publisher.agency
Denmark

February, 2026
№ 12



Copenhagen, Denmark
19-20.2.2026

International Scientific Conference

Foundations and Trends in Research

UDC 001.1
P 97

Publisher.agency: Proceedings of the 12th International Scientific Conference «Foundations and Trends in Research» (February 19-20, 2026). Copenhagen, Denmark, 2026. 217p

ISBN 978-6-9160-7223-2
DOI 10.5281/zenodo.18737655

Editor: Sofia Axelsson, Professor, University of Copenhagen
International Editorial Board:

Hanne Olofsson
Professor, Technical University of Denmark
Susanne Bergqvist
Professor, Copenhagen Business School
Oliver Bengtsson
Professor, Aarhus University
Peter Lundin
Professor, Roskilde University
Valdemar Gustafsson
Professor, Aalborg University
Mette Sjöberg
Professor, University of Southern Denmark
Rasmus Nilsson
Professor, West Jutland University College
Ole Björk
Professor, University College South
Kirsten Eriksson
Professor, Danish University of Pharmaceutical Science
Elliot Isaksson
Professor, Royal School of Library and Information Science
Daniel Olsson
Professor, Danish Pharmaceutical College
Lucas Engström
Professor, Pharmaceutical College, Copenhagen
Camilla Svensson
Professor, Danish School of Media and Journalism
Frederik Holmberg
Professor, University College Absalon

editor@publisher.agency
https://publisher.agency/

Table of Contents

Pedagogical Sciences

DEVELOPING GIFTED STUDENTS' INTELLECTUAL ABILITIES THROUGH DIFFERENTIATED INSTRUCTION BASED ON MODERN EDUCATIONAL TECHNOLOGIES IN BIOLOGY TEACHING 6
Orazkul I.S.
Omarova D.R.
Bekenova N.A.

МЕТОДЫ ФОРМИРОВАНИЯ НАВЫКОВ САМОРЕГУЛЯЦИИ У МЛАДШИХ ШКОЛЬНИКОВ ПОСРЕДСТВОМ ДИФФЕРЕНЦИРОВАННОГО ОБУЧЕНИЯ 17
Жусип Э.М.
Альмухамбетов Б.А.
Гювен М.

ФОРМИРОВАНИЕ ТВОРЧЕСКИХ РЕЧЕВЫХ НАВЫКОВ СТУДЕНТОВ ПРИ ОБУЧЕНИИ АНГЛИЙСКОМУ ЯЗЫКУ 27
Ш.Б. Калбергенова

AN INTEGRATIVE INNOVATIVE MODEL OF TEACHING AEROBICS AND COMPREHENSIVE PHYSICAL TRAINING IN HIGHER EDUCATION: EFFECTS ON STUDENTS' PHYSICAL ACTIVITY AND PSYCHOLOGICAL WELL-BEING 32
Turgenbayeva Aizhan Shokhanovna
Ali Maksat Esengeldievich
Ospanova Zhuldyz Kairatkizy
Rabatov Akyltay Abdimuratuly

VIRTUAL EDUCATION IN CHILE, AN EXAMPLE OF A NEW SPACE FOR LEARNING 36
Jose Manuel Salum Tomé

РАЗВИТИЕ ОБРАЗОВАТЕЛЬНОГО ЛИДЕРСТВА ЧЕРЕЗ ПОДГОТОВКУ РУКОВОДИТЕЛЕЙ: КАЗАХСТАНСКИЙ ОПЫТ И МЕЖДУНАРОДНЫЕ ПОДХОДЫ 43
Калиева Айым Космановна
Иргебаева Назиля Мукатаевна

Technical Sciences

INNOVATIVE TECHNOLOGIES IN THORIUM-BASED MOLTEN SALT REACTORS: COMPARATIVE ANALYSIS OF TMSR-LF1, COPENHAGEN ATOMICS DESIGN, AND BN-1200M ADAPTATION 48
Marat K. Baipakov
Zinetula Insepov
Zulkhair A. Mansurov

ФОРМАЛИЗАЦИЯ МОДЕЛИ УГРОЗ СЕРВЕРНЫХ КОМПОНЕНТОВ ВЕБ-ПРИЛОЖЕНИЙ В МИКРОСЕРВИСНОЙ АРХИТЕКТУРЕ С УЧЕТОМ МЕЖСЕРВИСНОГО ВЗАИМОДЕЙСТВИЯ 53
Жолдасов Темірлан Жанұлы
Майлыбаев Ерсайын Құрманбайұлы

TRANSITION TO POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS IN CRITICAL SOFTWARE: CHALLENGES AND STRATEGIES 67
Tamilla Bayramova
Ramin Mammadov

MULTIFUNCTIONAL ADDITIVES FOR LUBRICATING OILS 72
Kulaliev Ikram Jannatali oglu
Sadirzade Inara Aligeydar kizi
Gahramanova Konul Ramiz kizi
Ibragimova Tarana Muradaga kizi
Ismayilli Aytaj Sadig kizi
Almammadova Aygun Ershad kizi

АВТОМАТИЗАЦИЯ ДОКУМЕНТООБОРОТА С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ И АНАЛИЗА ТЕКСТОВ 74
Кырыкбаев А.М.
Бекбаева Р.С.

Medical Sciences

GASTRIC CANCER: MODERN DIAGNOSTIC AND CLINICAL STRATEGY 82
Arman Khozhayev
Lyalya Tashenova
Marzhan Sagynbekova
Akerke Koxegen
Dina Orynbassarova
Zhanar Chomchekova
Zhanerke Kuandykova
Dana Gabit

Transition to Post-Quantum Cryptographic Algorithms in Critical Software: Challenges and Strategies

Tamilla Bayramova
Institute of Information Technology, Baku, Azerbaijan
Ramin Mammadov

Abstract: This thesis presents a systematic analysis of the transition to post-quantum cryptography (PQC) in critical software, exploring the technical, organizational, and strategic aspects of this transformation. Critical challenges identified include increased key and signature sizes, higher computational requirements, compatibility issues with legacy systems, and the "harvest now, decrypt later" threat. The study formulates a comprehensive migration strategy based on the principles of crypto-agility, a hybrid approach, risk-based prioritization, and phased implementation. The findings are of critical importance for CISOs, security architects, cryptographic system developers, and policymakers shaping national cybersecurity strategies in the era of quantum computing.

Keywords: post-quantum cryptography, quantum computing, cryptographic migration, NIST standards, critical infrastructure, crypto-agility

INTRODUCTION

The rapid progress of quantum computing poses an existential threat to modern cryptographic infrastructure, as quantum computers utilizing Shor's algorithm are capable of compromising widely used systems such as RSA, ECC, and Diffie-Hellman [1]. The contemporary digital infrastructure of global society is fundamentally dependent on cryptographic systems that ensure the confidentiality, integrity, and authenticity of digital communications [2]. Public-key cryptography, based on the mathematical complexity of integer factorization (RSA) and discrete logarithms in elliptic curves (ECC), forms the bedrock of modern PKI infrastructure [3].

However, this paradigm faces an existential threat from quantum computing. In 1994, Peter Shor developed a quantum algorithm capable of solving factorization and discrete logarithm problems in polynomial time, rendering RSA and ECC cryptographically insecure in the presence of a sufficiently powerful quantum computer [4]. The critical urgency of this transformation is further amplified by the "harvest now, decrypt later" (HNDL) threat, where attackers are already collecting encrypted data today with the intent to decrypt it once quantum computers emerge. For data with long-term confidentiality requirements, this threat is a current reality.

In response, NIST initiated a multi-year standardization process for post-quantum cryptography, which culminated in the publication of three final FIPS standards in August 2024. This thesis explores the challenges and strategies for transitioning to post-quantum cryptography within the context of critical software.

This thesis explores the challenges and strategies of transitioning to post-quantum cryptography within the context of critical software, where requirements for security, reliability, and operational continuity are most stringent. We analyze the technical characteristics of post-quantum algorithms, identify critical migration challenges, and formulate a comprehensive strategy for a successful transition.

1. NIST POST-QUANTUM STANDARDS

In August 2024, NIST published three final standards, concluding a process initiated in 2016 that involved the evaluation of 82 candidates submitted by researchers from 25 countries [5], [6]:

FIPS 203: ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) represents a key encapsulation mechanism based on lattice cryptography. ML-KEM is designed to replace RSA and Diffie-Hellman in key establishment protocols such as TLS. Lattice-based cryptography relies on the mathematical complexity of problems in high-dimensional lattices, which remain difficult even for quantum computers. ML-KEM provides three security levels (128, 192, and 256 bits).

FIPS 204: ML-DSA (Module-Lattice-Based Digital Signature Standard) specifies a digital signature scheme also based on lattice cryptography. ML-DSA is intended to replace RSA and ECDSA signatures in applications requiring data authentication and integrity.

FIPS 205: SLH-DSA (Stateless Hash-Based Digital Signature Standard) presents an alternative digital signature scheme based on hash functions. SLH-DSA is built on more conservative cryptographic assumptions, making it attractive for applications with extreme long-term security requirements; however, it is characterized by significantly larger signature sizes.

NIST continues the standardization process for additional algorithms to ensure cryptographic diversity. The Falcon algorithm is in the final stages of standardization and offers more compact signatures compared to ML-DSA. The HQC (Hamming Quasi-Cyclic) mechanism is also undergoing standardization as an alternative to ML-KEM, based on code-based cryptography. Post-quantum algorithms possess fundamentally different characteristics compared to classical systems, specifically requiring significantly larger key and signature sizes. For instance, SLH-DSA exhibits extremely large signature sizes (nearly 8 KB). These increased dimensions have direct implications for bandwidth, storage, and overall system performance [7].

Table 1.

Comparative characteristics of cryptographic algorithms

Algorithm	Type	Public Key Size (Bytes)	Signature / Ciphertext Size (Bytes)	Quantum Resistance
RSA-2048	Classical	256	256	No
ECDSA P-256	Classical	32	64	No
ML-KEM-768	PQC (KEM)	1,184	1,088	Yes
ML-DSA-65	PQC (Signature)	1,952	3,309	Yes
SLH-DSA-128s	PQC (Signature)	32	7,856	Yes
Falcon-512	PQC (Signature)	897	666	Yes

2. CRITICAL MIGRATION CHALLENGES

Technical Challenges: Post-quantum algorithms are characterized by fundamentally different performance profiles. For resource-constrained systems, such as IoT devices and embedded systems, these requirements may pose a fundamental limitation. Post-quantum algorithms require significantly larger keys and produce larger signatures and ciphertexts, leading to cascading effects on bandwidth, storage, memory footprint, and latency. Protocols with strict packet size constraints may require a fundamental redesign [8]. Critical infrastructure often includes legacy systems with lifecycles measured in decades. Cryptography is deeply integrated

into network protocols (TLS, IPsec, SSH), authentication protocols (Kerberos, SAML, OAuth), and data formats (X.509 certificates, CMS, JWT). Migration necessitates the update of all these components.

Organizational Challenges: The first critically important step is a comprehensive inventory of all instances where cryptography is used within an organization. In modern distributed systems, cryptography may be embedded in applications, libraries, firmware, hardware security modules, and third-party components. Organizations must conduct a comprehensive risk assessment that considers data sensitivity, long-term confidentiality requirements, exposure to HNDL (Harvest Now, Decrypt Later) attacks, regulatory requirements, and operational criticality. Migration affects multiple systems, teams, and organizations. Post-quantum cryptography is a new field for most practitioners. Developers, architects, and security specialists require training to understand the characteristics of new algorithms and their associated best practices [9].

Economic and time challenges: The transition represents a significant investment, including software and firmware updates, hardware replacement, extensive testing, personnel training, and potential downtime. For large organizations, the cost may reach tens or hundreds of millions of dollars [10]. NIST has established a 2035 deadline for the complete removal of quantum-vulnerable algorithms from federal standards. During the transition period, systems must support both classical and post-quantum algorithms to ensure interoperability. This dual-mode operation increases complexity, the attack surface, and operational overhead.

4. MIGRATION STRATEGIES

1. Crypto-Agility: Crypto-agility represents a fundamental architectural principle that ensures a system's ability to adapt to changes in cryptographic algorithms without a fundamental redesign. Systems designed with crypto-agility abstract cryptographic primitives through well-defined interfaces, allowing the replacement of implementations without altering the application logic. Key principles of crypto-agility include algorithm abstraction, configuration-driven selection, centralized key management, as well as versioning and negotiation [11]. Investing in crypto-agility facilitates not only a smoother post-quantum migration but also provides resilience against future cryptographic breakthroughs.

2. Hybrid Approach: A hybrid approach combines classical and post-quantum algorithms within a single cryptographic operation, providing protection against both quantum and classical threats [12]. The security of a hybrid scheme is determined by the stronger of the two algorithms: if a post-quantum algorithm proves vulnerable to an unknown attack, the classical algorithm provides protection against classical computers; if a quantum computer becomes available, the post-quantum algorithm ensures security. The hybrid approach is particularly attractive for critical systems with extreme security requirements, where the cost of failure is catastrophic. Financial clearing systems, government communications, critical infrastructure control systems, and medical systems are prime candidates for a hybrid approach [13].

3. Risk-Based Prioritization: Limited resources necessitate a strategic prioritization of systems for migration. Critical factors include data sensitivity, long-term confidentiality requirements, operational criticality, regulatory requirements, and technical feasibility. A formal risk assessment process should quantitatively evaluate these factors to produce a prioritized roadmap for migration.

4. Phased Migration: Migration should follow a structured, phased approach:

- Inventory and Assessment: Comprehensive discovery of all cryptographic assets, assessment of the current state of crypto-agility, and risk assessment for system prioritization.
- Pilot Projects: Selection of representative systems for pilot migration, performance and compatibility testing, identification of issues in a controlled environment, and development of migration playbooks.
- Migration of Critical Systems: Priority migration of high-risk systems using a hybrid approach, extensive testing, and staged rollout with rollback capabilities.
- Mass Migration: Scaling the migration to the remaining systems, automating migration processes, and continuous performance monitoring.
- Deprecation of Classical Algorithms: Upon completion of migration, a planned deprecation of classical quantum-vulnerable algorithms according to a clear timeline.

CONCLUSION

The transition to post-quantum cryptography represents one of the most significant transformations in the history of digital security, comparable in scale to the migration from DES to AES or the widespread implementation of PKI infrastructure. The quantum computing threat to modern cryptography is not hypothetical but a real and present danger requiring immediate action, particularly in the context of "harvest now, decrypt later" attacks that may already be occurring today.

The publication of NIST standards FIPS 203, 204, and 205 in August 2024 marks a critical milestone, providing the cryptographic foundation for protection against quantum threats. These standards, based on years of rigorous cryptanalysis by the international community, provide confidence in the security of post-quantum algorithms. However, the existence of standards is only the first step; the actual migration of critical infrastructure represents a massive engineering, organizational, and economic challenge.

This thesis has identified the critical challenges of migration, including technical complexities related to increased key and signature sizes, performance, and compatibility; organizational challenges of inventory, prioritization, and coordination; as well as economic and time constraints. These challenges are especially acute for critical software, where requirements for security, reliability, and operational continuity are most stringent.

A comprehensive migration strategy based on the principles of crypto-agility, a hybrid approach, risk-based prioritization, and phased implementation provides a pragmatic framework for a successful transition. Crypto-agility ensures architectural flexibility for adaptation to changes. The hybrid approach balances protection against quantum threats with hedging against potential vulnerabilities in new algorithms. Risk-based prioritization optimizes the use of limited resources, while a phased approach manages complexity and minimizes operational risk.

It is critically important that post-quantum migration begins immediately. While the NIST 2035 deadline may seem distant, considering the scale and complexity of migration in large organizations with extensive legacy infrastructure, many are already within a critical time window. Delaying migration increases exposure to quantum threats and the risk of regulatory non-compliance.

Post-quantum migration is not only a technical challenge but also an opportunity to fundamentally improve an organization's cryptographic hygiene and security posture. The process of inventorying cryptographic assets, assessing risk exposure, and implementing crypto-agile architectures provides long-term benefits beyond post-quantum migration, creating a more resilient and adaptable security infrastructure.

The success of post-quantum migration requires a coordinated effort at the level of industry, governments, and the international community. Standards bodies, vendors, researchers, practitioners, and policymakers must collaborate to address technical challenges, share best practices, and ensure interoperability. Only through such a collective effort can the global digital society successfully navigate this fundamental transformation and ensure security in the era of quantum computing.

References

[1] Buchanan, W., & Woodward, A. (2017). Will quantum computers be the end of public key encryption? Journal of Cyber Security Technology, 1(1), 1-22.

[2] Bayramova, T. A., & Malikova, N. C. (2024). Developing a conceptual model for improving the software system reliability. Problems of Information Society, 42-56.

[3] Moody, D., et al. (2024). NIST IR 8547: Transition to Post-Quantum Cryptography Standards. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8547/ipd

[4] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134.

[5] NIST. (2024). Post-Quantum Cryptography PQC. National Institute of Standards and Technology.

[6] Saarinen, M. J., & Smith-Tone, D. (Eds.). (2024). Post Quantum Cryptography: 15th International Workshop, PQCrypto 2024. Springer.

[7] Azhari, R., & Salsabila, A. N. (2024). Analyzing the impact of quantum computing on current encryption techniques. IAIC Transactions on Sustainable Digital Innovation, 5(2). https://aptikom-journal.id/itsdi/article/view/662

[8] Хайруллин, Р. Р., & Лаптева, М. Г. (2025). Кибербезопасность в эпоху постквантовой криптографии. Вестник науки, 1(82).

[9] Ajala, O. A., et al. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. Magna Scientia Advanced Research and Reviews, 10(2).

[10] Swedroe, L. (2024). The Quantum Computing Threat to Financial Systems. Substack. https://larryswedroe.substack.com/p/the-quantum-computing-threat-to-financial

[11] NCCoE. (2024). Migration to Post-Quantum Cryptography Project. National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[12] Google. (2026). The quantum era is coming. Are we ready to secure it? Google Blog. https://blog.google/innovation-and-ai/technology/safety-security/the-quantum-era-is-coming-are-we-ready-to-secure-it/

[13] Seiler, G. (2024). Quantum Computing and the Future of Encryption. Scholarly Review Journal, 3(1).