ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 9

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 9

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

ENERGY-AWARE ADAPTIVE HYBRID POST-QUANTUM CRYPTOGRAPHIC MODEL FOR RESOURCE-CONSTRAINED IOT ENVIRONMENTS

Turdiyev Temur Taxirovich
Senior Lecturer, Department of Information Security, Faculty of Computer Engineering, Urgench State University named after Abu Rayhan Beruni
E-mail: temurbek199002@gmail.com

Annotatsiya. Ushbu maqolada resurslari cheklangan IoT va edge qurilmalari uchun energiya samaradorligiga yo‘naltirilgan adaptiv gibrid post-kvant kriptografik model taklif etiladi. Kvant hisoblash texnologiyalarining rivojlanishi RSA va ECC kabi an’anaviy kriptografik algoritmlarga jiddiy xavf tug‘diradi. Shu sababli kvant hujumlariga bardoshli, lekin kam quvvat sarflaydigan kriptografik yechimlarni ishlab chiqish dolzarb masala hisoblanadi. Taklif etilgan modelda NTRUEncrypt ma’lumotlarni shifrlash, SPHINCS+ raqamli imzo yaratish, BIKE esa xavfsiz kalit almashinuvi uchun qo‘llaniladi. Maqolada hisoblash va energiya sarfini baholash uchun matematik model ishlab chiqildi. Natijalar shuni ko‘rsatadiki, adaptiv yondashuv xavfsizlik, energiya samaradorligi va ishlash tezligi o‘rtasida maqbul muvozanatni ta’minlaydi.

Kalit so‘zlar. post-kvant kriptografiya, IoT xavfsizligi, gibrid kriptografik model, NTRUEncrypt, SPHINCS+, BIKE, energiya samaradorligi, edge computing.

Аннотация. В данной статье предлагается энергоэффективная адаптивная гибридная постквантовая криптографическая модель для IoT- и edge-устройств с ограниченными ресурсами. Развитие квантовых вычислительных технологий создает серьезную угрозу традиционным криптографическим алгоритмам, таким как RSA и ECC. Поэтому разработка криптографических решений, устойчивых к квантовым атакам и потребляющих минимальное количество энергии, является актуальной задачей. В предложенной модели NTRUEncrypt используется для шифрования данных, SPHINCS+ — для цифровой подписи, а BIKE — для безопасного обмена ключами. В статье разработана математическая модель для оценки вычислительных затрат и энергопотребления. Результаты показывают, что адаптивный подход обеспечивает оптимальный баланс между безопасностью, энергоэффективностью и производительностью.

Ключевые слова. постквантовая криптография, безопасность IoT, гибридная криптографическая модель, NTRUEncrypt, SPHINCS+, BIKE, энергоэффективность, edge computing.

Abstract. This article proposes an energy-aware adaptive hybrid post-quantum cryptographic model for resource-constrained IoT and edge devices. The development of quantum computing technologies creates serious threats to

traditional cryptographic algorithms such as RSA and ECC. Therefore, it is necessary to design cryptographic solutions that are resistant to quantum attacks while maintaining low energy consumption. The proposed model uses NTRUEncrypt for data encryption, SPHINCS+ for digital signatures, and BIKE for secure key exchange. A mathematical model is introduced to evaluate computational cost and energy consumption. The results show that the adaptive approach provides a reasonable balance between security, energy efficiency, and performance.

Keywords. post-quantum cryptography, IoT security, hybrid cryptographic model, NTRUEncrypt, SPHINCS+, BIKE, energy efficiency, edge computing.

INTRODUCTION.

The rapid development of quantum computing is creating new challenges for modern information security systems. Traditional public-key cryptographic algorithms such as RSA and elliptic curve cryptography are widely used in digital communication, cloud services, banking systems, IoT platforms, and government information infrastructures. However, these algorithms are based on mathematical problems that may become vulnerable to quantum attacks.

Shor's algorithm can theoretically solve integer factorization and discrete logarithm problems in polynomial time on a quantum computer [1]. As a result, RSA and ECC-based security mechanisms may no longer provide long-term protection in the future quantum era. Grover's algorithm also affects brute-force search by reducing the effective security level of symmetric cryptographic operations [2].

Post-quantum cryptography is designed to protect digital systems against both classical and quantum adversaries [3]. The main post-quantum cryptographic families include lattice-based, hash-based, code-based, and multivariate polynomial-based approaches. However, each algorithm family has its own limitations in terms of key size, signature size, computational cost, and energy consumption [4].

The uploaded source article focuses on application-specific optimization of hybrid post-quantum cryptographic frameworks in resource-constrained environments. It evaluates NTRUEncrypt, SPHINCS+, and BIKE on ARM Cortex-A53 and FPGA Kintex-7 platforms, showing that FPGA acceleration can significantly improve throughput and reduce energy consumption [5].

This article continues that research direction by proposing an energy-aware adaptive hybrid post-quantum cryptographic model. The main aim of the study is to develop a model that can dynamically select suitable cryptographic operations depending on device capability, available energy, latency requirements, and required security level.

ISSN 3030-3907

LITERATURE REVIEW.

Post-quantum cryptography has become an important research direction due to the expected impact of quantum computers on classical cryptographic systems. Shor's algorithm demonstrated that quantum computers could break RSA and ECC by solving their underlying mathematical problems efficiently. Grover's algorithm also showed that quantum search can reduce the complexity of exhaustive key search.

Lattice-based cryptography is one of the most promising post-quantum approaches. It relies on the hardness of lattice problems and provides efficient encryption and key encapsulation mechanisms. NTRUEncrypt is a well-known lattice-based algorithm that offers high-speed encryption and can benefit from hardware acceleration [6], [7].

Hash-based cryptography provides security based on one-way hash functions. SPHINCS+ is a stateless hash-based digital signature scheme that can provide strong security guarantees against quantum attacks [8]. However, hash-based signatures may require larger signature sizes and higher computational resources compared with some classical signature algorithms.

Code-based cryptography is based on the difficulty of decoding random linear codes. The McEliece cryptosystem is one of the oldest and most studied post-quantum cryptographic systems [9]. BIKE is a modern code-based key encapsulation mechanism that can provide efficient and low-latency key exchange [10].

Previous studies show that no single post-quantum algorithm is optimal for all cryptographic tasks. Lattice-based algorithms are usually efficient for encryption, hash-based algorithms are strong for digital signatures, and code-based algorithms are suitable for conservative key exchange. Therefore, hybrid frameworks can combine the strengths of several algorithm families [11].

Table 1

Comparison of selected post-quantum cryptographic algorithms

Algorithm	Family	Main function	Advantage	Limitation
NTRUEncrypt	Lattice-based	Data encryption	High throughput	Requires parameter optimization
SPHINCS+	Hash-based	Digital signature	Strong hash-based security	Signature overhead

ISSN 3030-3907

BIKE	Code-based	Key exchange	Low latency	Key management complexity
McEliece	Code-based	Key encapsulation	Long-term security	Large public key size

The literature analysis shows that resource-constrained systems require not only quantum-resistant security but also careful optimization of energy, memory, and processing time. This is especially important for IoT sensors, embedded controllers, telemedicine devices, and industrial monitoring systems.

RESEARCH METHODOLOGY.

The methodology of this study is based on structural modeling, comparative analysis, and energy-aware evaluation of hybrid post-quantum cryptographic operations. The proposed model consists of three main layers: encryption, digital signature, and key exchange.

The first layer uses NTRUEncrypt for data encryption. This layer is responsible for protecting the confidentiality of transmitted information. NTRUEncrypt was selected because lattice-based encryption can provide high performance and can be accelerated on hardware platforms.

The second layer uses SPHINCS+ for digital signatures. This layer ensures data integrity, sender authentication, and non-repudiation. It is especially important in IoT systems where transmitted sensor data must be protected from modification.

The third layer uses BIKE for secure key exchange. This layer establishes session keys between communicating devices. BIKE was selected because it can provide low-latency key exchange and quantum-resistant security assumptions.

Proposed adaptive model

The proposed model includes an adaptive control module. This module analyzes four factors before selecting the cryptographic operation mode:

- device processing capacity;
- available battery or energy level;
- required security level;
- maximum acceptable latency.

If the device has sufficient energy and requires high security, the full hybrid mode is activated. If the device has limited battery, the model reduces the frequency of heavy signature operations and reuses secure session keys for a limited time. If the device works as an edge gateway or FPGA-based accelerator, the model enables high-throughput cryptographic processing.

Mathematical model

ISSN 3030-3907

The total processing time of the proposed hybrid cryptographic system is calculated as follows:

$$T_{total} = T_{kex} + T_{enc} + T_{sig} + T_{ver} + T_{comm}$$

where:

T_{total}

is the total secure transmission time;

T_{kex}

is the key exchange time using BIKE;

T_{enc}

is the encryption time using NTRUEncrypt;

T_{sig}

is the signature generation time using SPHINCS+;

T_{ver}

is the signature verification time;

T_{comm}

is the communication delay.

The energy consumption of one secure transmission cycle can be expressed as:

$$E_{cycle} = E_{kex} + E_{enc} + E_{sig} + E_{ver} + E_{idle}$$

where:

E_{cycle}

is the total energy consumption per secure communication cycle;

E_{kex}

is the energy used for key exchange;

E_{enc}

is the energy used for encryption;

E_{sig}

is the energy used for signature generation;

E_{ver}

is the energy used for verification;

E_{idle}

is the energy consumed during waiting or idle state?

To select the optimal mode, the adaptive suitability score is defined as:

$$A = \frac{S \times P}{T_{total} \times E_{cycle} \times M}$$

where:

A

is the adaptive suitability score;

S

ISSN 3030-3907

is the security level;

P

is the performance coefficient;

M

is the memory consumption factor.

A higher value of A means that the selected cryptographic configuration is more suitable for a resource-constrained device.

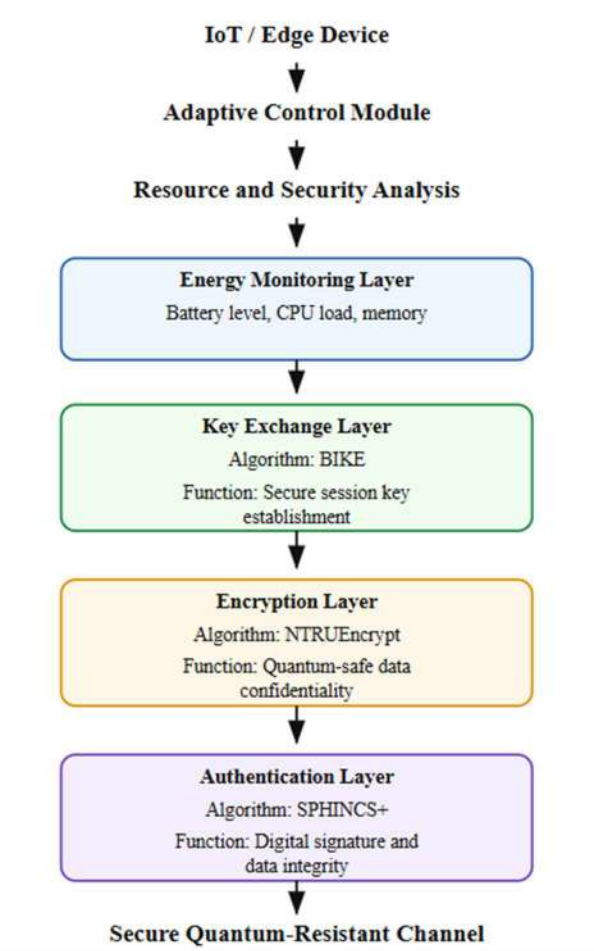


Figure 1. Architecture of the energy-aware adaptive hybrid post-quantum cryptographic model [5].

The figure describes the proposed adaptive workflow. First, the IoT or edge device sends a communication request to the adaptive control module. Then, the module analyzes energy level, CPU load, memory capacity, and security requirements. After that, BIKE establishes a secure session key, NTRUEncrypt encrypts the transmitted data, and SPHINCS+ provides digital signature and integrity protection.

RESULTS AND DISCUSSION.

The proposed energy-aware model was analyzed using performance values reported in the uploaded source article. In that study, the hybrid framework was tested on ARM Cortex-A53 and FPGA Kintex-7 platforms. The comparison

ISSN 3030-3907

shows that hardware acceleration significantly improves performance and energy efficiency.

Table 2

Performance comparison of ARM and FPGA platforms [5]

Metric	ARM Cortex-A53	FPGA Kintex-7	Observation
Encryption speed using NTRUEncrypt	180 MB/s	520 MB/s	FPGA gives approximately 3× improvement
SPHINCS+ signature generation	620 ops/s	1450 ops/s	FPGA reduces signature overhead
BIKE key exchange latency	1.2 ms	0.4 ms	FPGA achieves lower latency
Energy consumption per operation	3.5 mJ	1.1 mJ	FPGA consumes about 65% less energy

The results show that FPGA-based implementation is more suitable for high-performance edge gateways, industrial control nodes, and secure communication hubs. It provides higher encryption throughput, faster signature generation, lower key exchange latency, and lower energy consumption.

ARM-based implementation is slower but remains suitable for low-cost IoT devices. Since ARM processors are widely used in embedded systems, the proposed hybrid framework can still be applied in practical IoT environments. However, the adaptive module should reduce unnecessary cryptographic overhead when the device battery level is low.

Table 3

Adaptive operation modes of the proposed model

Mode	Device condition	Cryptographic strategy	Expected benefit
Full security mode	High energy, critical data	BIKE + NTRUEncrypt + SPHINCS+ for every session	Maximum protection

ISSN 3030-3907

Energy-saving mode	Low battery	Reduce signature frequency and reuse short-term sessions	Lower energy consumption
High-throughput mode	FPGA or edge gateway	Parallel encryption and accelerated signatures	High performance
Balanced mode	Normal IoT operation	Standard hybrid workflow	Security-performance balance

The main advantage of the proposed model is that it does not use the same cryptographic configuration for all devices and all situations. Instead, it adapts to the current system state. This is important because IoT environments are heterogeneous: some devices have very limited battery power, while others work as powerful edge gateways.

The mathematical model confirms that secure data transmission must be evaluated not only by encryption speed but also by key exchange time, signature generation, verification, communication delay, energy consumption, and memory overhead. Therefore, the adaptive suitability score can help select the most appropriate configuration for each device.

The proposed approach also improves system resilience. Since NTRUEncrypt, SPHINCS+, and BIKE are based on different mathematical assumptions, the compromise of one algorithm family does not automatically break the entire system. This layered protection is important for long-term quantum-safe infrastructures.

However, several implementation challenges remain. First, post-quantum algorithms may require larger keys and signatures than traditional algorithms. Second, SPHINCS+ signature generation may become a bottleneck in high-frequency IoT communication. Third, key management must be carefully designed to avoid session reuse risks. Fourth, FPGA acceleration may not be available in all low-cost environments.

CONCLUSION AND RECOMMENDATIONS.

This article proposed an energy-aware adaptive hybrid post-quantum cryptographic model for resource-constrained IoT and edge environments. The model is based on the combination of NTRUEncrypt, SPHINCS+, and BIKE, which provide encryption, digital signature, and secure key exchange respectively.

ISSN 3030-3907

The study showed that hybrid post-quantum cryptography can provide strong protection against future quantum threats while remaining practical for constrained systems. The performance values from ARM Cortex-A53 and FPGA Kintex-7 platforms demonstrate that FPGA acceleration significantly improves encryption speed, signature generation, key exchange latency, and energy efficiency.

The proposed adaptive module is the main contribution of this article. It allows the system to select a suitable cryptographic mode depending on energy level, device capability, latency requirements, and security needs. This makes the model suitable for IoT sensors, telemedicine systems, industrial IoT, smart city infrastructure, and secure edge computing platforms.

Future research should focus on real-world implementation of the adaptive control module, optimization of SPHINCS+ signature processing, secure session key lifecycle management, and integration with AI-based decision systems. Additional experiments should also be conducted in 5G/6G networks, cloud-edge architectures, and battery-powered embedded devices.

REFERENCES

1. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.
2. L. K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, pp. 212–219, 1996.
3. D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.
4. N. J. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, A. Liu, C. Miller, D. Moody, R. Perlner, and D. Smith-Tone, “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process,” NIST, 2020.
5. T. Khudaybergenov, B. Sabirov, T. Khudayberganov, and T. Turdiyev, “Application-Specific Optimization of Hybrid Post-Quantum Cryptographic Frameworks in Resource-Constrained Environments,” 2025 IEEE XVII International Scientific and Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE), 2025.
6. J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” Algorithmic Number Theory, Springer, pp. 267–288, 1998.
7. C. Peikert, “A Decade of Lattice Cryptography,” Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016.
8. D. J. Bernstein, D. Hopwood, A. Hülsing, S. Rijneveld, P. Schwabe, and G. M. Zaverucha, “SPHINCS+: A Stateless Hash-Based Signature Scheme for Post-

ISSN 3030-3907

Quantum Security," Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 368–397, 2015.
9. R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," DSN Progress Report, pp. 114–116, 1978.
10. R. Misoczki et al., "BIKE: Bit Flipping Key Encapsulation," post-quantum cryptography submission documentation, 2020.
11. L. Chen, S. Jordan, Y. K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," NIST Internal Report 8105, 2016.

ISSN 3030-3907