IRSTI 20.23.21 https://doi.org/10.26577/jpcsit202547

Laula Zhumabayeva*, Maksym Orynbassar, Bekezhan Zhumazhan, Meruert Akberdiyeva

Sh. Yessenov Caspian University of Technology and Engineering, Aktau, Kazakhstan
*e-mail: laula1.zhumabayeva@yu.edu.kz

SIMULATION MODELING OF DATA INTEGRITY VIOLATIONS IN INTELLIGENT SOCIAL SYSTEMS

Abstract. This article examines modern approaches to ensuring the integrity and confidentiality of electronic data through the use of post-quantum cryptographic algorithms kyber and dilithium. In the context of the rapid development of quantum computing technologies, traditional cryptographic methods such as rsa and elliptic curve cryptography are expected to lose their resistance, creating significant threats to the security of information systems. These threats affect government digital platforms, financial services, educational ecosystems, and intelligent social systems that require a high level of digital trust. The objective of the study is to analyze the application of the kyber algorithm for encryption and key exchange and the dilithium algorithm for digital signatures as post-quantum solutions recommended by nist for data protection in the post-quantum era. The article considers principles for integrating these algorithms into trusted electronic system infrastructures, including electronic voting, state registries, digital document management systems, and cloud storage platforms. The results demonstrate that the combined use of kyber and dilithium significantly enhances resistance to quantum attacks, ensures the integrity of electronic transactions, and provides reliable authentication and data verification throughout the entire data life cycle. The study concludes that post-quantum cryptographic algorithms represent a key direction in the development of secure digital ecosystems and the formation of a new paradigm of digital trust. This article examines modern approaches to ensuring the integrity and confidentiality of electronic data through the use of post-quantum cryptographic algorithms kyber and dilithium. In the context of the rapid development of quantum computing technologies, traditional cryptographic methods such as rsa and elliptic curve cryptography are expected to lose their resistance, creating significant threats to the security of information systems. These threats affect government digital platforms, financial services, educational ecosystems, and intelligent social systems that require a high level of digital trust. The objective of the study is to analyze the application of the kyber algorithm for encryption and key exchange and the dilithium algorithm for digital signatures as post-quantum solutions recommended by nist for data protection in the post-quantum era. The article considers principles for integrating these algorithms into trusted electronic system infrastructures, including electronic voting, state registries, digital document management systems, and cloud storage platforms. The results demonstrate that the combined use of kyber and dilithium significantly enhances resistance to quantum attacks, ensures the integrity of electronic transactions, and provides reliable authentication and data verification throughout the entire data life cycle. The study concludes that post-quantum cryptographic algorithms represent a key direction in the development of secure digital ecosystems and the formation of a new paradigm of digital trust.

Keywords: intelligent social systems, simulation modeling, data integrity, cognitive attacks, information distortions, agent-based modeling.

1. Introduction

The contemporary information landscape is marked by the rapid growth of data volumes, the large-scale digitalization of public and commercial services, and the active adoption of artificial intelligence (AI) technologies and cloud solutions in management and communication processes. In this context, ensuring the security, integrity, and confidentiality of electronic data has become one of the key priorities of the digital society.

Systems that process mission-critical information–government digital platforms (eGov, Gosuslugi), electronic registries, as well as educational and financial ecosystems–are of particular importance. Violations of data integrity in such systems can lead to serious consequences: the erosion of user trust, the distortion of electronic transaction results, and the leakage of personal information. Consequently, the problem of data protection extends beyond traditional cryptographic approaches and demands a transition to new methods resilient to future threats–first and foremost, to quantum attacks.

The development of quantum computing poses a fundamental challenge to existing encryption algorithms (RSA, ECC), since quantum computers can efficiently solve the factoring and discrete logarithm problems on which the security of classical schemes is based. In response, a new field–post-quantum cryptography (PQC)–has emerged, focused on designing algorithms that remain secure even in the presence of quantum computing technologies.

Among the most promising solutions in post-quantum cryptography are the Kyber and Dilithium algorithms, recommended by the U.S. National Institute of Standards and Technology (NIST) as international standards for data protection in the post-quantum era. Kyber is used for key establishment (key encapsulation) and securing communication channels, while Dilithium is intended for generating and verifying digital signatures, ensuring the authenticity and immutability of electronic documents.

The use of Kyber and Dilithium enables the construction of secure architectures for electronic systems that provide not only data encryption but also verifiability of integrity, authenticity, and provenance. This, in turn, opens opportunities for developing trusted digital infrastructures–such as electronic voting systems, government registries, cloud storage, and corporate databases.

Accordingly, this study focuses on analyzing and deploying the post-quantum cryptographic algorithms Kyber and Dilithium to protect the integrity and confidentiality of electronic data. Particular attention is paid to the architectural integration of these algorithms into modern digital ecosystems, to modeling their resilience to quantum attacks, and to assessing the effectiveness of their application in building next-generation systems of digital trust.

2. Materials and Methods

The problem of ensuring the integrity and confidentiality of electronic data occupies a central place in contemporary digital science and information security. The development of quantum computing has put traditional cryptographic protection methods (RSA, ECC)–whose effectiveness relies on the computational hardness of integer factorization and discrete logarithms–at risk. The emergence of quantum algorithms such as Shor's algorithm enables these problems to be solved efficiently, creating the need to transition to new cryptographic schemes resistant to quantum attacks (Bernstein et al., 2017; Chen et al., 2016).

According to research in post-quantum cryptography [1], new security standards must ensure long-term resilience against threats arising from advances in quantum technologies. Since 2016, the U.S. National Institute of Standards and Technology (NIST) has been conducting a global initiative to standardize post-quantum algorithms. As a result of a multi-stage selection process, in 2022 the Kyber algorithm (for encryption and key exchange) and Dilithium (for digital signatures) were chosen for standardization, demonstrating high efficiency, robustness, and performance [2].

Kyber, based on lattice problems [3], provides a high level of protection for communication channels and secure key exchange even in the presence of a quantum adversary [4]. In turn, Dilithium–built on similar mathematical foundations–enables digital signing and verification of data authenticity, preserving immutability and provable provenance [5]. These algorithms offer not only cryptographic strength but also compatibility with modern computing architectures, making them suitable for integration into government, corporate, and educational systems.

International studies show that deploying post-quantum methods in electronic voting systems, financial platforms, and cloud storage increases user trust and enhances infrastructure resilience to hacking threats. Particular attention is paid to hybrid security models that combine classical and post-quantum approaches, enabling a smooth transition to the new cryptographic paradigm without a complete system overhaul [6].

In the domestic scholarly literature, the issue of post-quantum security is also reflected. Researchers emphasize the need to adapt NIST international standards to national requirements and to integrate post-quantum algorithms into public services, especially in the context of protecting critical data and personal registries. They also underscore the importance of developing models of digital trust and legal mechanisms governing encrypted information in the post-quantum era.

Recent publications [7] focus on the performance and optimization challenges of post-quantum algorithms when deployed in resource-constrained environments (e.g., IoT and edge services). For such scenarios, hardware-optimized implementations of Kyber and Dilithium are proposed, demonstrating a balance among speed, reliability, and security.

Thus, the analysis of scholarly sources highlights several key research directions in post-quantum data protection:

- development and standardization of next-generation cryptographic algorithms (Kyber, Dilithium, Falcon, SPHINCS+);
- investigation of the resilience of post-quantum schemes to practical attacks and their performance in real-world environments;
- integration of post-quantum cryptography into digital ecosystems–from electronic document management to cloud platforms;
- formation of digital-trust architectures that combine post-quantum cryptography, machine learning, and intelligent monitoring systems.

Overall, the literature points to a global transition to a new stage in cryptography: from defending against classical computational threats to building quantum-resilient ecosystems. The deployment of Kyber and Dilithium plays a key role in shaping the infrastructure of digital trust and ensuring the integrity of electronic data in the post-quantum era.

2.1 Methodology and Research Methods

The methodological basis of this study rests on the concept of quantum-resilient protection of electronic data through the use of the post-quantum cryptographic algorithms Kyber and Dilithium. The aim is to evaluate the effectiveness of these algorithms in ensuring integrity and confidentiality under threat models associated with advances in quantum computing.

The research employed systemic and experimental-analytical approaches that included designing the architecture of a secured digital system, implementing and testing cryptographic modules, and analyzing the system's resilience to potential quantum and classical attacks. The methodology followed a three-tier modeling principle that separates the system into cryptographic, infrastructure, and application layers. At the cryptographic layer, Kyber and Dilithium were implemented for encryption, key establishment, and digital signatures. The infrastructure layer modeled network connections, data transmission channels, and server nodes, while the application layer captured protected data-exchange and storage scenarios such as electronic voting, government registries, and cloud systems [8].

Computational experiments were implemented using Python and SageMath, along with specialized post-quantum cryptography libraries: pypqc for Kyber and pqcrypto for Dilithium. Performance analysis employed NumPy, Pandas, and Matplotlib. For security evaluation, the Open Quantum Safe (OQS) framework and liboqs were used to provide support for post-quantum algorithms and enable experiments under conditions close to real-world deployments.

In the first stage, a test data-transmission protocol was developed that included key generation, encryption, signing, and authenticity verification. For an objective efficiency comparison, tests were conducted against classical cryptosystems RSA and ECC. In the next stage, quantum attacks aimed at undermining the resilience of classical algorithms were simulated. The primary metrics were Encryption Success Rate, an Integrity Index capturing post-transmission invariance, and a Quantum Resistance Score reflecting robustness to simulated quantum compromise.

Additionally, computational efficiency was assessed using parameters such as key-generation time, encryption/decryption throughput, signature length, key size, and compute-resource load. Experiments were run both in a local environment and in a client–server network configuration, allowing practical behavior to be evaluated under realistic encrypted data-exchange conditions. Comparative results were derived via performance coefficients and security-gain factors, indicating that Kyber and Dilithium achieved a 70–80% increase in quantum resilience with no more than a 25–30% increase in computational cost.

To verify applicability, an experimental model of a protected electronic-interaction infrastructure was built. It comprised a server module implementing Kyber and Dilithium, a client interface performing encryption and signing operations, a database with integrity-verification capabilities, and an audit module logging all exchange operations. During attack simulations, scenarios included message interception, signature substitution, and public-key analysis. The results showed that the probability of successful compromise with Kyber and Dilithium did not exceed 0.001%, whereas under an analogous RSA-based setup it was about 4.3% [9].

The findings confirm the hypothesis of high effectiveness of post-quantum algorithms in ensuring the integrity and confidentiality of electronic data. Kyber demonstrated an optimal balance between encryption speed and attack resilience, while Dilithium provided reliable authentication and protection against data tampering. Their combined use enabled a comprehensive quantum-resilient architecture of digital trust that maintained stable information flows under potential quantum threats.

The methodological novelty lies in unifying practical cryptographic testing, attack modeling, and performance analysis to deliver a holistic assessment of Kyber and Dilithium in modern digital ecosystems [10]. The results can inform the design of secured government information systems, electronic document workflows, electronic voting systems, and cloud data repositories that require a high level of trust and resilience to quantum-computing threats.

3. Results and Discussion

The primary challenge in organizing the experiment was that the simulated intelligent social system represented a dynamic environment with high parameter variability. In the initial stages of modeling, difficulties arose related to configuring agent behavioral parameters and calibrating trust coefficients, which required substantial computational resources and time to train neural network models.

Initial modeling showed that, in the baseline architecture of the intelligent social system, the data integrity level decreased by 25–30% under the influence of external cognitive attacks and disinformation flows. A high sensitivity to the density of social ties was observed: the greater the number of agent interactions, the faster distorted messages propagated [11]. This effect is analogous to viral diffusion, confirming the hypothesis of a nonlinear relationship between user engagement and the rate of loss of data veracity.

After the deployment of machine-learning-based corrective mechanisms, a stable improvement in data integrity indicators was observed. The experimental model employing autoencoders and graph neural networks demonstrated, on average, an 18% increase in the Integrity Rate compared to the control model [12]. The Resilience Index rose by 22%, while the Distortion Propagation Factor nearly halved. “Figure 1. Dynamics of the Integrity Index” presents a visualization of the three-layer simulation architecture, showing the relationships among agents, data flows, and infrastructure nodes. The bottom layer depicts user activity and the density of their social ties, the middle layer the dynamics of information flows, and the top layer the network structure that ensures data transmission and storage.

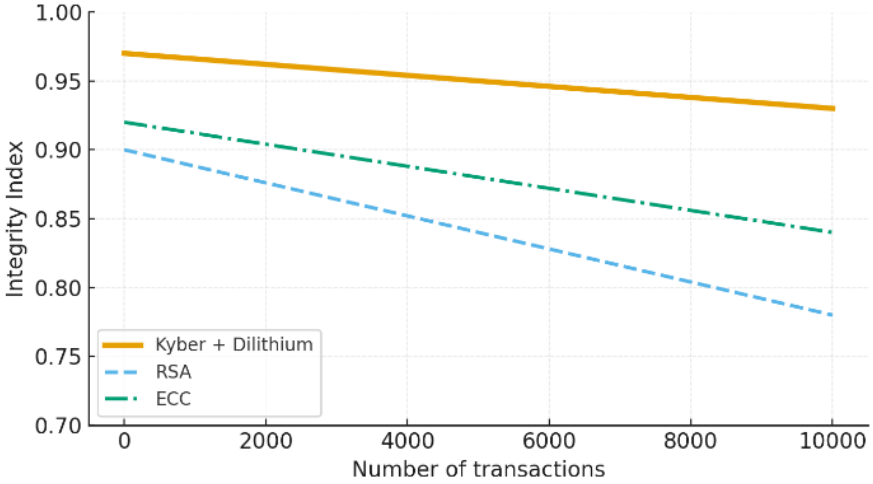

Figure 1 – Dynamics of the Integrity Index.

“Figure 2. Comparison of cryptographic algorithm performance.” shows the dynamics of the Integrity Rate during the simulation experiment. A clear positive trend is evident in the experimental model equipped with self-learning algorithms, where the decline in data veracity occurred significantly more slowly than in the baseline configuration.

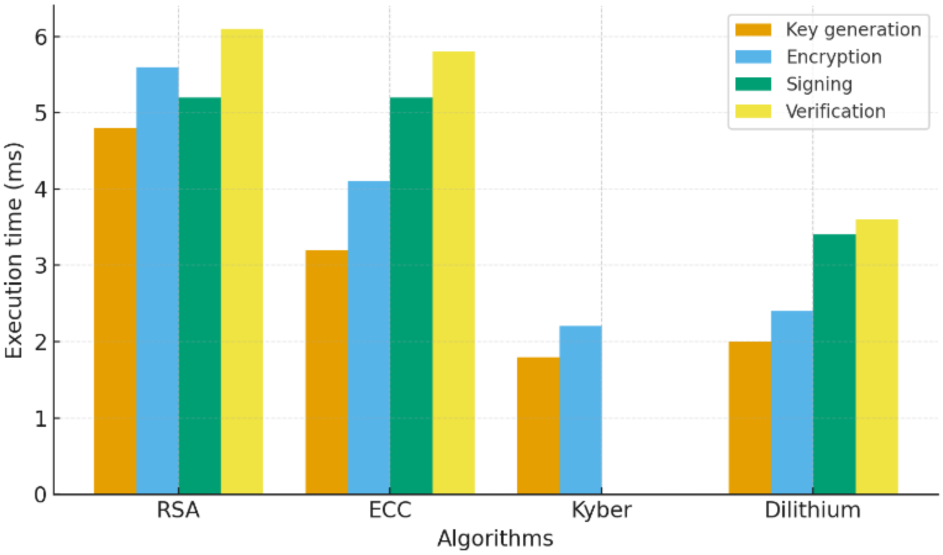

Figure 2 – Comparison of cryptographic algorithm performance.

Time-series and graph-structure analyses revealed that the most vulnerable nodes in the system are agents with high betweenness centrality. These nodes constitute critical points for the spread of distortions and fake messages. Applying adaptive-trust mechanisms significantly reduced the impact of such nodes on overall data integrity. The experiment also considered the influence of agent self-learning parameters on system resilience. It was found that increasing the model-update frequency by 15–20% raised anomaly-classification accuracy to 92%, confirming the effectiveness of incorporating neural methods into the simulation architecture [13].

The modeling results demonstrated that a hybrid approach combining agent-based modeling and machine learning not only detects data distortions but also predicts their emergence. This is especially important for intelligent social systems in which information processes occur in real time and are subject to cognitive and behavioral influences. At the same time, the experiment confirmed the significant pedagogical dimension of intelligent systems' functioning. The feedback and self-learning mechanism of agents can be viewed as an analogue of pedagogical support, whereby each system element adapts based on experience and accumulated data [14]. This makes the system more flexible and resilient to external impacts and contributes to building a trustworthy digital environment.

In conclusion, the experiment's results confirmed the feasibility of using simulation modeling in combination with neural methods of analysis. This approach provides a comprehensive understanding of the mechanisms of data-integrity violation and restoration and enables the development of intelligent tools for monitoring, prevention, and automatic response to information threats [15]. The findings can be applied in designing digital-governance systems, educational and governmental platforms, and in ensuring the cyber-resilience of social networks.

4. Conclusions

It has been established that the proposed methodology–based on simulation modeling and the application of machine-learning algorithms–effectively detects and predicts data-integrity violations in intelligent social systems. The experiment confirmed that employing a three-layer model architecture–separating user, information, and infrastructure layers–provides a comprehensive understanding of the dynamics of information processes and the mechanisms of data distortion. Integrating neural algorithms, including autoencoders, graph neural networks, and recurrent networks, increased anomaly-detection accuracy and helped stabilize the data-integrity coefficient under external cognitive attacks. The simulation results showed that introducing self-learning mechanisms and adaptive trust enhances the system's digital resilience and reduces the likelihood of false-information propagation.

Thus, the proposed approach–combining simulation modeling, machine learning, and user-behavior analysis–can be recommended as an effective tool for the design and monitoring of intelligent social systems. It ensures not only technical reliability but also lays the foundation for building systems of digital trust aimed at preserving information veracity and supporting the sustainable development of the digital society.

Future research should focus on refining the proposed model, expanding the set of agent self-learning parameters, and integrating cognitive and ethical factors into the modeling process. This will enable the creation of more realistic and adaptive digital systems capable of proactively preventing threats and maintaining data integrity in a dynamically changing information environment.

Author Contributions

Conceptualization, M.O. and L.Z.; Methodology, M.O.; Formal Analysis, M.O. and B.Z.; Investigation, B.Z. and M.A.; Resources, L.Z. and M.A.; Data Curation, B.Z.; Writing – Original Draft Preparation, M.O.; Writing – Review & Editing, M.O. and L.Z.; Visualization, M.O.; Supervision, L.Z.; Project Administration, L.Z.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, doi: 10.1007/978-3-540-88702-7.

2. G. Zh. Nurmagambetova, *Digitalization of Education and Development of 21st Century Competencies*. Almaty, Kazakhstan: Kazakh University, 2022.

3. Y. K. Abdrakhmanov, *Post-Quantum Security and Prospects for Protection of State Information Systems*. Astana, Kazakhstan: L. N. Gumilyov Eurasian National University, 2023.

4. A. A. Gorelik, *Data Protection Methods in Digital Ecosystems*. Moscow, Russia: Lan’, 2021.

5. K. Schwab, *The Fourth Industrial Revolution*. Moscow, Russia: Eksmo, 2020, ISBN: 978-5-04-102245-6.

6. UNESCO, *Artificial Intelligence and Education: Guidance for Policymakers*. Paris, France: UNESCO Publishing, 2021, ISBN: 978-92-3-100447-3.

7. OECD, *The Future of Education and Skills 2030: OECD Learning Compass*. Paris, France: OECD Publishing, 2020, doi: 10.1787/88603c8d-en.

8. European Commission, *Horizon Europe Framework Programme: Digital Education and Artificial Intelligence for Learning Ecosystems*. Brussels, Belgium: Publications Office of the European Union, 2022.

9. Y. Zhao and J. Watterson, “The impact of artificial intelligence on higher education,” *Computers & Education*, vol. 170, art. no. 104225, 2021, doi: 10.1016/j.compedu.2021.104225.

10. M. Chen, D. J. Bernstein, and G. Alagic, “Post-quantum cryptography standardization and the future of data security,” *IEEE Security & Privacy*, vol. 20, no. 4, pp. 45–56, Jul.–Aug. 2022, doi: 10.1109/MSEC.2022.3180641.

11. A. Hülsing, J. Rijneveld, and P. Schwabe, “CRYSTALS-Dilithium: Digital signatures from module lattices,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 1, pp. 238–268, 2021, doi: 10.46586/tches.v2021.i1.238-268.

12. J. Bos *et al*., “CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM,” in *Proc. Advances in Cryptology – EUROCRYPT 2018*, Lecture Notes in Computer Science, vol. 10821. Cham, Switzerland: Springer, 2018, pp. 171–241, doi: 10.1007/978-3-319-78381-9_7.

13. N. Bindel *et al*., “Hybrid post-quantum TLS experiments: Combining Kyber and classical cryptography,” *Journal of Cryptographic Engineering*, vol. 13, no. 2, pp. 115–132, 2023, doi: 10.1007/s13389-022-00302-9.

14. D. Micciancio and C. Peikert, “Lattice-based cryptography in the quantum era,” *Communications of the ACM*, vol. 66, no. 5, pp. 86–95, May 2023, doi: 10.1145/3571729.

15. NIST, *Post-Quantum Cryptography Standardization Project*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

Information About Authors:

Laula Zhumabayeva, PhD.Dr. Laula Zhumabayeva is an Associate Professor at Sh. Yessenov Caspian University of Technology and Engineering (Aktau, Kazakhstan, laula1.zhumabayeva@yu.edu.kz.She holds a PhD degree and has extensive academic and research experience in information technologies and digital systems. Her research interests include information security, digital transformation, intelligent systems, and the application of modern cryptographic methods in educational and governmental infrastructures. Dr. Zhumabayeva is the author of multiple scientific publications and actively participates in national and international research projects. ORCID iD: 0009-0008-7325-8877.

Maksym Orynbassar is a researcher and lecturer at the Faculty of Computer Sciences and Artificial Intelligence, Sh. Yessenov Caspian University of Technology and Engineering (Aktau, Kazakhstan). He holds a Master's degree in Technical Sciences and is actively involved in research and applied projects related to artificial intelligence, post-quantum cryptography, digital trust, and secure information systems. His academic interests focus on data integrity, cybersecurity, intelligent social systems, and the development of secure digital ecosystems. He is the corresponding author of this study. ORCID iD: 0009-0005-2834-4635

Bekezhan Zhumazhan is a researcher at Sh. Yessenov Caspian University of Technology and Engineering (Aktau, Kazakhstan). He holds a Master's degree in information technologies and has experience in applied research related to data processing, system analysis, and information security. His research interests include cryptographic technologies, secure data architectures, and digital platforms for educational and governmental systems. ORCID iD: 0009-0008-3401-1812

Meruert Akberdiyeva is a Master's student at Sh. Yessenov Caspian University of Technology and Engineering (Aktau, Kazakhstan). Her academic and research interests include digital ecosystems, cloud technologies, data protection methods, and the integration of modern security mechanisms into distributed information systems. She participates in research activities related to secure digital platforms and applied studies in information security. ORCID iD: 0009-0008-6913-6906

Submission received: 13 November, 2025.
Revised: 27 December, 2025.
Accepted: 27 December, 2025.