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

AN ADAPTIVE HYBRID POST-QUANTUM CRYPTOGRAPHIC MODEL FOR PERFORMANCE-AWARE SECURE DATA TRANSMISSION

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 kvant hisoblash texnologiyalari rivojlanishi sharoitida xavfsiz ma’lumot uzatish uchun adaptiv gibrid post-kvant kriptografik model taklif etiladi. Tadqiqot CRYSTALS-Kyber, XMSS va Classic McEliece algoritmlarining turli kriptografik vazifalardagi imkoniyatlarini tahlil qilishga qaratilgan. Taklif etilgan modelda Kyber tezkor shifrlash va kalit inkapsulyatsiyasi uchun, XMSS raqamli imzo va autentifikatsiya uchun, Classic McEliece esa uzoq muddatli xavfsiz kalit almashinuvi uchun qo‘llaniladi. Maqolada tizimning umumiy kechikish vaqtini baholash uchun matematik formula ishlab chiqildi. Natijalar adaptiv yondashuv xavfsizlik, samaradorlik va tizim barqarorligi o‘rtasida muvozanat yaratishini ko‘rsatadi.

Kalit so‘zlar. post-kvant kriptografiya, gibrid model, CRYSTALS-Kyber, XMSS, Classic McEliece, xavfsiz ma’lumot uzatish, kvant xavfsizligi.

Аннотация. В данной статье предлагается адаптивная гибридная постквантовая криптографическая модель для безопасной передачи данных в условиях развития квантовых вычислительных технологий. Исследование направлено на анализ возможностей алгоритмов CRYSTALS-Kyber, XMSS и Classic McEliece при выполнении различных криптографических функций. В предложенной модели Kyber используется для быстрого шифрования и инкапсуляции ключей, XMSS — для цифровой подписи и аутентификации, а Classic McEliece — для долгосрочного безопасного обмена ключами. В статье разработана математическая формула для оценки общей задержки системы. Результаты показывают, что адаптивный подход обеспечивает баланс между безопасностью, производительностью и устойчивостью системы.

Ключевые слова. постквантовая криптография, гибридная модель, CRYSTALS-Kyber, XMSS, Classic McEliece, безопасная передача данных, квантовая безопасность.

Abstract. This article proposes an adaptive hybrid post-quantum cryptographic model for secure data transmission in the context of rapidly developing quantum computing technologies. The study analyzes the functional capabilities of CRYSTALS-Kyber, XMSS, and Classic McEliece in different cryptographic roles. In the proposed model, Kyber is used for fast encryption and key

ISSN 3030-3907

encapsulation, XMSS is applied for digital signatures and authentication, while Classic McEliece is used for long-term secure key exchange. A mathematical formula is introduced to estimate the total latency of the system. The results show that the adaptive approach provides a balance between security, performance, and system resilience.

Keywords. post-quantum cryptography, hybrid model, CRYSTALS-Kyber, XMSS, Classic McEliece, secure data transmission, quantum security.

INTRODUCTION.

The rapid development of quantum computing is changing the security requirements of modern communication systems. Traditional public-key cryptographic algorithms such as RSA, Diffie–Hellman, and elliptic curve cryptography are widely used in cloud platforms, banking systems, digital signatures, secure messaging, and government information infrastructures [1], [2].

However, the security of these classical algorithms is based on mathematical problems such as integer factorization and discrete logarithms. These problems are difficult for classical computers, but they may be efficiently solved by quantum computers using Shor's algorithm. Therefore, cryptographic infrastructures based only on traditional public-key algorithms may become vulnerable in the future quantum era.

Post-quantum cryptography has emerged as a solution to this problem. It studies cryptographic algorithms that are believed to be secure against both classical and quantum attacks [3]. The main families of post-quantum cryptography include lattice-based, hash-based, code-based, multivariate polynomial-based, and isogeny-based approaches [4].

The uploaded IEEE article proposes a hybrid post-quantum cryptographic framework for high-performance secure data transmission. In that work, CRYSTALS-Kyber is used for encryption, XMSS is used for digital signatures, and Classic McEliece is used for key exchange. The layered architecture shown in the source article demonstrates how these algorithms can be placed into separate functional layers: application layer, Kyber encryption layer, XMSS signature layer, and McEliece key exchange layer.

This article continues that research direction and proposes an adaptive version of the hybrid framework. The main aim is to develop a model that can evaluate performance, security level, and resource consumption before selecting the most suitable post-quantum cryptographic operation.

LITERATURE REVIEW.

Post-quantum cryptography has become one of the most important research areas in modern cybersecurity. The main reason is the threat that quantum computers create for classical asymmetric cryptographic systems. Shor's

ISSN 3030-3907

algorithm can theoretically break RSA and ECC by solving their underlying mathematical problems in polynomial time. Grover's algorithm also affects brute-force search complexity, which means that symmetric key sizes and hash-based security parameters must be carefully selected [5].

Lattice-based cryptography is one of the most promising directions in post-quantum cryptography. CRYSTALS-Kyber is a lattice-based key encapsulation mechanism that provides high speed, relatively compact parameters, and practical implementation efficiency [6]. In the uploaded article, Kyber is selected as the encryption layer because it has low latency and high throughput.

Hash-based cryptography provides security based on cryptographic hash functions. XMSS, or Extended Merkle Signature Scheme, is a hash-based digital signature scheme standardized in RFC 8391 [7]. XMSS can provide message authentication, integrity, and non-repudiation. However, it is a stateful signature scheme, which means that signature key usage must be carefully managed [8].

Code-based cryptography is another strong post-quantum approach. Classic McEliece is based on algebraic coding theory and has a long history of cryptanalytic resistance [9]. Its main disadvantage is its large public key size, but it remains one of the most conservative and trusted post-quantum candidates for secure key exchange [10].

The source article compares post-quantum algorithm families and shows that lattice-based schemes usually provide high performance, hash-based schemes provide strong signature security, and code-based schemes provide conservative long-term security. This confirms that a hybrid approach can be more practical than relying on only one cryptographic family.

Table 1

Comparison of post-quantum cryptographic algorithm families [1]

Algorithm family	Example algorithm	Main function	Main advantage	Main limitation
Lattice-based	CRYSTALS-Kyber	Encryption / KEM	High speed and compact parameters	Requires correct parameter selection
Hash-based	XMSS	Digital signature	Strong hash-based security	Stateful key management
Code-based	Classic McEliece	Key exchange	Strong long-term security	Large public key size

ISSN 3030-3907

Multivariate-based	Rainbow/HFE	Signature/encryption	Fast computation	Security concerns in some schemes

RESEARCH METHODOLOGY.

The methodology of this study is based on structural modeling and performance-aware analysis of hybrid post-quantum cryptographic systems. The proposed model uses the same algorithmic foundation as the uploaded article, but it adds an adaptive decision module to improve flexibility.

The proposed model consists of three main cryptographic layers. The first layer is the key establishment layer based on Classic McEliece. It is responsible for generating and exchanging a secure session key. The second layer is the encryption layer based on CRYSTALS-Kyber. It protects the transmitted data with fast quantum-safe encryption. The third layer is the authentication layer based on XMSS. It provides digital signature generation and message integrity verification.

The main difference between the proposed model and a static hybrid model is the adaptive decision module. This module analyzes system requirements before selecting cryptographic operations. For example, if the communication system requires high throughput, the model prioritizes Kyber-based encryption. If long-term authenticity is required, the model applies XMSS signatures. If conservative key exchange is required, Classic McEliece is used.

Mathematical model

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

$$T_{total} = T_{key} + T_{enc} + T_{sig} + T_{ver} + T_{net}$$

where:

T_{total} is the total time required for secure data transmission;

T_{key} is the key exchange time;

T_{enc} is the encryption time;

T_{sig} is the digital signature generation time;

T_{ver} is the signature verification time;

T_{net} is the network transmission delay.

ISSN 3030-3907

The efficiency coefficient of the adaptive hybrid cryptographic model can be expressed as:

$$E = \frac{S}{T_{total} \times R}$$

where:

E

is the efficiency coefficient;

S

is the security level of the system;

T_{total}

is the total processing time;

R

is the resource consumption factor.

This formula shows that the efficiency of the system increases when the security level is high, while total processing time and resource consumption remain low.

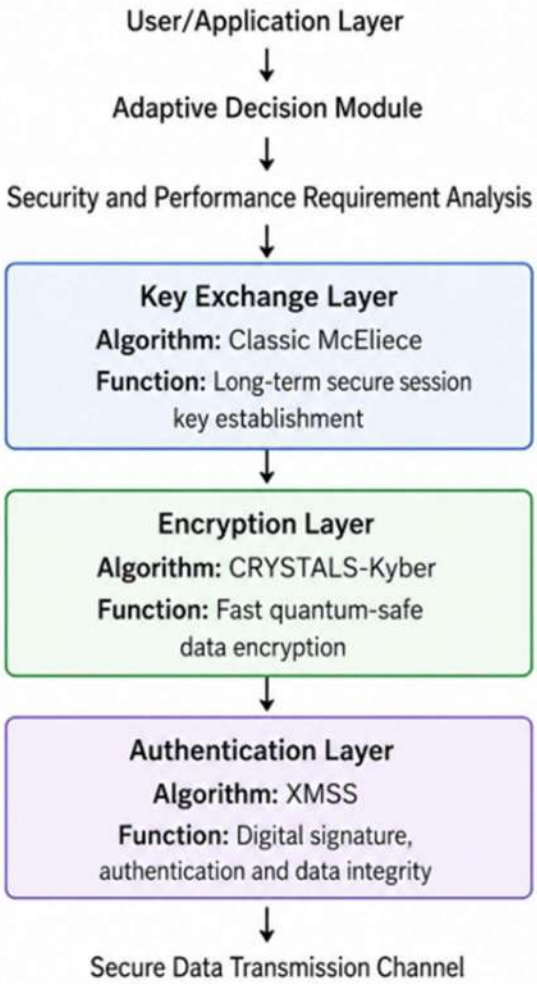


Fig. 1. Architecture of the adaptive hybrid post-quantum cryptographic model [1].

ISSN 3030-3907

The figure describes the workflow of the proposed model. First, the user or application sends a request to the adaptive decision module. Then, the module analyzes security and performance requirements. After that, Classic McEliece is used for secure key exchange, CRYSTALS-Kyber is applied for fast encryption, and XMSS is used for digital signature generation. Finally, the protected data is transmitted through a secure communication channel.

RESULTS AND DISCUSSION.

The proposed adaptive model improves the flexibility of hybrid post-quantum cryptographic systems. The uploaded article reports that Kyber has low encryption latency, XMSS provides moderate signature performance, and Classic McEliece offers strong key exchange security despite its large public key size. The execution time comparison chart in the source article also shows that Kyber performs encryption operations faster than XMSS and McEliece, while McEliece requires more time mainly because of its key generation and key size overhead.

Table 2

Functional role of algorithms in the proposed adaptive model

Layer	Algorithm	Function	Main advantage	Limitation
Key exchange	Classic McEliece	Secure session key establishment	Strong long-term security	Large public key size
Encryption	CRYSTALS-Kyber	Fast data protection	Low latency and high throughput	Requires correct parameter selection
Authentication	XMSS	Digital signature	Strong hash-based security	Stateful key management

According to the benchmark values presented in the source article, McEliece key generation takes approximately 5.12 ms, Kyber encryption takes approximately 0.45 ms, and XMSS signature generation takes approximately 1.75 ms [1]. These results show that each algorithm has a different performance profile. Therefore, assigning a separate cryptographic function to each algorithm is more efficient than using one algorithm for all security operations.

Table 3

Performance indicators used for adaptive evaluation [1]

Operation type	Algorithm	Average time	Practical meaning

ISSN 3030-3907

Key generation	Classic McEliece	5.12 ms	Suitable for session-level key establishment
Encryption	Kyber768	0.45 ms	Suitable for high-speed message encryption
Signature	XMSS SHA2-256	1.75 ms	Suitable for authentication and integrity control

The adaptive decision module is the main novelty of the proposed approach. It allows the system to choose the most suitable cryptographic configuration depending on communication requirements. In cloud systems, the model can prioritize throughput and encryption speed. In government or military communication, it can prioritize long-term key security. In IoT environments, it can reduce heavy key exchange operations and reuse secure session configurations when appropriate.

Table 4

Expected performance impact of the adaptive hybrid model

Evaluation criterion	**Expected result**
Security level	High
Encryption speed	High due to CRYSTALS-Kyber
Signature reliability	High due to XMSS
Key exchange security	Strong due to Classic McEliece
Flexibility	Improved through adaptive decision logic
Implementation complexity	Medium to high

The main advantage of the proposed model is cryptographic diversity. Since Kyber, XMSS, and Classic McEliece are based on different mathematical assumptions, the failure of one algorithm family does not automatically compromise the entire system. This is important for long-term quantum-safe infrastructures.

However, several limitations must be considered. Classic McEliece has a large public key size, which may increase memory and bandwidth requirements. XMSS requires state management, and incorrect state handling may create

ISSN 3030-3907

security risks. In addition, combining several algorithms increases protocol complexity and requires careful implementation.

CONCLUSION AND RECOMMENDATIONS.

This article proposed an adaptive hybrid post-quantum cryptographic model for secure data transmission. The proposed model is connected with the uploaded study on a hybrid post-quantum cryptographic framework based on CRYSTALS-Kyber, XMSS, and Classic McEliece.

The study shows that CRYSTALS-Kyber is suitable for fast encryption, XMSS is reliable for digital signatures, and Classic McEliece provides strong long-term key exchange. Their combination creates a layered and flexible cryptographic architecture for quantum-safe secure communication.

The proposed mathematical model allows the system to estimate total processing time and evaluate efficiency according to security level and resource consumption. This can be useful for cloud platforms, IoT systems, government networks, banking systems, and critical infrastructure protection.

Future research should focus on experimental implementation of the adaptive decision module, automatic parameter selection, optimization of Classic McEliece key storage, secure XMSS state management, and integration with post-quantum TLS and VPN protocols.

REFERENCES

1. T. Khudaybergenov, T. Turdiyev, T. Khudayberganov, and B. Sabirov, “Hybrid Post-Quantum Cryptographic Framework for High-Performance Secure Data Transmission,” 2025 IEEE XVII International Scientific and Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE), 2025.

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. J. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, “Post-quantum key exchange — A New Hope,” Proceedings of the USENIX Security Symposium, pp. 327–343, 2016.

5. L. K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 1996.

6. P. Schwabe, D. Kales, M. Kölbl, and S. Mehrabi, “Benchmarking CRYSTALS-Kyber and Dilithium,” Proceedings of PQCrypto, pp. 198–226, 2020.

ISSN 3030-3907

7. A. Hülsing, D. Butin, S. Gazdag, and J. Rijneveld, “XMSS: Extended Merkle Signature Scheme,” IETF RFC 8391, pp. 1–59, 2018.
8. A. Hülsing, “On Stateless and Stateful Hash-Based Signatures,” Proceedings of PQCrypto, pp. 1–15, 2014.
9. R. J. McEliece, “A Public-Key Cryptosystem Based on Algebraic Coding Theory,” DSN Progress Report, Jet Propulsion Laboratory, Pasadena, CA, USA, pp. 114–116, 1978.
10. D. J. Bernstein, T. Lange, C. van Vredendaal, T. Chou, T. Hülsing, S. R. Lucks, and R. Misoczki, “Classic McEliece: Submission to NIST PQC Project,” NIST PQC Submission Document, pp. 1–40, 2019.

ISSN 3030-3907