Ербол Амангазович Оспанов* – PhD, доцент, Университет Шәкәрім, Семей; e-mail: y.ospanov@shakarim.kz. ORCID: https://orcid.org/0000-0001-5342-274X.
Ардақ Мергенбаевна Ахметова – phD, доцент, Казахский национальный университет имени аль-Фараби, Алматы;e-mail: ardak_66@gmail.com. ORCID: https://orcid.org/0000-0001-8360-5504.
Нурлан Садуакасович Сарсенбаев – кандидат технических наук, доцент, Казахский национальный исследовательский технический университет имени К. Сатпаева, Алматы; e-mail: n_sarsenbayev75@satbayev.university. ORCID: https://orcid.org/0000-0001-8640-7175.
Акамбай Агыбайович Бейсембаев – кандидат технических наук, доцент, Казахский национальный исследовательский технический университет имени К. Сатпаева, Алматы; e-mail: akambaybeisembayev@gmail.com. ORCID: https://orcid.org/0000-0002-4763-0769.

Information about the authors

Askhat Asset – PhD doctoral student, Senior Lecturer, Al-Farabi Kazakh National University, Almaty; e-mail: asset.askhat.81@gmail.com. ORCID: https://orcid.org/0009-0005-8842-328X.
Yerbol Ospanov* – PhD, Associate Professor, Shakarim University, Semey; e-mail: y.ospanov@shakarim.kz. ORCID: https://orcid.org/0000-0001-5342-274X.
Ardak Mergenbaevna Akhmetova – PhD, Associate Professor, Al-Farabi Kazakh National University, Almaty; e-mail: ardak_66@gmail.com. ORCID: https://orcid.org/0000-0001-8360-5504.
Nurlan Saduakasovich Sarsenbayev – Candidate of Technical Sciences, Associate Professor, Kazakh National Research Technical University named after K. Satpayev, Almaty; e-mail: n_sarsenbayev75@satbayev.university. ORCID: https://orcid.org/0000-0001-8640-7175.
Akambay Agybayovich Beisembaev – Candidate of Technical Sciences, Associate Professor, Kazakh National Research Technical University named after K. Satpayev, Almaty; e-mail: akambaybeisembayev@gmail.com. ORCID: https://orcid.org/0000-0002-4763-0769.

Редакцияға енуі 06.04.2026
Өңдеуден кейін түсуі 17.08.2026
Жариялауға қабылданды 18.08.2026

https://doi.org/10.53360/2788-7995-2026-3(23)-19

МРНТИ: 81.93.29

A.T. Kerimbayeva
Satbayev University,
050000, Republic of Kazakhstan, Almaty, 22 Satbayev St.
e-mail: aygerim744@gmail.com

MATHEMATICAL MODEL AND COMPUTATIONAL ANALYSIS OF A LIGHTWEIGHT LATTICE-BASED SIGNATURE FOR IOT DEVICES

Abstract: *This paper details a mathematical model and a performance evaluation of FALCON-M, a novel, lightweight post-quantum signature scheme specifically engineered for Internet of Things (IoT) applications. The importance of this contribution is underscored by the imperative to secure IoT devices from future quantum attacks, a challenge not adequately met by existing standards like Falcon and Dilithium, which are too demanding for resource-constrained settings owing to their use of rejection sampling and floating-point computations. Our study seeks to close the gap between theoretical post-quantum cryptographic solutions and their feasible integration into embedded systems.*

The proposed scheme is based on a lattice-based signature defined over the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ *with parameters* $n = 512$, $q = 12289$, $\sigma = 4.0$, $\tau = 60$. *A key feature is the complete absence of rejection sampling, which guarantees deterministic execution time and inherent resistance to timing side-channel attacks.*

Analysis reveals that the scheme achieves notably small key sizes: the public key is 928 bytes, the secret key is 256 bytes, and the signature is 973 bytes. Projections for performance on an ARM Cortex-M4 processor operating at 100 MHz indicate a signing duration of 7.4 ms. This speed is comparable to established post-quantum cryptography methods, yet it provides superior resilience against side-channel vulnerabilities.

©A.T. Kerimbayeva, 2026

The primary scientific advancement is the creation of a mathematically rigorous model that avoids the shortcomings of existing approaches. Its practical importance is demonstrated by its applicability to a broad spectrum of Internet of Things devices, including intelligent sensors, implanted medical devices, and industrial control systems.

Key words: *post-quantum cryptography, digital signature, Internet of Things, lattices, FALCON.*

1. Introduction

The accelerating development of quantum computing presents a fundamental vulnerability to current public key cryptography, including RSA and ECC. Quantum algorithms like Shor's and Grover's are capable of efficiently breaking these schemes, rendering them inadequate for enduring security. In response, the cryptographic community has devised post-quantum cryptography (PQC), culminating in NIST-standardized digital signatures: ML DSA (Dilithium), FN DSA (Falcon), and SLH DSA (SPHINCS+). However, the practical deployment of these theoretically secure algorithms on resource-limited Internet of Things (IoT) devices is problematic. Dilithium's dependence on rejection sampling leads to variable execution times, a critical issue for real-time systems and devices reliant on battery power. Falcon's reliance on a trapdoor mechanism and floating-point calculations imposes significant computational and memory burdens on typical microcontrollers. SPHINCS+ generates signatures that are orders of magnitude larger than what many IoT applications can accommodate. To mitigate these limitations, we propose FALCON M, a resource-efficient post-quantum signature scheme built upon ring lattices. This scheme removes the need for rejection sampling and trapdoor constructions, ensuring deterministic timing and constant-time operations. It exclusively utilizes integer arithmetic and is engineered to fit within the stringent memory constraints of IoT devices.

This research aims to develop a mathematical framework for FALCON M and assess its efficiency via a computational complexity examination. Our findings indicate that the system offers reduced key and signature dimensions (928 B for the public key, 256 B for the private key, and 973 B for the signature). Furthermore, by estimating cycle counts, we project an execution time of approximately 7.4 ms on a 100 MHz ARM Cortex M4 microcontroller, rendering it a practical choice for numerous Internet of Things deployments.

2. Materials and Methods

2.1. Mathematical Model

The scheme operates in the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ with the following parameters:

- $n = 512$ – ring dimension
- $q = 12289$ – prime modulus, satisfying $q \equiv 1(\mathrm{mod}2n)$ for NTT compatibility
- $\sigma = 4.0$ – standard deviation of the discrete Gaussian distribution $\mathcal{D}_\sigma$
- $\tau = 60$ – Hamming weight of the sparse challenge polynomial c
- $\delta = 50$ – verification bound for the infinity norm

All polynomial operations (addition, multiplication) are performed modulo q and modulo $x^{512} + 1$. Multiplication is accelerated via the Number Theoretic Transform (NTT), which has complexity $O(n \log n)$.

Key Generation (KeyGen).

The secret key consists of two small polynomials $s_1, s_2 \in \{-1,0,1\}^n$. The public key is a pair (a, t), where $a \in R_q$ is uniformly random (expanded from a 32-byte seed), and

$$t = as_1 + s_2(\mathrm{mod}q).$$

Signature Generation (Sign).

For a message m, the signature $\sigma = (z_1, z_2, c)$ is generated as:

1. Sample ephemeral noise $y_1, y_2 \leftarrow \mathcal{D}_\sigma$.
2. Compute commitment $w = ay_1 + y_2(\mathrm{mod}q)$.
3. Derive challenge $c = \mathrm{EncodeChallenge}\big(H(\mathrm{DS} \parallel m \parallel w)\big)$, where H is SHAKE-256 (512-bit output) and $\mathrm{EncodeChallenge}$ maps the hash to a sparse polynomial with exactly τ non-zero coefficients ± 1.
4. Compute responses $z_1 = y_1 + cs_1$, $z_2 = y_2 + cs_2$. The algorithm contains **no rejection sampling**; the execution path is deterministic.

Verification (Verify).

To verify a signature σ for message m:

1. Check $\| z_1 \|_\infty \leq \delta$ and $\| z_2 \|_\infty \leq \delta$.
2. Reconstruct $w' = az_1 + z_2 - ct(\mathrm{mod}q)$.

3. Compute $c' = \mathrm{EncodeChallenge}\big(H(\mathrm{DS} \parallel m \parallel w')\big)$.

4. Accept if $c' = c$ (constant-time comparison).

2.2. Performance Evaluation Methodology

To estimate performance on a representative IoT microcontroller, we use a cycle-counting **approach**. The target platform is an ARM Cortex-M4 processor running at 100 MHz, a common choice for resource-constrained devices [1]. The computational cost is measured in terms of elementary operations that can be mapped directly to CPU cycles.

We count the number of NTT butterfly operations, modular multiplications, additions/subtractions, and hash function calls required for each algorithm. The NTT length is $N_{\text{ntt}} = 1024$ (for $n = 512$). One NTT forward/inverse transform consists of $N_{\text{ntt}} \log_2 N_{\text{ntt}} = 10240$ butterflies. Each butterfly comprises:

- 1 modular multiplication
- 2 modular additions/subtractions
- 1 memory access

Efficient NTT implementations for lattice-based cryptography are well studied [11, 12].

These counts are derived from the algorithmic descriptions and include all necessary operations (NTTs for polynomials, pointwise multiplications, additions, etc.). They are independent of the specific implementation and provide a hardware-neutral measure of complexity.

2.3. Packing Schemes

All keys and signatures are stored in packed binary format to minimise memory footprint. The packing methods are as follows:

- Public key: The polynomial a is stored as a 32-byte seed. The polynomial t is encoded using 14 bits per coefficient, because its coefficients lie in the range $[0, q-1]$ with $q = 12289 < 2^{14}$.
- Secret key: The polynomials s_1, s_2 are encoded using 2 bits per coefficient, mapping the values $-1,0,1$ to 0, 1, 2 respectively.

Signature:

- The responses z_1, z_2 are encoded using 7 bits per coefficient.
- The challenge polynomial c (which has exactly $\tau = 60$ non-zero coefficients ± 1) is stored by listing the positions of its non-zero entries using 9 bits each, together with their signs using 1 bit each.

These encodings are designed to achieve compact representation while preserving the ability to efficiently unpack the data during verification.

3.1. Performance Evaluation

To estimate the computational cost on a typical IoT microcontroller, we counted the number of elementary operations required for each algorithm. The counts are based on the algorithmic descriptions and the NTT implementation details (see Section 2.2). The following assumptions, derived from previous performance analyses of lattice-based schemes [13], were made:

- NTT is implemented in-place with length $N_{\text{ntt}} = 1024$.
- One NTT butterfly consists of:
- 1 modular multiplication,
- 2 modular additions/subtractions,
- 1 assignment (or permutation).
- Polynomial multiplication via NTT requires:
- 2 forward NTTs, 1 inverse NTT → **3 transforms**,
- plus pointwise multiplication (1024 multiplications).
- Pointwise multiplication counts as 1 multiplication per coefficient.
- Polynomial addition/subtraction requires n operations.
- Gaussian sampling uses a constant-time CDT table (no loops); each sample is estimated as 2–3 arithmetic operations plus a table lookup.
- Hashing (SHAKE-256) is counted as a single call; on an MCU this may take several thousand cycles, but for relative comparison it is treated separately.

The operation counts for KeyGen, Sign, and Verify are presented in Tables 1-3.

Table 1 –. Operation counts for KeyGen

Step	Description	Count
1	Generate a from seed	1 SHAKE-256 call
2	Generate s_1, s_2	2×512 random numbers (~1024 ops)
3	Multiply $a \cdot s_1$ via NTT	3×10240 butterflies + 1024 pointwise multiplications
4	Add $as_1 + s_2$	512 additions
Total NTT butterflies		30 720
Total modular multiplications		~31 744
Total additions/subtractions		~31 232

Table 2 – Operation counts for Sign

Step	Description	Count
1	Generate y_1, y_2 (Gaussian)	2×512 CDT lookups
2	NTT for y_1, y_2	$2 \times 10\,240$ butterflies
3	Pointwise multiplication $a \cdot y_1$	1 024 multiplications
4	Add $ay_1 + y_2$ (NTT domain)	1 024 additions
5	INTT for w	10 240 butterflies
6	Hashing (SHAKE-256)	1 call
7	NTT for c	10 240 butterflies
8	NTT for s_1, s_2	(cached) 0
9	Pointwise multiplications $c \cdot s_1, c \cdot s_2$	$2 \times 1\,024$ multiplications
10	INTT for z_1, z_2	$2 \times 10\,240$ butterflies
11	Symmetric reduction	2×512 comparisons/subtractions
12	Packing	bit operations (negligible)
Total NTT butterflies		61 440
Total modular multiplications		~64 512
Total additions/subtractions		~63 488

Table 3 – Operation counts for Verify

Step	Description	Count
1	Check $\| z_1 \|_\infty, \| z_2 \|_\infty \leq \delta$	2×512 comparisons
2	NTT for z_1, z_2	$2 \times 10\,240$ butterflies
3	Pointwise multiplication $a \cdot z_1$	1 024 multiplications
4	NTT for c	10 240 butterflies
5	NTT for t	10 240 butterflies
6	Pointwise multiplication $c \cdot t$	1 024 multiplications
7	Add/subtract for w'	$2 \times 1\,024$ operations
8	INTT for w'	10 240 butterflies
9	Hashing (SHAKE-256)	1 call
10	NTT for c' (implicit in encode_challenge)	10 240 butterflies
11	Constant-time comparison of c and c'	512 comparisons
Total NTT butterflies		61 440
Total modular multiplications		~2 048
Total comparisons/additions		~3 584

Assuming an optimised NTT implementation on an ARM Cortex-M4 microcontroller running at 100 MHz, where each butterfly takes approximately 12 cycles [12], the signing time is estimated as:

$$T_{\text{sign}} = \frac{61\,440 \times 12}{100 \times 10^6} \approx 7.4 \text{ ms.}$$

Verification requires a similar number of NTT butterflies and thus is expected to take about the same time. These estimates indicate that FALCON-M can perform a full signing operation within a few milliseconds, which is suitable for a wide range of IoT applications.

3.2. Summary of Operation Counts

For a quick overview, Table 4 summarises the total number of elementary operations for each algorithm.

Table 4 – Summary of operation counts for FALCON-M

Algorithm	NTT butterflies	Modular multiplications	Additions/comparisons	SHAKE-256 calls
KeyGen	30 720	~31 744	~31 232	1
Sign	61 440	~64 512	~63 488	1
Verify	61 440	~2 048	~3 584	1

The data show that the signing and verification operations are dominated by NTT butterflies (over 60 000 each), while KeyGen requires about half that number. Modular multiplications follow a similar pattern. The SHAKE-256 hash function is called once per operation and does not constitute a bottleneck.

Based on these figures and assuming an optimised NTT implementation on an ARM Cortex-M4 at 100 MHz (12 cycles per butterfly), the signing time is estimated to be approximately 7.4 ms. Verification is expected to take a comparable amount of time. These results confirm that FALCON-M is suitable for resource-constrained IoT devices.

4. Discussion

The proposed FALCON-M signature scheme is designed for resource-constrained IoT devices. The operation counts show that signing requires about 61 440 NTT butterflies, which translates to an estimated 7.4 ms on a 100 MHz ARM Cortex-M4 (assuming 12 cycles per butterfly [14]). This performance is adequate for typical IoT scenarios such as sensor authentication and firmware updates.

The deterministic nature of FALCON-M, achieved by eliminating rejection sampling, guarantees predictable execution time. This advancement streamlines the process of predicting energy usage for battery-operated gadgets and eliminates a significant vulnerability related to timing information [6, 7]. Furthermore, the exclusion of a trapdoor feature and the avoidance of floating-point calculations contribute to a less complex design for microcontrollers [8,11].

The performance estimates are derived from operation counts and assumed cycle counts; actual hardware measurements may differ.

Future directions include an optimised C++ implementation on ARM Cortex-M and RISC-V platforms, integration into real IoT protocols, and a formal security proof in the QROM model.

5. Conclusions

The presented work introduces FALCON M, a lightweight post-quantum signature scheme specifically tailored for IoT devices. The scheme's design obviates the necessity for rejection sampling and trapdoor mechanisms, thereby ensuring deterministic execution and a simplified integer-only implementation. Performance estimations, derived from operation counts, project a signing time of approximately 7.4 ms on a 100 MHz ARM Cortex M4 microcontroller. These outcomes validate FALCON M's appropriateness for a wide array of IoT applications.

References

1. Atzori L. The Internet of Things: A Survey / L. Atzori, A. Iera, G. Morabito // Computer Networks. – 2010. – Vol. 54, № 15. – P. 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010.

2. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P.W. Shor // SIAM Journal on Computing. – 1997. – Vol. 26, № 5. – P. 1484-1509. https://doi.org/10.1137/S0097539795293172.

3. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA) [Electronic resource]. – Gaithersburg: NIST, 2024. https://doi.org/10.6028/NIST.FIPS.204 (accessed: 11.03.2026).

4. National Institute of Standards and Technology. FIPS 206: NTRU-Based Digital Signature Standard (FN-DSA) (Draft) [Electronic resource]. – Gaithersburg: NIST, 2024.
5. Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures / V. Lyubashevsky // Advances in Cryptology – ASIACRYPT 2009: Proc. Intern. Conf. – Berlin: Springer, 2009. – P. 598-616. https://doi.org/10.1007/978-3-642-10366-7_35.
6. CRYSTALS-Dilithium: Digital Signatures from Module Lattices / L. Ducas et al // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2018. – Vol. 2018, № 1. – P. 238-268. https://doi.org/10.13154/tches.v2018.i1.238-268.
7. FALCON / T. Prest et al. – Gaithersburg: NIST, 2020. – Technical Report.
8. Oder T. Implementing the Candidate FALCON Signature Scheme on Embedded Devices / T. Oder, T. Güneysu // 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Proc. Intern. Conf. – Piscataway: IEEE, 2019. – P. 272-281.
9. Lyubashevsky V. On Ideal Lattices and Learning with Errors over Rings / V. Lyubashevsky, C. Peikert, O. Regev // Journal of the ACM. – 2013. – Vol. 60, № 6. – P. 1-35. https://doi.org/10.1145/2535925.
10. The SPHINCS+ Signature Framework / D.J. Bernstein et al // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19): Proc. Intern. Conf. – New York: ACM, 2019. – P. 2129-2146. https://doi.org/10.1145/3319535.3363229.
11. Micciancio D. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller / D. Micciancio, C. Peikert // Advances in Cryptology – EUROCRYPT 2012: Proc. Intern. Conf. – Berlin: Springer, 2012. – P. 700-718. https://doi.org/10.1007/978-3-642-29011-4_41.
12. Longa P. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography / P. Longa, M. Naehrig // Cryptology and Network Security – CANS 2016: Proc. Intern. Conf. – Cham: Springer, 2016. – P. 124-139. https://doi.org/10.1007/978-3-319-48965-0_8.
13. Testing and Benchmarking NIST PQC on ARM Cortex-M4 / M.J. Kannwischer et al // IACR Cryptology ePrint Archive. – 2019. – № 844. https://api.semanticscholar.org/CorpusID:201059112.
14. ARM Ltd. ARM Cortex-M4 Processor Technical Reference Manual. – Cambridge: ARM, 2020.

Acknowledgement

The authors express their gratitude to the Vice-Rector for Science and Corporate Development of Satbayev University, Yerzhan Kuldeyev, for the support in securing the funding for this research.

Ә.Т. Керімбаева
Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті,
050000 Қазақстан Республикасы, Алматы қ., Сәтбаев көш.22.
e-mail: aygerim744@gmail.com

IOT ҚҰРЫЛҒЫЛАРЫНА АРНАЛҒАН ЖЕҢІЛ ТОРЛЫ (LATTICE-BASED) ҚОЛТАҢБАНЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛІ ЖӘНЕ ЕСЕПТЕУ ТАЛДАУЫ

Бұл мақалада Интернет заттары (IoT) құрылғыларына арналған жеңіл пост-кванттық қолтаңба схемасы FALCON-M математикалық моделі және өнімділігін бағалау ұсынылған. Өзектілігі IoT құрылғыларын кванттық шабуылдардан қорғау қажеттілігімен түсіндіріледі, ал қолданыстағы стандарттар (Falcon, Dilithium) rejection sampling және өзгермелі нүктелі амалдардың кесірінен ресурсы шектеулі орталарға жарамсыз. Зерттеу теориялық пост-кванттық криптография мен ендірілген платформаларда практикалық орналастырарасындағы алшақтықты жоюға бағытталған. Ұсынылып отырған схема параметрлері n=512, q=12289, $\sigma = 4.0, \tau = 60$ болатын $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ сақинасында анықталған торға негізделген қолтаңбаға негізделген. Басты ерекшелігі – rejection sampling-нің толық болмауы, бұл детерминирленген орындалу уақытын және уақытша жанама арналар шабуылдарына төзімділікті қамтамасыз етеді.

Нәтижелер ықшам өлшемдерді көрсетеді: ашық кілт 928 байт, жабық кілт 256 байт, қолтаңба 973 байт. 100 МГц жиіліктегі ARM Cortex-M4 үшін бағалау қолтаңба уақыты 7.4 мс екенін көрсетеді, бұл қолданыстағы пост-кванттық схемалармен бәсекеге қабілетті, сонымен қатар жанама арналарға төзімділігі жағынан артықшылыққа ие. Ғылыми үлес – қолданыстағы схемалардың кемшіліктерінен ада математикалық негізделген модельді әзірлеу; практикалық

маңыздылығы – схеманың ақылды сенсорлар, медициналық имплланттар және өнеркәсіптік контроллерлерді қоса алғанда, IoT құрылғыларының кең ауқымына жарамдылығын көрсету.

Түйін сөздер: *постквантты криптография, цифрлық қолтаңба, заттар интернеті, торлар, FALCON.*

А.Т. Керимбаева
Казахский национальный исследовательский технический университет имени К.И. Сатбаева,
050000 Республика Казахстан, г. Алматы, ул. Сатпаева, 22
e-mail: aygerim744@gmail.com

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И ВЫЧИСЛИТЕЛЬНЫЙ АНАЛИЗ ОБЛЕГЧЕННОЙ ПОДПИСИ НА РЕШЕТКАХ ДЛЯ УСТРОЙСТВ IOT

В данной статье представлены математическая модель и оценка производительности легковесной пост-квантовой схемы подписи FALCON-M, предназначенной для устройств интернета вещей (IoT). Актуальность обусловлена необходимостью защиты IoT-устройств от квантовых атак, в то время как существующие стандарты (Falcon, Dilithium) непригодны для ресурсно-ограниченных сред из-за использования rejection sampling и операций с плавающей точкой. Исследование направлено на преодоление разрыва между теоретической пост-квантовой криптографией и практическим развёртыванием на встраиваемых платформах.

Предлагаемая схема основана на решёточной подписи, определённой над кольцом $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ *с параметрами* $n = 512$, $q = 12289$, $\sigma = 4.0$, $\tau = 60$. *Ключевая особенность – полное отсутствие rejection sampling, что гарантирует детерминированное время выполнения и устойчивость к атакам по времени выполнения.*

Результаты показывают компактные размеры: открытый ключ 928 байт, закрытый ключ 256 байт, подпись 973 байта. Оценочное время подписи для ARM Cortex-M4 на частоте 100 МГц составляет 7.4 мс, что конкурентоспособно с существующими пост-квантовыми схемами и превосходит их по устойчивости к атакам по побочным каналам. Научный вклад заключается в разработке математически обоснованной модели, свободной от недостатков существующих схем; практическая значимость состоит в демонстрации пригодности схемы для широкого круга IoT-устройств, включая интеллектуальные датчики, медицинские импланты и промышленные контроллеры.

Ключевые слова: *постквантовая криптография, цифровая подпись, интернет вещей, решетки, FALCON.*

Сведения об авторе

Айгерим Танирбергеновна Керимбаева – магистр, кафедра кибербезопасности, Казахский национальный исследовательский технический университет имени К.И. Сатбаева, Казахстан; e-mail: aygerim744@gmail.com. ORCID: https://orcid.org/0000-0002-5762-8400.

Автор туралы мәліметтер

Әйгерім Тәңірбергенқызы Керімбаева – магистр, Киберқауіпсіздік кафедрасы, Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Қазақстан; e-mail: aygerim744@gmail.com. ORCID: https://orcid.org/0000-0002-5762-8400.

Information about the authors

Aygerim Kerimbayeva – Master of Science, Department of Cybersecurity, Satbayev University, Kazakhstan; e-mail: aygerim744@gmail.com. ORCID: https://orcid.org/0000-0002-5762-8400.

Received 01.06.2026
Revised 01.07.2026
Accepted 24.08.2026