https://doi.org/10.33271/nvngu/2025-6/148

I. S. Laktionov,
orcid.org/0000-0001-7857-6382,
V. V. Hnatushenko*,
orcid.org/0000-0003-3140-3788,
I. M. Udovyk,
orcid.org/0000-0002-5190-841X,
V. I. Olevskyi,
orcid.org/0000-0003-3824-1013

Dnipro University of Technology, Dnipro, Ukraine
* Corresponding author e-mail: Hnatushenko.V.V@nmu.one

SIMULATION-DRIVEN ASSESSMENT OF CRYPTOGRAPHIC ALGORITHMS FOR RESOURCE-CONSTRAINED INFOCOMMUNICATION NETWORKS

Purpose. To conduct a multi-criteria evaluation and analysis of the performance of encryption algorithms that may be potentially resistant to contemporary cyberattacks, including quantum attacks. The evaluation takes into account the ability of the algorithms to be deployed on devices with limited computational resources within the infocommunication networks during the transmission of information messages.

Methodology. Software implementation, testing and validation of selected cryptographic algorithms based on Python, considering the impact of limited resources and destabilising factors, such as signal noise components, based on computer experiments were applied. The performance of the studied cryptographic algorithms was analysed using statistical data processing methods and a multi-criteria evaluation approach.

Findings. The symmetric algorithms AES-256-GCM and ChaCha20-Poly1305 demonstrated the highest accuracy in signal recovery following encryption and decryption (MSE ranges from $1.95 \cdot 10^{-6}$ to $5.12 \cdot 10^{-5}$). The time taken to encrypt and decrypt I/Q signals using symmetric algorithms was found to be around 2.5 times faster than that required by the Kyber family. Computer experiments confirmed the existence of a trade-off between processing speed and security level. Symmetric algorithms are optimal for scenarios with critical processing speed requirements. However, Kyber provides greater protection reliability, albeit at the cost of additional resources. The correctness of the proposed computer model, which enables the computational and information-functional characteristics of cryptographic algorithms to be evaluated, has been proven.

Originality. Patterns of the destabilising influence of signal-to-noise ratio indicators and signal length on the accuracy of digital signal recovery after encryption have been established for different cryptographic algorithms (AES, ChaCha20 and the Kyber) in the context of their use in resource-constrained infocommunication systems.

Practical value. Implementing the computer model proved its suitability for studying cryptographic algorithms in resource-constrained environments, as well as its potential for improving information security protocols and selecting optimal algorithms based on processing speed requirements and desired security levels.

Keywords: *cryptographic algorithm, signal, noise, ciphertext, infocommunication network, accuracy, model*

Introduction. In the contemporary digital landscape, wireless infocommunication technologies, specifically encompassing mobile and satellite communication networks, have become indispensable for industrial operations and critical infrastructure [1, 2]. These systems underpin global navigation services, telemetry, general-purpose and specialised infocommunication platforms, transportation and logistics chains, energy facilities, and many other domains. The growing dependence of industry, commerce, transport, logistics and telecommunications on mobile and satellite communication technologies highlights the urgent need to improve their resilience and reliability against cyberattacks. These threats can include jamming, signal interception, spoofing and targeted attacks on cryptographic mechanisms, authentication protocols and channel control frameworks.

Statistical analysis of empirical data reveals an unprecedented increase in documented cyber incidents, highlighting the urgent need to develop and deploy advanced protective strategies against conventional cyber intrusions and radio-frequency disruptions. For example, the International Air Transport Association reported that the frequency of GPS jamming incidents increased by a factor of 1.75 in 2024, while the number of spoofing incidents surged fivefold compared to 2023. Between 2021 and 2024, the cumulative number of GPS signal disruptions, including both jamming and spoofing, increased more than twofold [3, 4]. Further corroborating analyses [5] emphasise that cases of global

navigation satellite system jamming alone increased fivefold in 2024. Experts caution that the accessibility and low cost of jamming devices enable even technically unsophisticated individuals to significantly compromise the operational integrity of GPS- and Galileo-based receivers. Additional monitoring by SeRo Systems indicates that GNSS signal distortion has been detected on an almost daily basis since mid-2023, with a clear upward trajectory across the business, transport and industrial sectors since early 2024 [6].

In response, regulatory bodies and standardisation consortia are stepping up their efforts to strengthen cybersecurity in the mobile and satellite sectors. The International Telecommunication Union is advancing recommendations addressing satellite channel security, with an emphasis on physical-layer protections and cryptographic safeguards for telemetry [7, 8]. The European Union Agency for Cybersecurity has published comprehensive directives on securing satellite systems, encompassing infrastructure hardening, access control, and cryptographic requirements [9]. The *3rd* Generation Partnership Project has established cybersecurity frameworks for 5G networks, detailing authentication mechanisms, encryption protocols and defence strategies against sophisticated attacks [10].

Further academic research highlights the urgent need to advance mobile and satellite network security in the face of cyber threats. Taken together, the increasing number of cyberattacks on mobile and satellite infrastructures, and the disruptive nature of computing technologies, make cryptographic resilience a matter of strategic urgency. Wireless infocommunication systems that are constrained by limited computational resources and lack continuous oversight are particularly susceptible.

In the current context of cyber threats, particular attention should be paid to researching encryption algorithms that can withstand quantum threats. This is due to the rapid development of quantum computing, which has the potential to break modern cryptographic protocols that are based on classical mathematical algorithms. As quantum computers are expected to become more powerful, traditional encryption methods are becoming vulnerable, posing a serious risk to the security of data and information in infocommunication networks. Therefore, developing and testing cryptographic algorithms that are resistant to contemporary cyberattacks, including quantum attacks, is crucial to ensuring the confidentiality of information and the reliability of modern communication systems in the future.

Mitigating these risks requires not only the timely migration to post-quantum communication protocols, but also a fundamental reconfiguration of network architectures and the integration of intelligent intrusion-detection frameworks. Additionally, harmonised international regulatory standards must be established.

Literature review. Researching cryptographic algorithms that are potentially resistant to quantum threats is important because of the rapid development of quantum computing, which could compromise the security of traditional cryptographic methods. In this context, algorithms such as AES-256, ChaCha20 and Kyber are attracting attention thanks to their high efficiency [11, 12].

In study [13], the authors conducted an analytical investigation to examine and systematise the characteristics of quantum theories used to develop post-quantum cryptosystems. They also compared software platforms for programming in quantum environments, providing a detailed description of the potential applications of post-quantum cryptography (PQC) algorithms. Particular attention was given to analysing the computational characteristics of the CRYSTALS-Kyber algorithm.

The authors of the research article [14] investigated the AES-256 algorithm's ability to withstand quantum cyber threats. The results showed that breaking AES-128 on classical computers is as difficult as breaking AES-256 on quantum computers.

The authors of the research [15] conducted a detailed analysis of the impact of quantum computing on network protocols. They emphasised the potential threats posed by quantum attacks and evaluated the effectiveness of PQC solutions. The conclusions drawn contribute to a deeper understanding of the influence of quantum computing on network security and provide practical recommendations for protocol designers, particularly through the application of ChaCha20 and AES algorithms at various levels of network interaction.

In the study [16], the authors proposed and investigated a hybrid, modular and adaptive protocol that integrates quantum key distribution (QKD) with PQC mechanisms. This has enabled the continuous exchange of quantum-secure keys even under challenging network conditions.

The study [17] comprehensively examined international initiatives focused on the development and standardisation of quantum-resistant cryptographic algorithms, evaluating the operational efficiency of the leading contenders. The analysis underscored that the majority of quantum-safe schemes demand greater computational resources, increased memory capacity and longer key lengths. This raised questions about their practical viability and the feasibility of implementation.

An innovative framework for standalone and hybrid PQC–AES public-key encryption schemes was proposed and investigated in [18]. The findings showed that the balance between security and computational efficiency was better than with conventional approaches. This was reinforced by a thorough security evaluation that proved the system's resilience against a wide range of attack vectors.

The research [19] provides an in-depth examination of the integration process. It focuses on the latency profiles of different PQC encapsulations during the initial handshake procedures between virtual network functions and the subsequent effects on packet size in 5G networks. The results showed only a slight increase in data consumption and a negligible extension in user equipment connection establishment time. This suggests that the security benefits of embedding PQC into 5G and future 6G core services substantially outweigh the minor performance compromises.

The authors of [20] studied a high-performance implementation of the PQC public-key encryption scheme based on the modular learning with rounding problem, optimised through the use of number theoretic transform techniques. The proposed method achieved an effective balance between security and computational efficiency. Key generation, encryption and decryption operations consumed 1,422, 1,040 and 2,647 CPU cycles respectively, corresponding to execution times of

approximately 68.9 microseconds for key generation, and 34.5 microseconds for encryption and decryption.

Based on the analysis of studies [21, 22], it has been established that particular attention should be paid to wireless access, especially in 5G and LTE, from a mobile network cybersecurity perspective. This is because wireless access is primarily conducted over open transmission environments (radio channels), which are vulnerable to jamming, eavesdropping, spoofing and man-in-the-middle attacks. Despite long-term development and widespread use, typical mobile network authentication, which relies on SIM cards and the AKA protocol, remains susceptible to cyberattacks. The main vulnerabilities of LTE and 5G networks today are compromised user identities, a lack of full end-to-end encryption, signalling-level attacks and replay attacks on authentication, as well as other related threats.

A comprehensive analysis of studies [23, 24] shows that, in terms of cybersecurity in satellite communication networks, it is important to emphasise that the current architecture is vulnerable to cyber threats at all levels. This underscores the need for the development and implementation of protection methods against cyberattacks such as jamming, spoofing, eavesdropping, man-in-the-middle attacks and modchip attacks. A detailed review presented in study [25] shows that satellite communication systems are vulnerable to attacks in all three areas: the space segment, the ground segment and the communication links between the two. The main types of these cyber threats include spoofing, DDoS attacks, eavesdropping and the compromise of control commands.

Thus, based on a critical analysis and logical synthesis of the relevant research findings on the development and implementation of cybersecurity mechanisms for infocommunication networks, including those that are potentially resistant to post-quantum threats, it can be concluded that significant progress has been made in this scientific and technical field. However, given the substantial body of high-quality results, it is clear that further development is needed. A key area in need of advancement is investigating the practical aspects of implementing efficient, potentially quantum-resistant encryption algorithms in software and hardware on devices with limited computational resources.

The main aim and objectives of the study. The primary aim of this article is a multi-criteria evaluation and analysis of the performance of encryption algorithms that could potentially resist contemporary cyberattacks, including quantum attacks. It considers their ability to be deployed on devices with limited computational resources within infocommunication networks when transmitting information.

Based on the principle of decomposing the main aim, a set of research tasks has been formulated and addressed in this study:

- to review and critically analyse the state-of-the-art of scientific and applied achievements in the development and implementation of cryptographic algorithms that are potentially resistant to quantum threats;

- to substantiate a general research framework for evaluating the performance and practicality of cryptographic algorithms for deployment on devices with limited computational resources;

- to implement selected algorithms in software for testing through computer simulation by modelling the encryption and decryption processes of information messages, including the destabilising effects of signal noise;

- to conduct a multi-criteria comparative assessment of the studied cryptographic algorithms based on key metrics, including encryption/decryption time, decoding error, cipher size and others;

- to provide practical recommendations for integrating the studied algorithms into modern infocommunication networks using portable devices with limited computational resources, to ensure the secure transmission of information messages and signals.

Therefore, the study of this article is expected to advance the understanding of cryptographic algorithms and their computational behaviour under resource-constrained environments. The developed software-based models provide practical insights for selecting and optimising cryptographic schemes for real-world deployment in infocommunication networks, with performance evaluated against key metrics.

The expected outcomes provide practical guidance on integrating potentially quantum-resistant cryptographic algorithms into infocommunication networks, ensuring secure transmission of information messages while maintaining operational efficiency.

Materials and methods. To achieve the main aim and address the defined scientific tasks, a set of methods and approaches that had been validated by international research were used. In particular, the review and systematisation of scientific and technical achievements in the field of modern cryptographic algorithms was conducted using methods of criteria-based information retrieval, comparative analysis and logical generalisation.

During the implementation, testing and validation of the selected algorithms in the Python environment, simulation modelling and computer experiment methods were used to take into account the impact of limited resources and destabilising factors, such as signal noise components. Additionally, statistical data processing and multi-criteria evaluation methods were used to analyse the performance of the cryptographic algorithms under study.

The research used the Google Colab service and the required set of Python 3.12 libraries, enabling the full computer experimentation cycle, including simulation, analysis, and graphical interpretation of results. The specific purpose of the applied libraries is as follows:

- numpy 2.0.2 was used to generate test signals, add noise, perform numerical modelling and compute key metrics;

- matplotlib 3.10.0 was used to visualise results in the form of signal dynamics plots and distribution diagrams of key metrics;

- pandas 2.3.2 was used to aggregate and provide a tabular representation of experimental results;

- cryptography 41.0.3 was used to create and simulate primitives of the AES-GCM and ChaCha20-Poly1305 cryptographic algorithms;

- pqcrypto 0.3.4 was used to create and simulate the primitives of the CRYSTALS-Kyber algorithm;

- os and time (standard Python libraries) were used to generate random nonces during encryption and to measure encryption and decryption times, respectively.

In the simulation, an in-phase/quadrature (I/Q) base signal model corresponding to real digital signals

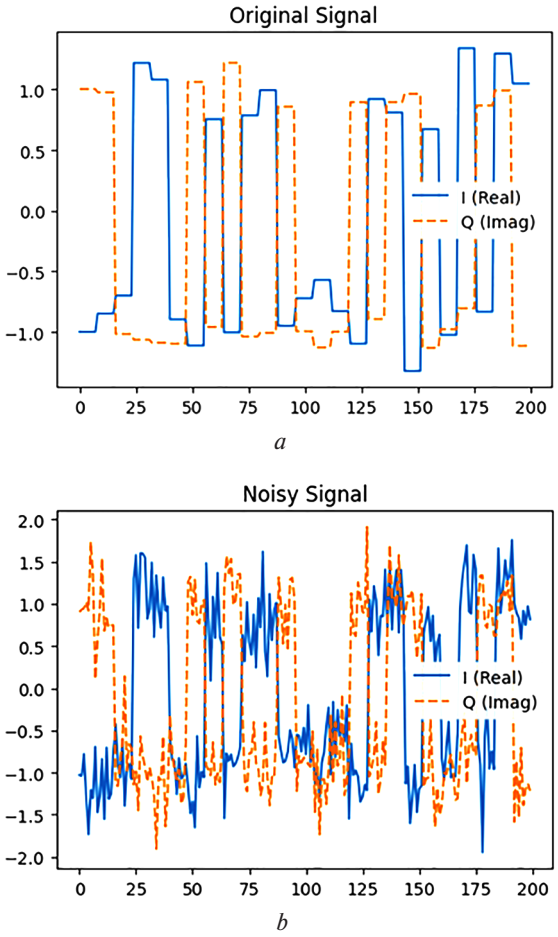


Fig. 1. Graphical interpretation of test signal fragments: a – original I/Q signal; b – noisy I/Q signal (SNR = = 10 dB)

in infocommunication networks was generated. The test signal parameters were as follows: number of symbols – 1,000; samples per symbol – 8; synthetic symbols – Binary Phase Shift Keying (BPSK) on I and Q: ±1; symbol rate – 1,000 symbols/s; sampling frequency – 8 kHz.

To account for real transmission conditions in infocommunication system channels (e.g. fluctuations and interference), a noise component was added to the generated signal with the following characteristics: noise type – Additive White Gaussian Noise (AWGN); mean value – 0; variance depends on the selected signal-to-noise ratio (SNR) within the range of 5–20 dB.

An example of the visualisation of the original and noisy (SNR = 10 dB) test signals is shown in Fig. 1.

Additionally, a procedure for quantising the I/Q signal into bytes was implemented during the creation of the computer model of the studied process to increase its adequacy to real cryptographic processes. Realistic delays of between 10 and 20 milliseconds per kilobyte of data were also introduced, reflecting the actual computational capabilities of typical microcomputer devices.

The baseline cryptographic algorithms selected for this study were AES-256, ChaCha20 and Kyber (Kyber512, Kyber768, Kyber1024). These were chosen based on their a priori performance metrics and their potential to resist quantum cyber threats. The main characteristics of the algorithms used in the simulation studies are given in Table 1.

The key metrics used to evaluate the performance of the studied algorithms are given in Table 2.

Based on the above, the research methodology of this article has been substantiated through the use of computer experiments. The main stages of the proposed methodology, along with details of the corresponding research objects/processes and expected results, are shown in Fig. 2.

Thus, the proposed methodology facilitates a comprehensive computer-based evaluation of the performance of modern cryptographic algorithms for cyber protection of infocommunication networks, considering quantum threats and computational resource limitations. Using a synthetic harmonic signal with a noise model that is characteristic of real wireless channels enables the resilience of algorithms to recovery errors to be assessed, as well as their time efficiency in relation to the computational capabilities of microcomputer devices. It also allows the impact on the volume of transmitted data to be determined, which is critical when designing cyber-protected infocommunication systems.

Results. The main research results were obtained using the above-substantiated methodology, which involved investigating the performance indicators of cryptographic algorithms through computer experiments.

The first series of experiments examined the combined impact of SNR levels and signal length on the accuracy of signal recovery after encryption for different cryptographic algorithms, as shown in Fig. 3.

The following findings were established based on the analysis of the graphical dependencies presented in Fig. 3:

- all of the studied algorithms are characterised by a high degree of accuracy in signal recovery: for the AES

Table 1

Main characteristics of the cryptographic algorithms under research

Algorithm	Settings	Functional characteristics
AES-256	Mode: Galois/Counter Mode (GCM), key: 256 bits, block: 128 bits	Partitioning the input information message into 128-bit blocks, followed by encryption of each block using AES with 14 rounds, use of a counter to generate the key stream and universal hashing over a Galois field for authentication
ChaCha20	Mode: ChaCha20 combined with Poly1305, key: 256 bits	Generation of a pseudorandom stream with 20 rounds, encryption of the message using XOR with the generated stream and use of Poly1305 for message authentication
Kyber (Kyber512, Kyber768, Kyber1024)	Post-quantum lattice-based cryptographic algorithm, keys vary depending on parameters (512, 768, 1024)	The learning with errors procedure on lattices is applied, public and private keys are generated based on LWE, encryption is performed using the public key and decryption is performed using the private key, the signal is encrypted using AES-GCM with a key derived through Kyber

Table 2

Metrics used to evaluate the effectiveness of the cryptographic algorithms under research

Metrics	Formal description
Mean squared error (MSE) was used to assess signal accuracy after encryption/decryption procedures	$MSE = \frac{1}{N}\sum_{i=1}^{N}\left\|x_i - \hat{x}_i\right\|^2$, where MSE is the mean square error; N is the number of signal readings; x_i are the readings of the original (I/Q) signal; $\hat{x}_i$ are the values restored after decoding, $\|...\|$ is the modulus of a complex number
Encryption/decryption time was used to assess the computational complexity of the algorithms	$\begin{cases} T_{enc} = t_{end,enc} - t_{start,enc} \\ T_{dec} = t_{end,dec} - t_{start,dec} \end{cases}$, where T_{enc}, T_{dec} are the encryption and decryption time intervals, respectively; $t_{end,enc}$, $t_{start,enc}$, $t_{end,dec}$, $t_{start,dec}$ are the end and start timestamps of the encryption and decryption procedures, respectively, taking into account the actual delays of computational devices
Ciphertext size was used to evaluate coding efficiency	$S_{cipher} = \text{len}(C)$, where S_{cipher} is the ciphertext size (in bytes); C is the ciphertext

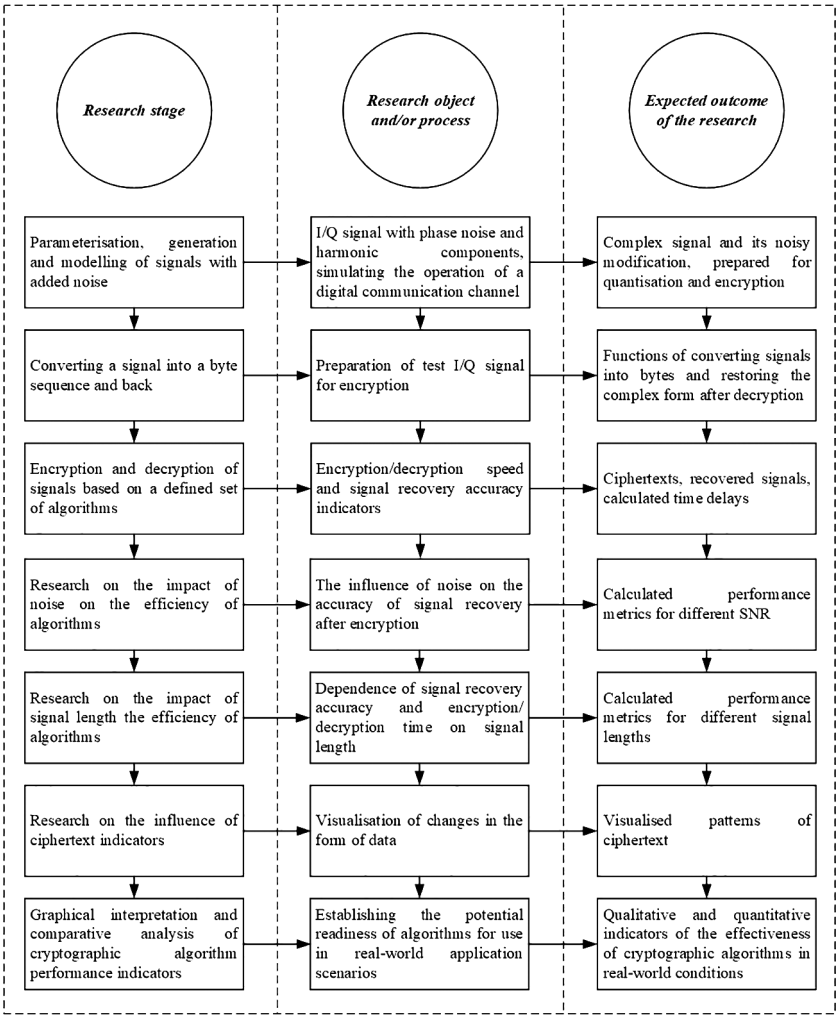
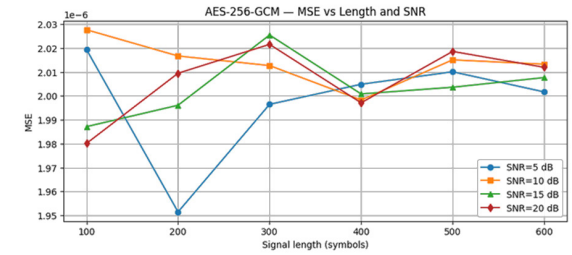


Fig. 2. Proposed methodology for researching the effectiveness of cryptographic algorithms

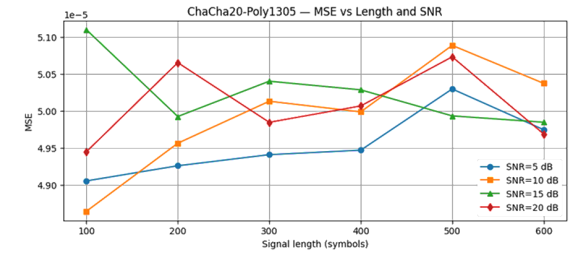
algorithm, the MSE ranges from $1.95 \cdot 10^{-6}$ to $2.03 \cdot 10^{-6}$; for the ChaCha20 algorithm, it ranges from $4.86 \cdot 10^{-5}$ to $5.12 \cdot 10^{-5}$; and for the family of Kyber algorithms, it ranges from $7.68 \cdot 10^{-4}$ to $8.32 \cdot 10^{-4}$. These values are influenced by the simulated errors incorporated into the model, reflecting the algorithms' inherent characteristics during signal quantisation and conversion;

- anomalous MSE values (i.e., an increase in MSE with increasing SNR) can be explained by the random nature of the generated noise in the model, as well as by the phase disturbances and harmonic interferences included in the software implementation. These factors enhance the adequacy of the model for real-world application scenarios. Notably, the Kyber768 and Kyber1024 algorithms demonstrated greater resilience to such disturbances and interferences;

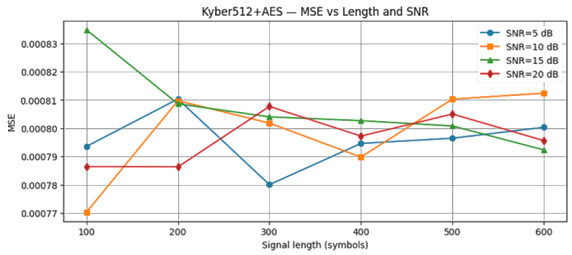
- the signal length parameter (i.e., the number of discrete symbols after upsampling), which was found to be in the range of 100 to 600, was discovered to have only a minor impact on the accuracy of signal recovery.



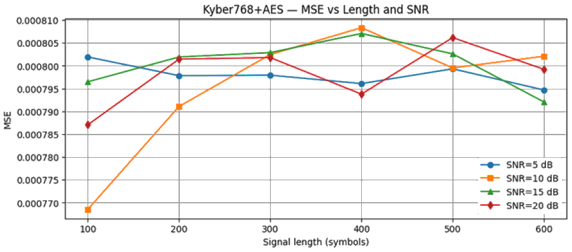
a



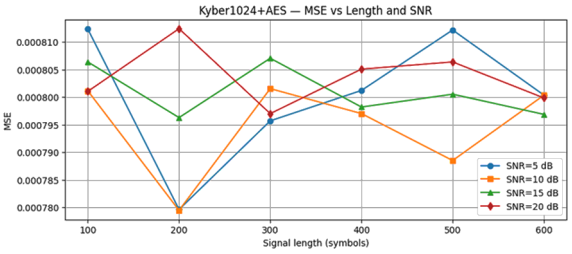
b



c



d



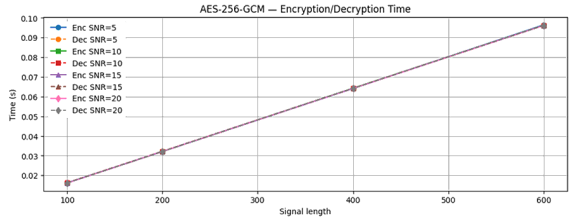
e

Fig. 3. Dependence of signal recovery accuracy on SNR and signal length:

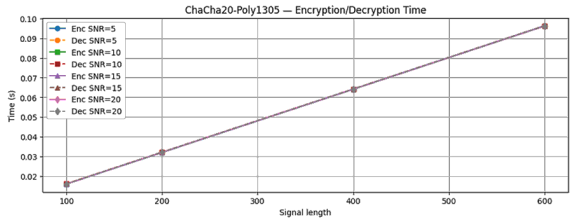
a – AES-256; b – ChaCha20; c – Kyber512+AES; d – Kyber768+AES; e – Kyber1024+AES

It is also worth noting that, in practical application cases [26, 27], the obtained dependencies (Fig. 3) can, in most instances, be used to analyse the qualitative characteristics of the suitability of the corresponding cryptographic algorithms. This is because the simulation model considers error components arising from stochastic interferences, thermal noise, phase disturbances, harmonic distortions, upsampling and discretisation approximately. It is also significantly determined by the technical and functional characteristics of the devices on which it is deployed.

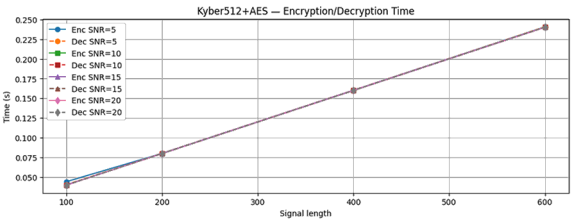
The second series of experiments was devoted to establishing the dependencies of the encryption/decryption time indicators for signals using the investigated cryptographic algorithms. This was done by taking into account the SNR levels, the length of the signals and the actual computational capabilities of the microcomputer devices, as shown in Fig. 4.



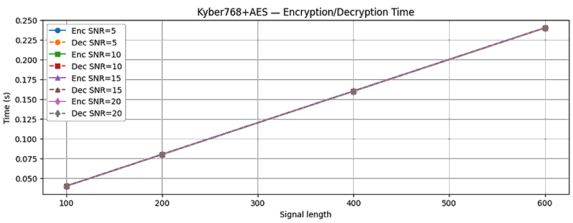
a



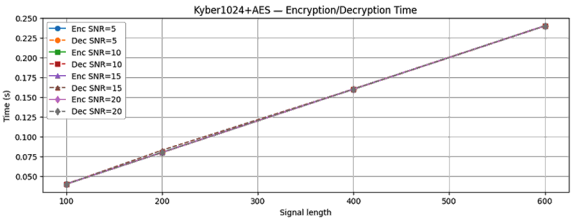
b



c



d



e

Fig. 4. Dependence of signal encryption/decryption time on SNR and signal length:

a – AES-256; b – ChaCha20; c – Kyber512+AES; d – Kyber768+AES; e – Kyber1024+AES

Based on the analysis of the graphical dependencies presented in Fig. 4, the following findings were established:

- the dependence of encryption/decryption time on signal length for the analysed types of cryptographic algorithms is linear;

- the SNR level does not affect the time characteristics of the encryption/decryption procedures, which confirms the practical principles of implementing these algorithms. As the cipher operates on data bytes and is not sensitive to the noise component of the signal, it can be stated that the implemented model accurately reflects the actual sequence of signal normalisation, quantisation and byte stream formation and alignment;

- the AES-256 and ChaCha20 algorithms are approximately 2.5 times faster than Kyber. This is consistent with the computational features of these algorithms, given that Kyber requires the execution of a significant number of polynomial and modular operations, as well as the generation of pseudorandom values.

The final stage of the computer experiment focused on investigating ciphertext characteristics through the graphical interpretation of data transformations, as shown in Fig. 5. Here, the abscissa axis represents the ciphertext byte index. In contrast, the ordinate axis represents the corresponding ciphertext rows.

The analysis of the graphical interpretation in the form of patterns presented in Fig. 5 demonstrates a chaotic distribution of values, confirming the robustness of the investigated encryption algorithms.

A multi-criteria evaluation of the performance of the AES, ChaCha20 and Kyber cryptographic algorithms was carried out during the processing of a composite digital signal under varying noise levels (SNR from 5 to 20 dB) and with different signal lengths (from 100 to 600 discrete symbols), as a result of the series of computer experiments conducted. Ciphertext visualisation revealed that all algorithms produced substantial data dispersion, concealing the structure of the original signal and confirming their strong cryptographic resilience.

In terms of signal recovery accuracy after decryption, the symmetric algorithms AES-256-GCM and ChaCha20-Poly1305 demonstrated almost identical precision and low error rates. In contrast, the simulated Kyber algorithms exhibited slightly higher MSE values. This reflects the impact of the additional computational operations and transformations involved in generating a symmetric key from the public-key stage. In terms of processing time, the symmetric algorithms were significantly faster than Kyber by a factor of 2.5, which is consistent with realistic expectations for devices with limited resources based on typical microcomputer platforms.

Discussions, limitations and prospect research directions. The research results showed that using symmetric cryptographic algorithms, such as AES and ChaCha20, ensures high computational efficiency with minimal loss of accuracy when recovering digital (I/Q) signals after encryption and decryption. This makes them particularly well-suited to deployment in infocommunication systems based on autonomous microcomputer devices with limited computational resources. At the same time, the Kyber family of algorithms are capable of countering potential threats from quantum computing due to their architecture and provide an enhanced level of cryptographic robustness. However, they exhibit substantially higher time costs and relatively larger mean squared error values. This clearly indicates a fundamental trade-off between performance and the level of data protection in modern infocommunication systems operating under real-world conditions.

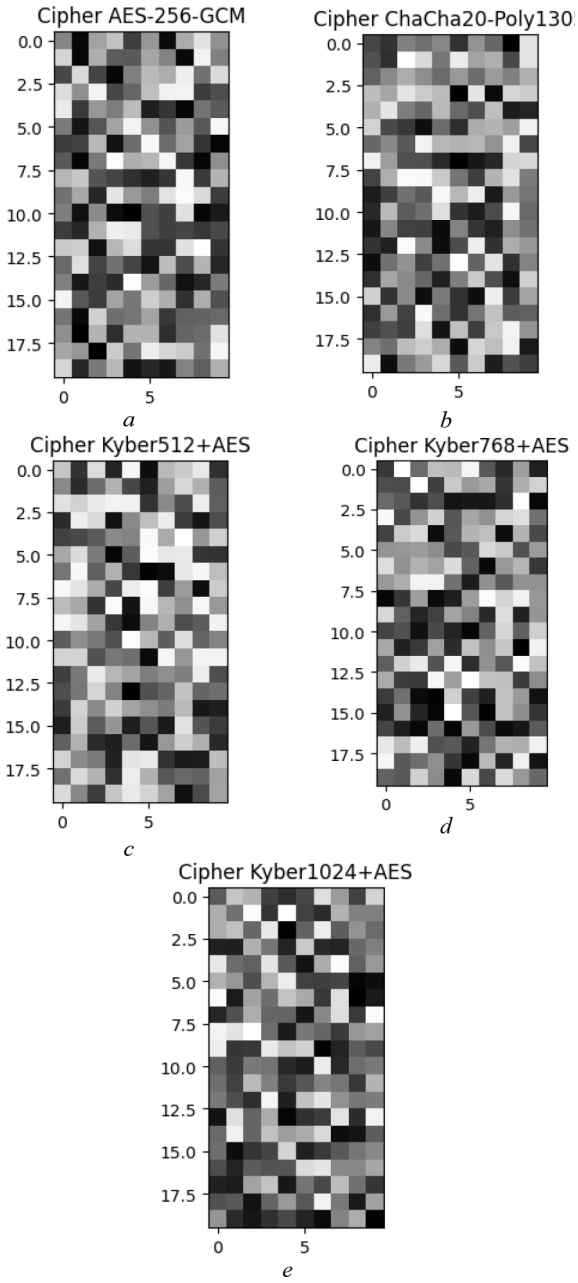


Fig. 5. Random data encryption patterns:
a – AES-256; b – ChaCha20; c – Kyber512+AES; d – Kyber768+AES; e – Kyber1024+AES

It should be noted, however, that the results obtained are characterised by certain limitations. Firstly, the research was conducted using computer experiment methods in a software environment, which prevented a full consideration and analysis of the hardware limitations of specialised microcomputing devices. Secondly, while the model took into account additive and phase interference, it only partially considered more complex factors affecting communication channels, such as the non-stationarity of processes and signals, in the formalised description of the studied infocommunication process.

Thus, the above-mentioned limitations highlight the prospects for further advancement of the obtained results in the following directions:

- expanding the experimental base through hardware testing of algorithms on real microcomputer devices in practical scenarios of infocommunication networks;
- developing hybrid protocols that combine the high performance of symmetric algorithms with post-quantum protection mechanisms to enhance cybersecurity without causing critical reductions in computational efficiency;
- investigating the technical and functional capabilities of cryptographic algorithms when subjected to various types of attack, such as active interference and spoofing;
- analysing the potential of applying machine learning and artificial intelligence methods to optimise the parameters of cryptographic algorithms and predict their resilience in dynamic environments.

Therefore, based on the foregoing, it can be concluded that the results obtained are significant in establishing the technical, technological, and methodological foundations for applying modern and post-quantum cryptographic algorithms in resource-constrained infocommunication systems. However, further comprehensive research is required to ensure their effective integration into practical deployment scenarios.

Conclusions. This article presents a simulation-based study of the performance of modern cryptographic algorithms, including AES, ChaCha20 and the Kyber family (used in conjunction with AES), when applied to resource-constrained infocommunication systems. The results obtained allow the following general conclusions to be drawn:

- the symmetric algorithms AES-256-GCM and ChaCha20-Poly1305 demonstrated the highest accuracy in signal recovery after encryption and decryption, indicating their high fidelity in data reconstruction. On average, the MSE for these algorithms remained in the range of $1.95 \cdot 10^{-6}$ to $5.12 \cdot 10^{-5}$;
- the time characteristics revealed the advantage of symmetric algorithms: the average encryption and decryption times were approximately 2.5 times lower than those of the Kyber family of algorithms. This confirms their suitability for deployment on devices with limited computational resources and stringent latency requirements;
- the experiments confirmed the existence of a trade-off between performance and security: symmetric algorithms are optimal for scenarios with critical processing speed requirements, whereas Kyber provides higher security reliability but demands greater computational resources;
- a qualitative analysis of the visualisations of signals and ciphertext validated the proposed simulation model, which enables the assessment of both computational and information and functional characteristics of cryptographic algorithms.

Thus, the developed simulation model has proven its suitability for investigating cryptographic algorithms in resource-constrained environments. The obtained quantitative and qualitative results can be used to further enhance information security protocols and select optimal algorithms based on performance and security requirements.

Acknowledgements. *The article was prepared within the framework of the project 2025.06/0047 "Information technologies of cryptographic protection and data authentication for mobile and satellite communication systems". This project received funding from the National Research Foundation of Ukraine.*

References.

1. Kashtan, V. Yu., Hnatushenko, V. V., Laktionov, I. S., & Diachenko, H. H. (2024). Intelligent Sentinel satellite image processing technology for land cover mapping. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (5), 143-150. https://doi.org/10.33271/nvngu/2024-5/143

2. Laktionov, I., Diachenko, G., Koval, V., & Yevstratiev, M. (2023). Computer-Oriented Model for Network Aggregation of Measurement Data in IoT Monitoring of Soil and Climatic Parameters of Agricultural Crop Production Enterprises. *Baltic Journal of Modern Computing*, *11*(3), 500-522. https://doi.org/10.22364/bjmc.2023.11.3.09

3. *IATA: IATA Releases 2024 Safety Report* (n.d.). Retrieved from https://www.iata.org/en/pressroom/2025-releases/2025-02-26-01/

4. *IATA: EASA and IATA Publish Comprehensive Plan to Mitigate the Risks of GNSS Interference* (n.d.). Retrieved from https://www.iata.org/en/pressroom/2025-releases/2025-06-18-01/

5. Blatnik, A., & Batagelj, B. (2025). Evaluating GNSS Receiver Resilience: A Study on Simulation Environment Repeatability. *Electronics*, *14*(9), 1797. https://doi.org/10.3390/electronics14091797

6. *SeRo Systems: Detecting and Monitoring GPS Jamming and Spoofing in the Airspace* (n.d.). Retrieved from https://www.sero-systems.de/case-studies/tracking-the-threat?

7. *ITU: SG17: Security. Available online* (n.d.). Retrieved from https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

8. *ITU: X.1303: Common alerting protocol* (n.d.). Retrieved from https://www.itu.int/rec/T-REC-X.1303-200709-I/en

9. *ENISA: State of cybersecurity in the EU* (n.d.). Retrieved from https://www.enisa.europa.eu/

10. *3GPP: A Global Initiative* (n.d.). Retrieved from https://www.3gpp.org/ftp//Specs/archive/33_series/33.501/

11. Szymanski, T. H. (2024). A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced CyberSecurity for Critical Infrastructures. *Information*, *15*(4), 173. https://doi.org/10.3390/info15040173

12. Ehsan, M. A., Alayed, W., Rehman, A. U., Hassan, W.U., & Zeeshan, A. (2025). Post-Quantum KEMs for IoT: A Study of Kyber and NTRU. *Symmetry*, *17*(6), 881. https://doi.org/10.3390/sym17060881

13. Alkurdi, Y., Abu Al-Haija, Q., & Al Fayoumi, M. (2024). Review of quantum theories for the design of post-quantum crypto systems: CRYSTALS-Kyber as a case study. *IET Conference Proceedings*, 610-618. https://doi.org/10.1049/icp.2025.0860

14. Rao, S. K., Mahto, D., & Yadav, D. K. (2017). The AES-256 Cryptosystem Resists Quantum Attacks. *International Journal of Advanced Research in Computer Science*, *8*(3), 404-408. https://doi.org/10.26483/ijarcs.v8i3.3025

15. Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, *142*, 103883. https://doi.org/10.1016/j.cose.2024.103883

16. Santo, A. D., Tiberti, W., & Cassioli, D. (2025). An Adaptive Dual-Stack QKD-PQC Framework for Secure and Reliable Inter-Site Communication. *Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)*, 1-12. Retrieved from https://ceur-ws.org/Vol-3962/paper56.pdf

17. Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array*, *15*, 100242. https://doi.org/10.1016/j.array.2022.100242

18. Ojetunde, B., Kurihara, T., Yano, K., Sakano, T., & Yokoyama, H. (2025). A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication. *Network*, *5*(2), 20. https://doi.org/10.3390/network5020020

19. Scalise, P., Garcia, R., Boeding, M., Hempel, M., & Sharif, H. (2024). An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics*, *13*(21), 4258. https://doi.org/10.3390/electronics13214258

20. Pandit, A. A., & Mishra, A. (2024). Efficient implementation of post quantum MLWR-based PKE scheme using NTT. *Computers and Electrical Engineering*, *118*(A), 1-18. https://doi.org/10.1016/j.compeleceng.2024.109358

21. Winter, A., Morrison, A., Hasler, O., & Sokolova, N. (2025). Exploitation of 5G, LTE, and Automatic Identification System Signals for Fallback Unmanned Aerial Vehicle Navigation. *Engineering Proceedings*, *88*(1), 49. https://doi.org/10.3390/engproc2025088049
22. Boodai, J., Alqahtani, A., & Frikha, M. (2023). Review of Physical Layer Security in 5G Wireless Networks. *Applied Sciences*, *13*(12), 7277. https://doi.org/10.3390/app13127277
23. Kang, M., Park, S., & Lee, Y. (2024). A Survey on Satellite Communication System Security. *Sensors*, *24*(9), 2897. https://doi.org/10.3390/s24092897
24. Abdelsalam, N., Al-Kuwari, S., & Erbad, A. (2025). Physical layer security in satellite communication: State-of-the-art and open problems. *IET Communications*, *19*, e12830. https://doi.org/10.1049/cmu2.12830
25. Salim, S., Moustafa, N., & Reisslein, M. (2025). Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *IEEE Communications Surveys & Tutorials*, *27*(1), 372-425. https://doi.org/10.1109/COMST.2024.3408277
26. Laktionov, I. S., Vovna, O. V., Kabanets, M. M., Sheina, H. O., & Getman, I. A. (2021). Information model of the computer-integrated technology for wireless monitoring of the state of microclimate of industrial agricultural greenhouses. *Instrumentation Mesure Metrologie*, *20*(6), 289-300. https://doi.org/10.18280/i2m.200601
27. Hnatushenko, V., Kogut, P., & Uvarov, M. (2022). Variational approach for rigid co-registration of optical/SAR satellite images in agricultural areas. *Journal of Computational and Applied Mathematics*, *400*, 113742. https://doi/org.10.1016/j.cam.2021.113742

Симуляційна оцінка криптографічних алгоритмів для застосування в інфокомунікаційних мережах із обмеженими ресурсами

І. С. Лактіонов, В. В. Гнатушенко, І. М. Удовик, В. І. Олевський*

Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна
* Автор-кореспондент e-mail: Hnatushenko.V.V@nmu.one

Мета. Багатокритеріальна оцінка й аналіз ефективності алгоритмів шифрування, що можуть бути потенційно стійкими до сучасних кібератак, у тому числі квантових. Цей аналіз проводиться з урахуванням їхньої здатності до розгортання на пристроях із обмеженими обчислювальними ресурсами в межах інфокомунікаційних мереж під час передавання інформаційних повідомлень.

Методика. Програмна реалізація, тестування й валідація обраних криптографічних алгоритмів мовою Python з урахуванням впливу обмежених ресурсів і дестабілізуючих факторів, зокрема шумової складової сигналів на основі методів імітаційного моделювання й комп'ютерного експерименту. Аналіз ефективності досліджуваних криптографічних алгоритмів методами статистичної обробки даних і багатокритеріальної оцінки.

Результати. Визначено, що симетричні алгоритми AES-256-GCM і ChaCha20-Poly1305 продемонстрували найвищі показники точності під час відновлення сигналу після шифрування й дешифрування, що свідчить про їхню високу точність у процесі відтворенні даних (MSE змінюється від $1{,}95 \cdot 10^{-6}$ до $5{,}12 \cdot 10^{-5}$). Встановлено, що часові характеристики шифрування й дешифрування I/Q сигналу із використанням симетричних алгоритмів приблизно у 2,5 рази є меншими, ніж у алгоритмів сімейства Kyber. Комп'ютерні експерименти підтвердили існування компромісу між швидкодією й рівнем безпеки. Встановлено, що симетричні алгоритми є оптимальними для сценаріїв із критичними вимогами до швидкості обробки, тоді як алгоритми сімейства Kyber забезпечують вищу надійність захисту, але потребують більше ресурсів. Доведена коректність запропонованої комп'ютерної моделі, що дозволяє оцінювати як обчислювальні, так і інформаційно-функціональні характеристики криптографічних алгоритмів.

Наукова новизна. Встановлені закономірності дестабілізуючого впливу показників відношення сигнал/шум і довжини сигналу на точність відновлення цифрового (I/Q) сигналу після шифрування для різних криптографічних алгоритмів (AES, ChaCha20 і сімейства Kyber) у контексті їх використання в інфокомунікаційних мережах із обмеженими ресурсами.

Практична значимість. Результати досліджень із реалізації комп'ютерної моделі довели її придатність для дослідження криптографічних алгоритмів у середовищах з обмеженими ресурсами. Обґрунтована можливість її використання під час подальшого вдосконалення протоколів захисту інформації та вибору оптимальних алгоритмів залежно від вимог до швидкодії й рівня безпеки.

Ключові слова: *криптографічний алгоритм, сигнал, шум, шифротекст, інфокомунікаційна мережа, точність, модель*

The manuscript was submitted 01.08.25.