ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 8

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 8

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

IMPLEMENTATION-ORIENTED ANALYSIS OF A HYBRID POST-QUANTUM CRYPTOGRAPHIC FRAMEWORK FOR SECURE DATA TRANSMISSION

Turdiyev Temur Taxirovich
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti Kompyuter injiniringi fakulteti Axborot xavfsizligi kafedra katta o‘qituvchisi
E-mail: temurbek199002@gmail.com

Annotatsiya. Ushbu maqolada post-kvant kriptografik algoritmlar asosida xavfsiz ma’lumot uzatish tizimlarini amaliy joriy etish masalasi tadqiq qilinadi. Kvant hisoblash texnologiyalarining rivojlanishi RSA va ECC kabi an’anaviy ochiq kalitli kriptografik algoritmlar xavfsizligiga tahdid tug‘diradi. Shu sababli kvant hujumlariga bardoshli kriptografik mexanizmlarni ishlab chiqish va mavjud axborot tizimlariga moslashtirish dolzarb masala hisoblanadi. Maqolada NTRUEncrypt, SPHINCS+ va BIKE algoritmlaridan tashkil topgan gibrid post-kvant kriptografik model amaliy joriy etish nuqtayi nazaridan tahlil qilinadi. Tadqiqotda xavfsizlik, tezkorlik, kalit hajmi, hisoblash murakkabligi va real tarmoq muhitida qo‘llash imkoniyatlari baholanadi. Natijalar gibrid yondashuv xavfsiz ma’lumot uzatish uchun istiqbolli yechim ekanini, biroq uni amaliy tizimlarga tatbiq etishda optimallashtirish zarurligini ko‘rsatadi.

Kalit so‘zlar. post-kvant kriptografiya, gibrid kriptografik model, NTRUEncrypt, SPHINCS+, BIKE, xavfsiz ma’lumot uzatish, kvant xavfsizligi.

Аннотация. В данной статье исследуется вопрос практического внедрения систем безопасной передачи данных на основе постквантовых криптографических алгоритмов. Развитие квантовых вычислительных технологий создает угрозу безопасности традиционных криптографических алгоритмов с открытым ключом, таких как RSA и ECC. Поэтому разработка и адаптация криптографических механизмов, устойчивых к квантовым атакам, является актуальной задачей. В статье анализируется гибридная постквантовая криптографическая модель, состоящая из алгоритмов NTRUEncrypt, SPHINCS+ и BIKE, с точки зрения практического внедрения. В исследовании оцениваются безопасность, скорость работы, размер ключей, вычислительная сложность и возможность применения в реальных сетевых условиях. Результаты показывают, что гибридный подход является перспективным решением для безопасной передачи данных, однако его внедрение в практические системы требует дополнительной оптимизации.

Ключевые слова. постквантовая криптография, гибридная криптографическая модель, NTRUEncrypt, SPHINCS+, BIKE, безопасная передача данных, квантовая безопасность.

Abstract. This article investigates the practical implementation of secure data transmission systems based on post-quantum cryptographic algorithms. The development of quantum computing technologies creates serious security challenges for traditional public-key cryptographic algorithms such as RSA and ECC. Therefore, the design and adaptation of cryptographic mechanisms resistant to quantum attacks have become important research tasks. The article analyzes a hybrid post-quantum cryptographic model consisting of NTRUEncrypt, SPHINCS+, and BIKE from an implementation-oriented perspective. The study evaluates security level, processing speed, key size, computational complexity, and applicability in real network environments. The results show that the hybrid approach is a promising solution for secure data transmission, but its deployment in practical systems requires further optimization.

Keywords. post-quantum cryptography, hybrid cryptographic model, NTRUEncrypt, SPHINCS+, BIKE, secure data transmission, quantum security.

INTRODUCTION.

The rapid development of quantum computing is creating new challenges for modern information security systems. Today, many digital infrastructures rely on public-key cryptographic algorithms such as RSA and elliptic curve cryptography. These algorithms are widely used in electronic commerce, digital signatures, cloud services, online banking, virtual private networks, and secure data transmission systems [1], [2].

The security of traditional public-key cryptographic algorithms is based on mathematical problems that are difficult for classical computers to solve. RSA relies on the difficulty of integer factorization, while elliptic curve cryptography relies on the discrete logarithm problem. However, the emergence of powerful quantum computers may weaken these assumptions. Shor's algorithm can theoretically solve integer factorization and discrete logarithm problems in polynomial time on a quantum computer. As a result, cryptographic systems that are currently considered secure may become vulnerable in the future quantum era.

Post-quantum cryptography has emerged as a promising field aimed at developing cryptographic algorithms that remain secure against both classical and quantum attacks [3], [4]. The main directions of post-quantum cryptography include lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial cryptography [5]. Each direction has its own advantages and limitations in terms of security level, key size, computational complexity, and practical implementation.

The uploaded IEEE article "Exploring Post-Quantum Cryptographic Algorithms for Secure Data Transmission" analyzes several post-quantum cryptographic approaches and proposes a hybrid framework based on

ISSN 3030-3907

NTRUEncrypt, SPHINCS+, and BIKE. This article continues that research direction by focusing on implementation and optimization aspects of such a hybrid model. The main purpose of this study is to evaluate how the combination of lattice-based, hash-based, and code-based algorithms can be used to provide secure, efficient, and quantum-resistant data transmission.

The scientific novelty of this article is the implementation-oriented analysis of a hybrid post-quantum cryptographic model. Unlike studies that only compare algorithms theoretically, this research considers practical factors such as encryption speed, digital signature generation, key exchange latency, key management, scalability, and deployment challenges.

LITERATURE REVIEW.

Post-quantum cryptography has become an important research area because of the possible future impact of quantum computing on modern cryptographic systems. The first major theoretical threat was introduced by Shor, who demonstrated that a quantum computer could solve integer factorization and discrete logarithm problems efficiently. Grover's algorithm also showed that quantum search can reduce the complexity of brute-force attacks, which affects symmetric cryptographic systems and hash functions [6].

Lattice-based cryptography is one of the most widely studied post-quantum approaches. It is based on the hardness of mathematical lattice problems, such as the Shortest Vector Problem and Learning with Errors. These problems are believed to be difficult for both classical and quantum computers [7], [8]. NTRUEncrypt is a well-known lattice-based encryption algorithm that provides efficient encryption and decryption operations while maintaining strong security assumptions [9]. In the uploaded IEEE article, NTRUEncrypt is selected as the encryption component of the hybrid framework because of its efficiency and resistance to quantum attacks.

Hash-based cryptography is mainly used for digital signatures. Its security is based on the properties of cryptographic hash functions. Merkle proposed one of the earliest hash-based digital signature schemes, which later became the foundation for modern hash-based signature systems [10]. SPHINCS+ is a stateless hash-based digital signature scheme designed to provide strong security against classical and quantum attacks. In secure data transmission systems, SPHINCS+ can be used to ensure message integrity, sender authentication, and non-repudiation [11].

Code-based cryptography relies on the difficulty of decoding random linear codes. The McEliece cryptosystem is one of the oldest post-quantum public-key cryptosystems and has resisted many cryptanalytic attacks for several decades [12]. BIKE is a modern code-based cryptographic mechanism that can be used for

ISSN 3030-3907

key exchange and key encapsulation. In the hybrid model discussed in this article, BIKE is selected for secure session key establishment because of its ability to provide efficient key exchange with quantum-resistant security assumptions [13].

Multivariate polynomial cryptography is another post-quantum approach based on solving systems of multivariate polynomial equations over finite fields. Algorithms in this category can offer fast computation, but some schemes have faced security concerns due to algebraic attacks [14]. Therefore, careful parameter selection and security analysis are required before applying multivariate schemes in practical systems.

The literature shows that each post-quantum cryptographic approach has both strengths and weaknesses. Lattice-based algorithms can provide high performance and strong security, but parameter selection may be complex. Hash-based algorithms offer strong security assumptions, but their signature sizes may be large. Code-based algorithms have a long security history, but they may require large keys. For this reason, a hybrid approach can be useful because it combines several cryptographic mechanisms to protect different aspects of secure communication.

Table 1

Comparison of post-quantum cryptographic approaches [1]

Cryptographic approach	Example algorithm	Main function	Security basis	Practical limitation
Lattice-based cryptography	NTRUEncrypt	Encryption	Lattice problems	Parameter selection complexity
Hash-based cryptography	SPHINCS+	Digital signature	Hash functions	Large signature size
Code-based cryptography	BIKE	Key exchange	Linear codes	Large key structure
Multivariate cryptography	Rainbow, HFE	Signature/encryption	Polynomial equations	Vulnerability to algebraic attacks

RESEARCH METHODOLOGY.

The methodology of this study is based on comparative analysis, structural modeling, and implementation-oriented evaluation of post-quantum cryptographic algorithms. The research focuses on three main security

ISSN 3030-3907

requirements for data transmission: confidentiality, integrity, and secure key exchange.

However, this article expands the analysis by considering implementation and optimization requirements. The model consists of three cryptographic layers: the confidentiality layer, the integrity and authentication layer, and the key establishment layer.

The first layer is the confidentiality layer. It uses NTRUEncrypt to encrypt transmitted data. The purpose of this layer is to protect sensitive information from unauthorized access. Since NTRUEncrypt is based on lattice problems, it provides resistance to known quantum attacks.

The second layer is the integrity and authentication layer. This layer uses SPHINCS+ to create and verify digital signatures. The sender signs the encrypted data, and the receiver verifies the signature before accepting the message. This mechanism helps ensure that the transmitted data has not been modified and that it was sent by a legitimate sender.

The third layer is the key establishment layer. This layer uses BIKE to establish a secure session key between communicating parties. Secure key exchange is essential because encryption systems depend on reliable key generation and key distribution mechanisms.

Table 2

Structure of the proposed hybrid post-quantum cryptographic model

Layer	Algorithm	Main task	Expected result
Confidentiality layer	NTRUEncrypt	Data encryption	Protection of confidential information
Integrity and authentication layer	SPHINCS+	Digital signature	Verification of data integrity and sender identity
Key establishment layer	BIKE	Key exchange	Secure session key generation

The general operation of the proposed model consists of several stages. First, the sender and receiver generate post-quantum key pairs for the required cryptographic algorithms. Second, BIKE is used to establish a secure session key. Third, the sender encrypts the original message using NTRUEncrypt. Fourth, the encrypted message is signed using SPHINCS+. Fifth, the receiver verifies the digital signature. Finally, the receiver decrypts the message and obtains the original data.

ISSN 3030-3907

The workflow of the proposed model can be described as follows:

Sender → key generation → BIKE-based key exchange → NTRUEncrypt-based encryption → SPHINCS+-based digital signature → secure transmission → signature verification → decryption → receiver.

This structure makes it possible to protect the communication process at several levels. Even if one component requires optimization or parameter adjustment, the other components continue to provide important security functions. Such modularity is one of the main advantages of the hybrid post-quantum model.

RESULTS AND DISCUSSION.

The analysis shows that the hybrid post-quantum cryptographic model can provide strong protection for secure data transmission. Unlike a single-algorithm approach, the proposed model separates cryptographic functions into different components. NTRUEncrypt protects data confidentiality, SPHINCS+ ensures integrity and authentication, and BIKE provides secure key establishment.

From the security perspective, the proposed model is resistant to major quantum-oriented threats because each algorithm is based on mathematical assumptions that are believed to be difficult for quantum computers. NTRUEncrypt relies on lattice problems, SPHINCS+ relies on secure hash functions, and BIKE relies on the difficulty of decoding random linear codes.

From the performance perspective, the uploaded IEEE article reports that the hybrid framework can achieve an encryption speed of 500 MB/s, digital signature generation of 1000 operations per second, and key exchange time of 0.5 ms [1]. These results indicate that the hybrid approach can be suitable for high-speed and low-latency data transmission systems.

Table 3

Performance indicators of the hybrid framework [1]

Indicator	Value	Practical meaning
Encryption speed	500 MB/s	Suitable for high-volume data transmission
Signature generation	1000 operations/s	Supports frequent authentication
Key exchange time	0.5 ms	Enables low-latency secure communication
Overall security level	High	Provides resistance to quantum-oriented attacks

ISSN 3030-3907

The results show that the proposed hybrid model can be applied in systems that require long-term data protection. Such systems include cloud computing platforms, electronic government services, financial networks, medical information systems, military communication channels, and critical infrastructure control systems. However, practical implementation also creates several challenges. The first challenge is key size. Many post-quantum algorithms require larger public and private keys than traditional algorithms. This can increase memory usage and network traffic. The second challenge is computational overhead. Although NTRUEncrypt, SPHINCS+, and BIKE are efficient within their own categories, combining them in one system may increase processing requirements. Therefore, optimization is required for devices with limited computational resources, such as IoT sensors and embedded systems.

The third challenge is compatibility with existing security protocols. Most current systems are designed around classical cryptographic algorithms. Replacing RSA or ECC with post-quantum mechanisms requires changes in protocol design, certificate structures, key management systems, and software libraries.

The fourth challenge is key management. Since the hybrid model uses several algorithms at the same time, key generation, storage, renewal, and revocation must be carefully controlled. Poor key management can reduce the overall security of the system even if the cryptographic algorithms themselves are strong.

Table 4

Advantages and implementation challenges of the proposed model

Aspect	Advantage	Challenge
Security	Resistance to quantum attacks	Requires correct parameter selection
Performance	Fast encryption and key exchange	Possible computational overhead
Scalability	Can be used in different environments	Integration complexity
Reliability	Provides confidentiality, integrity, and authentication	Requires advanced key management
Practical use	Suitable for cloud, finance, and government systems	Requires testing in real networks

ISSN 3030-3907

The discussion shows that hybrid post-quantum cryptography should be considered not only a theoretical solution but also a practical migration strategy. Organizations should begin evaluating their current cryptographic infrastructure and identify systems that depend on RSA, ECC, and other algorithms vulnerable to quantum attacks. A gradual transition to post-quantum algorithms can reduce future security risks and improve long-term data protection.

CONCLUSION AND RECOMMENDATIONS.

This article examined the implementation and optimization of a hybrid post-quantum cryptographic model for secure data transmission. The study was developed in connection with the uploaded IEEE article, which analyzed post-quantum cryptographic algorithms and proposed a hybrid framework based on NTRUEncrypt, SPHINCS+, and BIKE.

The results of the analysis show that combining different post-quantum cryptographic algorithms can provide a strong and balanced security architecture. NTRUEncrypt ensures confidentiality, SPHINCS+ provides integrity and authentication, and BIKE supports secure key exchange. Together, these components create a quantum-resistant communication model suitable for future secure data transmission systems.

The proposed model is promising for practical use in cloud computing, financial services, electronic government systems, healthcare platforms, and critical infrastructure networks. However, its successful implementation requires solving several technical problems, including large key sizes, memory consumption, computational overhead, protocol compatibility, and key management complexity.

Based on the results of the study, the following recommendations are proposed. First, the hybrid model should be tested in real network environments to evaluate its actual performance. Second, optimization methods should be developed for resource-constrained devices such as IoT and embedded systems. Third, secure key management procedures should be standardized for hybrid post-quantum systems. Fourth, organizations should prepare migration plans from classical public-key cryptography to quantum-resistant cryptographic solutions.

Future research should focus on experimental implementation, benchmarking, adaptive parameter selection, and integration of hybrid post-quantum mechanisms into existing security protocols. As quantum computing continues to develop, post-quantum cryptography will play a key role in protecting digital infrastructure and ensuring the long-term confidentiality of sensitive data.

ISSN 3030-3907

REFERENCES

1. S. R. Gulomov, T. R. Khudayberganov, M. X. Ravshanova, T. T. Turdiev, and S. S. Atabayev, “Exploring Post-Quantum Cryptographic Algorithms for Secure Data Transmission,” 2024 IEEE 3rd International Conference on Problems of Informatics, Electronics and Radio Engineering (PIERE), pp. 1480–1483, 2024, doi: 10.1109/PIERE62470.2024.10805050.
2. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, 1997.
3. D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.
4. L. Chen et al., “Report on Post-Quantum Cryptography,” National Institute of Standards and Technology, 2016.
5. N. J. Alagic et al., “NIST PQC Standardization Process,” National Institute of Standards and Technology, 2020.
6. L. K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 1996.
7. M. Ajtai, “Generating Hard Instances of Lattice Problems,” Proceedings of the 28th ACM Symposium on Theory of Computing, 1996.
8. C. Peikert, “A Decade of Lattice Cryptography,” Foundations and Trends in Theoretical Computer Science, 2016.
9. J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” Algorithmic Number Theory, Cambridge University Press, 2010.
10. [10] R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” Advances in Cryptology — CRYPTO ’87, Springer, 1988.
11. D. J. Bernstein et al., “SPHINCS+: A Compact Hash-Based Signature Scheme,” ACM SIGSAC Conference on Computer and Communications Security, 2015.
12. R. J. McEliece, “A Public-Key Cryptosystem Based on Algebraic Coding Theory,” Deep Space Network Progress Report, 1978.
13. R. Misoczki et al., “The BIKE Post-Quantum Cryptosystem,” IEEE Transactions on Information Theory, 2021.
14. J. Ding and A. Petzoldt, “Multivariate Public Key Cryptosystems,” Journal of Mathematical Cryptology, 2017.
15. L. Chen et al., “On the Security of Post-Quantum Cryptographic Systems,” Journal of Cryptographic Engineering, 2018.

ISSN 3030-3907