security of information transmission in such complex, multi-level and dynamic networks requires new approaches. In particular, highly efficient methods of noise-resistant coding are needed, capable not only of correcting errors, but also of making information interception more difficult. [19]

In this context, LDPC codes deserve special attention as a key technology for ensuring secrecy and noise immunity in next-generation wireless networks. Their flexibility, ability to work close to the Shannon limit, and compatibility with parallel processing make LDPC codes a promising tool for increasing the reliability and confidentiality of data transmission in 6G networks.

Modern 5G and 6G networks require new approaches to ensuring confidentiality and secrecy of data. Traditional TLS/SSL protocols, despite their wide application, demonstrate limited stability in dynamic and high-speed networks, in particular due to:

the possibility of analyzing traffic and identifying data by metadata and time characteristics;

delays during computationally intensive encryption and certificate verification;

vulnerability at the session negotiation stage;

the lack of mechanisms for detecting interference before decryption. [20,21]

Overcoming these limitations requires multi-layered protection that combines [21,22]:

1. Noise-resistant coding (LDPC, RS) at the transport layer to ensure data integrity before cryptographic processing.

2. Integration of post-quantum cryptography algorithms to resist quantum attacks and increase transmission secrecy.

3. Adaptive encryption using machine learning for traffic classification and anomaly detection.

4. “TLS + ECC/LDPC” models to combine cryptographic protection with error control and metadata obfuscation.

Thus, the combination of LDPC codes and post-quantum cryptography provides multi-layered protection, including confidentiality, concealment, integrity, and resilience to future quantum attacks. This makes the integration of such mechanisms a key direction for the development of secure communications in 6G, where network dynamics and device scalability create new challenges for traditional protocols.

2.3. Principles of operation of LDPC codes and basics of post-quantum cryptographic algorithms. Thus, LDPC codes are one of the most efficient classes of linear block codes, which have been widely used in next-generation wireless networks in recent years. Their key advantages are high noise immunity, flexible structure, and the ability to work effectively even in difficult channel conditions with noise, fading, or erasure.

The main properties of LDPC codes are as follows [23-26]:

sparse structure of the verification matrix H, which reduces computational complexity;

iterative decoding using belief propagation or minimum distance algorithms, which provides high accuracy of correction;

the possibility of parallel implementation at the hardware level, which makes LDPC a natural choice for 5G/6G networks;

approximation to the Shannon limit - with the right choice of the H matrix structure, LDPC codes operate at a distance of only ~0.0045 dB from the theoretical channel bandwidth limit.

This means that LDPCs provide the most efficient use of the spectrum and high reliability of data transmission without a significant increase in redundancy. In 5G systems, they are already used for data transmission channels, and in 6G their use is expected to expand with dynamic matrix reconstruction for specific network scenarios.

The contribution of LDPC codes to data secrecy is that these codes increase the level of secrecy due to the fact that:

information bits are distributed in the codeword in such a way that their interception does not allow data to be recovered without knowledge of the code structure;

when combined with physical encryption methods, an additional level of security is created at the physical layer;

in integration with chaotic modulations in 6G, hybrid security systems are created that simultaneously use the structural and random properties of the signal.

Thus, LDPC is not only an error correction tool, but also a component of a comprehensive approach to ensuring secrecy.

Post-quantum cryptographic algorithms (PQC) complement LDPC. With the development of quantum computing technologies, classical cryptographic algorithms (RSA, ECC) become vulnerable to attacks using quantum algorithms (in particular, the Shor and Grover algorithm). This requires a transition to post-quantum protection methods that are able to remain stable even in the presence of powerful quantum computers.

The main classes of post-quantum cryptographic algorithms include:

1. Lattice schemes that provide stability on the problems of finding the shortest vector in the lattice.

2. Code cryptography that uses the decoding complexity of random linear codes.

3. Multivariant cryptosystems that are based on

solving systems of polynomials over finite fields.

4. Isogenies of elliptic curves that are used to construct key exchanges.

5. Hash cryptography that uses the one-way properties of hash functions.

6. Integrated LDPC + PQC model for 5G/6G networks.

The combination of LDPC codes with post-quantum algorithms creates a multi-level protection system that:

provides resistance to noise and interference at the physical level (LDPC);

guarantees cryptographic resistance even against quantum attacks (PQC);

allows to maintain high throughput and data processing efficiency in high-speed networks.

As a result, such an integrated model forms a new standard of data secrecy that meets the requirements of future telecommunication systems, where reliability, speed, and security from quantum attacks are simultaneously critical.

2.4. Development of an integrated data privacy model. This model is based on the concept of integrating coding and cryptography to ensure resistance to attacks. The theoretical basis for developing an integrated data secrecy model involves the following stages:

formation of the model architecture, which provides for multi-level protection: at the physical level (LDPC) and the transport/network level (PQC);

determination of optimality criteria, namely high throughput, minimal delays, resistance to attacks;

carrying out optimization measures, i.e. selection of LDPC block lengths, matrix parameters and cryptographic algorithms.

development of research methodology: attack scenarios - passive (interception), active (insertion/modification), quantum (PQC decryption); experiment algorithm - modeling of communication channels, LDPC parameters, application of crypto algorithms; research tool base - MATLAB/Simulink, Python libraries (PyLDPC, PQCrypto), network emulators.

Thus, the integrated model looks like a multi-level architecture, where:

at the physical level, data is transmitted using LDPC codes and error minimization and signal structure masking are performed;

at the transport level, post-quantum crypto algorithms are used;

at the adaptation level, LDPC parameters and crypto algorithm are automatically selected for load and threats (active or passive attacks).

The general architecture of the integrated security model, which combines LDPC codes and PQC algorithms to ensure the stability of 5G/6G networks, is shown in Fig. 1.

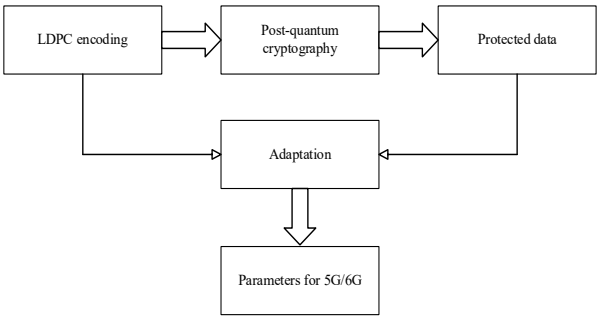

Fig. 1. Architectural diagram of the integrated model

As can be seen from Fig. 1, the integrated data secrecy model combines code protection mechanisms based on LDPC and post-quantum cryptography (PQC). LDPC coding provides resistance to transmission errors and a basic level of secrecy, which is especially important in conditions of high speeds and interference in 5G/6G networks. Post-quantum cryptography implements stable cryptographic protection mechanisms aimed at countering attacks by quantum computers, and guarantees reliable key exchange and authentication. At the output, a protected data module is formed, where the information retains both resistance to interference and cryptographic security. The Adaptation Block regulates the operation of the entire system based on the dynamic parameters of the transmission environment and the features of the next-generation network (5G/6G), ensuring optimal tuning of LDPC codes and PQC algorithms for specific conditions.

Thus, the model allows for an integrated increase in data secrecy and security, combining the capabilities of coding theory and modern cryptography, which is especially important for future mobile networks.

To fully reveal the potential of the integrated model, it is advisable to conduct a detailed examination of the internal mechanisms of operation that provide increased resistance to cyberattacks and comprehensive data protection. These aspects are specified in Fig. 2, which demonstrates the interrelationship of protection levels and their contribution to the formation of an integrated level of security.

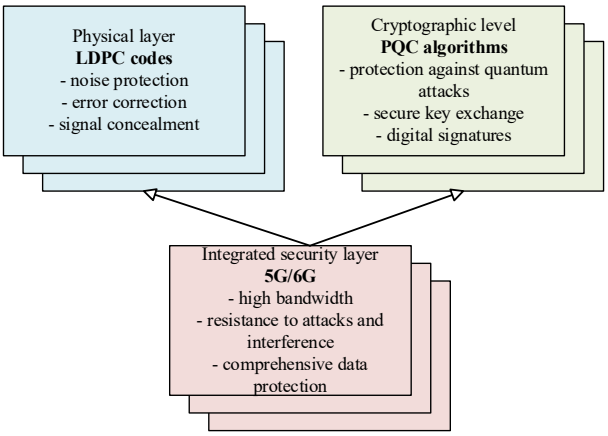

Fig. 2. Integrated LDPC + PQC model for 5G/6G networks

Analysis of Fig. 2 shows that the proposed integrated model of data secrecy and protection in 5G/6G networks effectively combines the physical security layer based on LDPC codes and the cryptographic layer using post-quantum algorithms (PQC). This approach provides multi-level protection: on the one hand, the influence of interference is reduced and signal secrecy is increased, and on the other hand, resistance to quantum attacks and secure key exchange are guaranteed. The result is an integrated 5G/6G security layer, characterized by high throughput, resistance to attacks and comprehensive data protection. This allows us to conclude that the combination of LDPC codes and PQC is a promising direction for increasing the cyber resilience of next-generation mobile networks.

3. Discussion of results

The results of the study confirmed the feasibility of integrating LDPC codes with post-quantum cryptography as an effective approach to increasing data secrecy in 5G/6G networks. The analytical conclusions obtained indicate that the use of LDPC codes not only provides high error correction and optimal use of bandwidth, but also creates an additional level of resistance to attacks aimed at compromising data.

Of particular importance is the synergistic combination of LDPC codes with post-quantum cryptography algorithms, which forms a multi-level protection system capable of counteracting both classical and quantum attacks. This indicates the practical significance of the approach for protecting critical information infrastructures, where traditional cryptographic methods may not be effective enough. Thus, the study demonstrates both theoretical and applied value, laying the foundation for implementation in future security standards for new generation mobile networks.

Further research in this area may be aimed at:

improving methods for adaptive tuning of LDPC code parameters in real-world 5G/6G network operating conditions, taking into account the dynamics of communication channels;

integrating post-quantum cryptographic algorithms with other security mechanisms, in particular authentication and key management protocols;

applying machine learning and artificial intelligence methods for automated management of data secrecy processes and optimizing the security system in 6G;

studying the scalability and power consumption of integrated solutions with a view to their implementation in IoT systems and critical infrastructures.

Thus, the results of the research open up broad opportunities for the development of the latest information protection technologies in the post-quantum era and contribute to the formation of a scientific and practical basis for future cyber security standards in next-generation networks.

4. Conclusions

The paper proposes an integrated approach to increasing data secrecy in 5G/6G networks by combining LDPC codes with post-quantum cryptography. The results obtained show that such a combination provides a stable multi-level protection model capable of counteracting both classical and promising quantum attacks.

The scientific novelty of the study lies in determining the optimal parameters of LDPC codes that increase information secrecy without reducing the system throughput, as well as in developing a concept for their synergistic use with PQC algorithms. The practical significance lies in the possibility of applying the proposed approach to protect critical information infrastructures, including financial services, medical systems, and intelligent city technologies.

Prospects for further research are related to improving methods for adaptively tuning LDPC code parameters in dynamic network operating conditions, integrating PQC with other protective mechanisms, and applying artificial intelligence technologies for automated security management in the 6G environment.

REFERENCES

1. Khan, R., Kumar, P., Jayakody, D. and Liyanage, M. (2019), “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions”, *IEEE Commun. Surveys & Tutorials*, DOI:10.1109/COMST.2019.2933899
2. Yazar, A., Dogan-Tusha, S. and Arslan H. (2020), “6G vision: An ultra-flexible perspective”, *ITU Journal on Future and Evolving Technologies*, Vol. 1, Iss. 1, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.itu.int/dms_pub/itu-s/opb/itujnl/S-ITUJNL-JFETF.V1I1-2020-P09-PDF-E.pdf
3. Alwis, C., Kalla, A., Pham, Q.-V., Kumar, P., Dev, K., Hwang, W.-J. and Liyanage, M. (2021), “Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research”, *IEEE Open J. Commun. Soc*., DOI:10.1109/OJCOMS.2021.3071496
4. Abdel Hakeem, S. A., Hussein, H.H. and Kim, H. (2022), “Security Requirements and Challenges of 6G Technologies and Applications”, *Sensors*, No22, https://doi.org/10.3390/s22051969
5. Subhi, M. I., Al-Doori, Q. and Alani, O. (2023), “Enhancing Data Communication Performance: A Comprehensive Review and Evaluation of LDPC Decoder Architectures”, *Ingénierie des Systèmes d’Information*, Vol. 28, No5, pp.1113-1125, https://doi.org/10.18280/isi.280501
6. Rowshan, M., Qiu, M., Xie, Y., Gu, X. and Yuan, J. (2024), “Channel Coding Toward 6G: Technical Overview and Outlook”, IEEE Open Journal of the Communications Society, Vol. 5, https://doi.org/10.1109/OJCOMS.2024.3390000
7. Meyer, A. (2025), “Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems”, *arXiv:2505.08791v1*, https://doi.org/10.48550/arXiv.2505.08791
8. Aguilar-Melchor, C., Aragon, N., Deneuville, J.-C., Gaborit, P.,·Lacan J. and Zémor, G. (2024), “Efficient error-correcting codes for the HQC post-quantum cryptosystem”, *Designs, Codes and Cryptography*, Vol. 92, pp. 4511–4530, https://doi.org/10.1007/s10623-024-01507-6

9. Chen, A. C. H. (2024), “Homomorphic Encryption Based on Lattice Post-Quantum Cryptography”, *arXiv:2501.03249,* https://doi.org/10.48550/arXiv.2501.03249
10. Kato, N., Mao, B., Tang, F., Kawamoto, Y. and Liu, J. (2020), “Ten Challenges in Advancing Machine Learning Technologies toward 6G”, *IEEE Wirel. Commun*, No27. pp. 96–103, DOI: 10.1109/mwc.001.1900476
11. Arapinis, M., Mancini, L.I., Ritter, E. and Ryan, M. (2014), “Privacy through pseudonymity in mobile telephony systems”, *In Proceedings of the 2014 Network and Distributed System Security Symposium, San Diego, CA, USA*, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ndss-symposium.org/wp-content/uploads/2017/09/05_2_1.pdf
12. Zahariadis, T. and Kazakos, D. (2003), “Revolution toward 4G mobile communication systems”, *IEEE Wirel. Commun*, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scss.tcd.ie/hitesh.tewari/bib_files/zk03.pdf
13. Goyal, P., Batra, S. and Singh, A. (2010), “A literature review of security attack in mobile ad-hoc networks”, *Int. J. Comput. Appl*, Vol. 9., No12, pp. 11–15, https://doi.org/10.5120/1439-1947
14. Kim, S.J., Lee, H. and Lee, M. (2015), “A Study of 4G Network for Security System”, *Int. J. Adv. Cult. Technol*, Vol. 3, No 2, pp. 77–86, http://dx.doi.org/10.17703/IJACT.2015.3.2.77
15. Akpakwu, G.A., Silva, B.J., Hancke, G.P. and Abu-Mahfouz, A.M. (2018), “A survey on 5G networks for the internet of things: Communication technologies and challenges”, *IEEE Access*, No6, pp. 3619–3647, DOI: 10.1109/ACCESS.2017.2779844
16. Hakeem, S.A., Hady, A.A. and Kim, H.W. (2020), “Current and future developments to improve 5G-newradio performance in Vehicle-to-everything communications”, *Telecommunication Systems*, Vol. 3, pp. 331–353, DOI: 10.1007/s11235-020-00704-7
17. Mazurczyk, W., Bisson, P., Jover, R.P., Nakao, K. and Cabaj, K. (2020), “Challenges and novel solutions for 5G network security, privacy and trust”, *IEEE Wireless Communications*, Vol. 27, DOI:10.1109/MWC.2020.9170261
18. Navarro-Ortiz, J., Romero-Diaz, P., Sendra, S., Ameigeiras, P., Ramos-Munoz, J.J. and Lopez-Soler, J.M. (2020), “A survey on 5G usage scenarios and traffic models”, *IEEE Communications Surveys & Tutorials*, DOI:10.1109/COMST.2020.2971781
19. Ren, Y., Zhang, L., Shen, Y. and Song, W. (2024), “Edge-Spreading Raptor-Like LDPC Codes for 6G Wireless Systems”, *arXiv preprint arXiv:2410.16875*, https://arxiv.org/abs/2410.16875
20. Chen, X., Feng, W., Ge, N. and Zhang, Y. (2022), “Zero Trust Architecture for 6G Security”, *arXiv:2203.07716v1 [cs.NI]*, https://doi.org/10.48550/arXiv.2203.07716
21. Huoh, T.-L., Luo, Y., Li, P. and Zhang, T. (2023), “Flow-Based Encrypted Network Traffic Classification With Graph Neural Networks”, *IEEE Transactions on Network and Service Management*, Vol. 20, Iss. 2, pp. 1224-1237, DOI: 10.1109/TNSM.2022.3227500
22. Dohler, M., Saikali, S., Gamal, A. and et al. (2025), “The crucial role of 5G, 6G, and fiber in robotic telesurgery”, *Robotic Surgery*, Vol. 19, https://doi.org/10.1007/s11701-024-02164-6
23. Zakharchenko, V.M. and Levkivskyi, M.S. (2014), “Teoriia informatsii ta koduvannia”, *Kyiv: KNU*, 340 s.
24. Rudenko, N.V. and Lutsiuk, I.V. (2023), “Metody pobudovy merezh piatoho pokolinnia na osnovi isnuiuchykh merezh”, *Naukovi zapysky DUT*, №2(4), S.39-44, DOI: 10.31673/2518-7678.2023.020505
25. Hallaher, R. (2017), “Teoriia koryhuiuchykh kodiv iz nyzkoiu shchilnistiu perevirok”, *Per. z anhl., K.: Tekhnika*, 214 s.
26. Richardson, T., Urbanke, R. (2008), “Modern Coding Theory”, *Cambridge University Press*, 576 p., chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.karlin.mff.cuni.cz/~holub/soubory/ModernCodingTheory.pdf

Received (Надійшла) 07.07.2025
Accepted for publication (Прийнята до друку) 28.07.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Дунаєв Сергій Владиславович – аспірант кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;

Sergii Dunaiev – postgraduate student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;

e-mail: serg.dynaev@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-8736-3602.

ІНТЕГРОВАНИЙ ПІДХІД ДО ПРИХОВАНОСТІ ДАНИХ У 5G/6G НА ОСНОВІ LDPC-КОДІВ ТА ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

С.В. Дунаєв

Анотація. Актуальність дослідження. У сучасних умовах розвитку бездротових мереж нового покоління (5G/6G) зростає необхідність забезпечення високого рівня прихованості та захисту даних в умовах складних кіберзагроз і перспективи появи квантових атак. Використання LDPC-кодів у поєднанні з методами постквантової криптографії створює можливість інтегрованого підходу, що дозволяє одночасно підвищити надійність кодування та стійкість до криптоаналітичних атак, зберігаючи високу пропускну здатність мережі. **Предмет дослідження.** Методи та моделі прихованості даних у мобільних мережах 5G/6G на основі LDPC-кодів, інтегрованих із алгоритмами постквантової криптографії, а також принципи їхнього поєднання для досягнення підвищеної стійкості до атак. **Мета дослідження.** Розробка та обґрунтування інтегрованої моделі прихованості даних, яка забезпечує оптимальне поєднання кодувальних і криптографічних механізмів для підвищення рівня безпеки та ефективності обробки інформації у високошвидкісних мережах 5G/6G. **Отримано наступні результати.** Проведено комплексний аналіз методів автентифікації та кодування в мережах 5G та 6G. Розроблено порівняльну таблицю механізмів автентифікації та кодування, включаючи постквантові криптографічні алгоритми (PQC). Визначено переваги та обмеження існуючих методів автентифікації 5G та запропоновано інтеграцію PQC для підвищення безпеки в мережах 6G. Проаналізовано принципи LDPC-кодів та продемонстровано їх ефективність у підвищенні конфіденційності даних. Запропоновано інтегровану модель приховування даних, яка поєднує LDPC-кодування з постквантовою криптографією для забезпечення як високошвидкісного зв'язку, так і стійкості до квантових атак. Представлені моделі дозволяють формалізувати процеси автентифікації, передачі даних та підвищення конфіденційності в мережах наступного покоління, а також їх адаптацію в режимі реального часу до різних мережевих умов та рівнів загроз. **Висновки.** Інтегрований підхід до секретності даних на основі LDPC-кодів та постквантової криптографії дозволяє значно підвищити стійкість систем зв'язку 5G/6G до поточних та майбутніх загроз, забезпечуючи баланс між швидкістю, надійністю та криптографічною стійкістю.

Ключові слова: 5G/6G; LDPC-коди; постквантова криптографія; прихованість даних; захист інформації; квантові атаки.