QUANTUM CRYPTOGRAPHY AND POST-QUANTUM SECURITY: CURRENT STATE, CHALLENGES, AND STRATEGIC DIRECTIONS

UDC: 004.056.55:530.145
DOI: https://doi.org/10.53486/tids2025.02

ZGUREANU AURELIU
Academy of Economic Studies of Moldova
zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

ANDRONATIEV VICTOR
Academy of Economic Studies of Moldova
andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

Abstract. Quantum cryptography is a new field of research that tries to resolve the critical security concerns brought by quantum computing. There is an increasing effort to construct quantum-safe cryptographic solutions due to the threat that quantum algorithms, especially Shor's and Grover's, pose to popular cryptographic systems. Traditional cryptographic methods like RSA and ECC are based on problems that will be efficiently tackled by quantum computers, putting them at risk in a post-quantum world. Also, symmetric cryptography, despite being stronger against that threat, faces its own challenges as well, especially from Grover's algorithm, which effectively slashes the key length by half, increasing the necessary key size for maintaining security.

The rise of quantum technologies has come with additional risks such as cyber threats and security vulnerabilities, therefore creating a need for research in quantum as well as post-quantum cryptography. Quantum cryptography particularly Quantum Key Distribution (QKD) exploits quantum mechanical phenomena to safeguard the exchange of cryptographic keys with information-theoretic security. Eavesdropping in QKD is always detectable. However, due to stringent hardware requirements, QKD is limited for broader practical use. Meanwhile, post-quantum cryptography (PQC) seeks to devise traditional algorithms for cryptography which will continue to remain secure under attacks from quantum computers. Such algorithms include lattice-based cryptography and code-based cryptography which, among others, are being standardized by NIST.

This paper examines the current status of quantum cryptography alongside the vulnerabilities present in traditional systems as well as the efforts dedicated to implementing post-quantum algorithms. It covers the standardization and implementation challenges while also outlining prospective future research avenues aimed at reinforcing the cryptographic infrastructure in the era of quantum computing.

Keywords: Quantum Cryptography, Post-Quantum Cryptography, Quantum Key Distribution, Cryptographic Algorithms Quantum Computing.

JEL Classification: O33, D80, G23.

INTRODUCTION

The rapid pace of technological advancement has made quantum cryptography one of the most crucial domains in the world's race to protect digital infrastructure. The increasing competition in computing technology and the possible widespread adoption of quantum computers will put to test most traditional cryptographic techniques that provide secure communication channels, protect

financial information, or safeguard data for governments. The consequences are dire. The existence of large-scale quantum computers would be catastrophic for the modern public key systems RSA, DSA, and ECC, which are used widely all over the world and could be broken in a matter of hours, exposing sensitive information that was previously considered secure for decades.

This concern is indeed valid, as both symmetric and asymmetric encryption systems have come under attack by quantum algorithms. Shor's algorithm, as an example, is able to factor large integers and calculate discrete logarithms at an exponential rate compared to classical algorithms. This essentially weakens the security of public key protocols that are used by almost everyone, making them vulnerable (Shor, P. W., 1994). On the other hand, symmetric encryption systems are not safe either. With his less destructive Grover's algorithm, symmetric encryption algorithms like AES are vulnerable too (Bennett *et al*., 1997). Because of both these algorithms, there is an added need for resilience in systems that rely on symmetric cryptography and an overhaul of the entire system's threat model in a post-quantum environment.

To address these newly developing challenges, researchers and organizations have created quantum cryptography and post-quantum cryptography as two complementary solutions. Quantum cryptography, and especially Quantum Key Distribution (QKD), uses the principles of quantum mechanics to provide security guarantees that are, in theory, impossible to break. It enables two parties to securely share keys with assurance of detection of any attempting eavesdropping due to quantum phenomena like superposition and the no-cloning theorem (Bennett, C.H. and Wiesner, S.J., 1992). Nevertheless, while QKD provides unmatched security, it is impractical for real world use because of physical range limitations, expensive equipment, and complex integration with traditional networks.

On the other hand, post-quantum cryptography (PQC) is a subclass of cryptographic algorithms meant to be secure against attacks from classical computers and quantum computers. They are based on certain mathematical problems believed to be very difficult to solve, even with the aid of quantum computers, such as those based on lattices, codes, and multivariate polynomials (ENISA, 2020). Unlike QKD, PQC can be implemented on traditional networks without the need for specialized quantum hardware, making it more readily scalable in the near term. Recognizing its strategic relevance, NIST commenced a pre-emptive globalization standardization initiative in 2016, which resulted in the selection of some promising post-quantum algorithms in 2022 (NIST, 2022a).

This paper examines the scope of quantum cryptography and countermeasures in post-quantum cryptography. It describes the shortcomings of traditional cryptography within information-theoretic frameworks, discusses quantum-initiated attacks, analyzes attempts to defend against them, and describes the actual work aimed at protecting information systems. It focuses on the normalization work, the policy implications considering the adoption barriers from the industrial side, and the impact on the cyberspace landscape, digital infrastructure, as well as policy making. The paper aspires to enhance the comprehension of the use of those measures expected to be taken on in the upcoming years.

MAIN CONTENT

1. Classical Cryptography vs. Quantum Computing

The bedrock of traditional cryptography, which has sustained digital security for over forty years now, rests on certain mathematical problems that are tough to solve using any conventional computing approaches. Solving large integer factorization, computing discrete logarithms, or even

elliptic curve discrete logarithm problems are some of these hard problems. These hardships provide support for most public key cryptosystems employed today due to being hardware infeasible.

Quantum computing poses the most threat to asymmetric cryptography. Popularly known algorithms such as RSA, Diffie-Hellman and ECC face harsh issues due to underlying such weak frameworks. These asymmetric methods rely on problems solvable with quantum mechanics such as Shor's algorithm. For example, the security underpinning RSA relies on the difficulty of factorization of two large prime numbers. While classically it takes sub-exponential time for a computer to accomplish this, quantum computers using Shor's algorithm will be able to do so in polynomial time (Shor, P. W., 1994). This indicates that with adequate advancements in quantum computing, mainly requiring thousands of logical qubits with error correction, RSA and ECC would instantaneously lose relevance alongside.

There are risks to digital signatures, which are critical to authentication and non-repudiation in modern communications. Weaker points of ECC pose the same threat to ECDSA, which is prevalent in several blockchain use cases and secure messaging applications. The global public key infrastructure that supports HTTPS, email encryption, and VPNs would face existential rupture in a post-quantum world without the adoption of new cryptographic primitives.

In contrast, symmetric cryptography is relatively more resilient. AES and other algorithms undergo no change in-status in the post-quantum setting, but rather their effective power is crippled. Proposed in 1996, Grover's algorithm allows a quantum computer to search an unordered list of N items in $O(\sqrt{N})$ time, which in turn, shrinks brute-force attack (Bennett *et al*., 1997). To illustrate, a quantum adversary would only receive a mere 64-bit protection from a 128-bit AES key. To counter this, NIST suggests adding extra brute-force replication layers by rising to AES-256. The same concept applies to hash-based functions where they shall be tested to ensure compliance to post-quantum standards for resistance against collisions and pre-images.

Regardless, the practical impact of Grover's Algorithm is much less pronounced than that of Shor's. The $\sqrt{N}$ exponential speedup provided by Grover's algorithm does not significantly change the security expectations for symmetric cryptosystems. Moreover, the quantum circuit depth and error correction layers suggest that the symmetric frameworks needed to effectively implement quantum algorithms are far too advanced for the available quantum resources in the near term.

The concept of "harvest now, decrypt later" is particularly perilous in the context of quantum computing threats. Bad actors could intercept encrypted communications protected by RSA or ECC, then await the emergence of sufficiently powerful quantum computers to decrypt the stored information. This scenario poses acute risk to sensitive governmental, military, and financial information that requires long-term, stringent confidentiality measures.

Thus, while symmetric cryptography remains a viable option in the quantum era (with strengthened parameters), the imminent collapse of asymmetric systems highlights the need for proactive migration strategies. There is an immediate need for cryptographers and cybersecurity experts to pivot from the out-dated public-key infrastructure to a post-quantum public-key framework that offers perpetual confidentiality and credibility.

2. Quantum and Post-Quantum Cryptography

In light of the functioning capabilities of quantum computers, there have been numerous paths explored within the field of cryptography. Each of these paths vary in their complexity, reasoning, and structure. One that stands out is quantum cryptography. It employs the foundations of quantum

physics to create secure channels of communication, enabling optimal protection against eavesdroppers. This quantum-mechanics-based solution operates seamlessly alongside post-quantum cryptography, which relies on classical hardware and complex mathematical problems believed to be resistant to quantum attacks. Both approaches tackle the quantum threat, however, they do so from different angles, accompanied by different benefits and limitations.

Quantum cryptography, particularly QKD, is regarded as one of the most secure methods of communication. Using quantum particles like photons, QKD allows two parties to create a shared secret key. Its security is founded on the no-cloning theorem and Heisenberg's uncertainty principle, which guarantees that any eavesdropping on the system will disturb the particles' quantum state and hence be detectable (Bennett, C.H. and Wiesner, S.J., 1992). Protocols such as BB84 and E91 have been tested and put into pilot systems across the globe, including quantum-secured inter-bank and inter-agency communication for a government (NIST, 2018).

A cornerstone of QKD is the information-theoretic security of the system. Unlike other methods, information-theoretic security is not based on computational assumptions. Furthermore, it is immune to both classical and quantum attacks, as long as the implementation is perfect with no side-channel attacks. Despite this, practical issues with QKD remain:

- the distance of transmission is limited by photon loss in fibre-optic cables;
- for longer distances, trusted nodes or quantum repeaters are needed which reintroduce points of susceptibility;
- the expenditure required for quantum devices, such as single-photon detectors and quantum random number generators, is exorbitant;
- there are difficulties in integrating traditional systems with key management infrastructures.

Regardless of the setbacks, QKD networks are expanding. For instance, China's QUESS satellite has conducted space-based quantum key exchange, advancing contemporary quantum global communication (Liao, S. K. et al., 2017).

On the contrary, *post-quantum cryptography* aims to defeat both quantum and classical adversaries by designing new cryptographic algorithms. Because these algorithms can be executed on classical computers, they are easier to assimilate into existing infrastructure. Unlike QKD, PQC does not rely on the physical realization of quantum phenomena but rather depends on robust mathematical challenges which, to date, there is no efficient quantum solution known.

Several families of cryptographic primitives have been identified as strong candidates for PQC:

- *Lattice-based cryptography*: These algorithms rely on the hardness of problems like the Shortest Vector Problem and Learning With Errors (Gentry, C., and Peikert, C., 2010). Not only do lattice-based schemes support encryption and signatures, they also include advanced functionalities such as homomorphic encryption. NIST has selected CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Dilithium (for digital signatures) for their standardization (Lyubashevsky *et al*., 2010) (NIST, 2022a).
- *Code-based cryptography*: Originating from the McEliece cryptosystem, code-based schemes are characterized by high security, although they tend to have large key sizes (Weger, V. et al., 2024). They are most beneficial in scenarios where the speed and size of a signature are less important than strength.
- *Multivariate polynomial cryptography*: This scheme is centred on multivariate quadratic equations over finite fields and is mainly used for digital signatures. Even though some

multivariate systems have been broken, others continue to undergo scrutiny as strong candidates.

- *Hash-based cryptography*: This type of scheme works with the security provided by cryptographic hash functions. Hash-based systems are ideal for use in digital signatures within resource-constrained environments (Vidaković, M., and Miličević, K., 2023). One such example is the SPHINCS+ signature scheme, which is built entirely on hash functions and offers very conservative security guarantees.

Remaining adaptable and scalable is the most notable advantage of PQC. Reconfiguration becomes easier because existing infrastructure can be leveraged for software and hardware implementation of algorithms. Since 2016, NIST has been spearheading a standalone PQC standardization project, from which finalists as well as alternate candidates are undergoing validation for performance, side-channel resilience, and overall practicality of deployment (NIST, 2022a).

Despite these overcoming these milestones, PQC still poses some of the following challenges:

- public key and ciphertext size issued by some schemes can create bandwidth strain and performance hindrance;
- hardware and software compatibility need to be audited and updated;
- migration for legacy systems becomes complicated for embedded systems;
- a number of these schemes are considered safe today, though there always some risk of a currently unknown quantum algorithm emerging which renders them useless.

Quantum and post-quantum techniques combined create a robust and sophisticated defensive approach. While QKD offers unrivalled security in theory, PQC serves a more practical use and provides ease of mass scaling prematurely in anticipation for proposed quantum threats on the horizon.

3. Standardization and Implementation

Replacing obsolete algorithms with newer ones is not sufficient for transitioning to quantum-resistant cryptography. Instead, it requires a more comprehensive strategy that includes resolving technological, organizational, and policy issues within multiple spheres. Though the shift is vital for avoiding a cryptographic collapse in the face of advancing quantum computers, it simultaneously guarantees a difficult balance of securing systems, ensuring compatibility, and minimizing disruptions.

Organizations must begin by identifying systems that rely on quantum-vulnerable algorithms. This includes algorithms utilized in TLS/SSL, VPNs, Secure Email, Digital Signatures, and Certificate Authorities. A risk assessment should be able to correlate data boundaries such as confidentiality lifetime. For instance, medical documents have strict privacy requirements for extended periods. These are ideal for the “store now, decrypt later” attack strategy.

Everyone, particularly government operators and critical infrastructure, must inventory their cryptographic escrows and determine where immediate action is necessary most. CISA's PQC roadmap final draft from 2022 suggests federal bodies adopt post-quantum cryptography and incorporates crypto-agility, hybrid cryptographic schemes, and pilot testing aimed at PQC (CISA Insights, 2022).

The importance of *crypto-agility* – the ability to change cryptographic schemes without a full system overhaul – is pivotal in transitional phases. Systems must be modular, flexible, and balanced so that updates do not heavily impact performance benchmarks or security thresholds.

A more practical approach to this dilemma is accepting a combination of classical and post-quantum algorithms – dubbed the hybrid cryptographic approach. Imagine a TLS handshake that uses RSA together with a lattice-based key agreement. This approach provides a secure bridge to the future while current security measures are sustained (Peikert, C., 2016). Easing the departure from outdated algorithms stimulates gradual adoption as standards progress prevents stagnation.

While the need for some form of migration is evident, there are a number of unresolved operational and technical issues:

- *Performance*: some PQC algorithms come with increased key size and ciphertext size. A case in point, McEliece has public key sizes on the order of several hundred kilobytes which poses an issue for bandwidth, memory constrained systems.
- *Hardware limits*: embedded systems like IoT devices frequently lack the necessary resources to run high-demand PQC algorithms, rendering such retrofits nearly impossible.
- *Legacy systems*: older systems are likely to be hard-wired using classic algorithms and therefore need more flexibility than they can afford.
- *Standardization lag*: while NIST has chosen a handful of algorithms, formal final standards and interoperability guidelines are still in progress. This poses risks and reluctance for large-scale deployment.

In addition, the real-world testing of post-quantum algorithms is still ongoing. Organizations need to develop test environments and engage in pilot programs before committing to full implementation.

Cryptographic migration is a global issue, and successful transition will require international coordination. For all countries with differing levels of infrastructure maturity, regulatory framework, and threat models, convergence on applicable standards and practices is essential.

Institutions like International Telecommunication Union and European Union Agency for Cybersecurity (ENISA) have embarked on developing studies and frameworks to aid in the adoption of quantum-resistant technologies. Other organizations such as NATO and the European Commission have also incorporated quantum-safe resiliency in their cybersecurity strategies highlighting the need for collective resilience (ENISA, 2020).

At the national level, governments are:

- financing research and development in post-quantum cryptography:
- developing guidelines and timelines for the migration process;
- building quantum communication testbeds;
- building regulatory checklists and compliance mandates.

Ultimately, transitioning to quantum-resistant systems will require collaboration between governments, academia, and industry, as well as a proactive investment in education, tooling, and awareness.

4. Case Studies and Practical Applications

To better understand how quantum and post-quantum cryptography are being applied in real-world contexts, this section reviews several case studies across industries. These examples illustrate how organizations are preparing for quantum threats and deploying secure technologies in diverse environments - from national security to commercial systems.

Financial Sector: Secure Banking and Payments. Due to the financial industry relying on data confidentiality, reputation, and operational integrity, it remains one of the sectors most susceptible to

quantum threats. Banking institutions heavily invest in cryptographic technologies for online banking, Secure SWIFT messaging, digital signature frameworks for transaction validation, and maintaining blockchain infrastructures.

A proactive example is ABN AMRO Bank in the Netherlands who, together with academic partners, investigated quantum key distribution (QKD) for secure interbank communications. In this project, a QKD link was used to secure high-valued communications between data centres using quantum channels augmented with classical encryption. The results not only proved the possibility of extending QKD into financial networks, but demonstrated significant problems in synchronization, mutual authentication, and scalability (ABN AMRO, 2019).

Other financial institutions have already joined PQC pilot projects, especially in relation to blockchain developments. PQC-based signature schemes are being implemented in testbeds of blockchain frameworks aimed at quantum resistance. This is vital since blockchain technologies supporting cryptocurrencies, including Bitcoin, utilize ECDSA for transaction signing which is known to be quantum vulnerable.

Government and Defence: National Quantum Communication Networks. Governments are investing in national infrastructures for quantum communication to safeguard classified information. China's Beijing-Shanghai quantum backbone, along with the Micius satellite (part of the QUESS program) are the most advanced QKD implementations to date. These systems have enabled secure video calls and data transmission through the use of entangled photons over thousands of kilometres (Liao, S. K. et al., 2017).

Similarly, the European Quantum Communication Infrastructure (EuroQCI) project aims to establish a QKD-based secure communication network between EU member states, expanding through fibre and satellite connections. This initiative is funded by the European Commission and the European Space Agency as part of the broader Digital Europe Programme. EuroQCI not only focuses on the technical deployment, but also on standardization and coordinated policy development among the member states (European Commission, 2020).

In the United States, the Department of Energy (DOE) partnered with several national laboratories and universities to develop the Quantum Internet Blueprint, which proposes a secure quantum communication layer to be integrated with the classical Internet (US DOE, 2020).

Industrial Applications: Cloud and IoT Security. One of the common cloud service providers, Amazon Web Services, Google Cloud, and Microsoft Azure are experimenting with post-quantum algorithms within their secure communication protocols. Post-quantum TLS key exchanges were tested in real world applications via Kyber (a lattice-based algorithm) integrated into Chrome Canary by Google in 2022. They aimed to prepare ecosystems in browsers to be able to switch seamlessly once PQC standards are issued. Their focus was ascertaining Experiential Value Optimization (Google Security Blog, 2022.).

IoT devices with their omnipresent nature and limited computational resources puts forth another challenging concern. Researchers are looking into PQC implementations that are more lightweight, specifically hash-based and lattice schemes that minimize operational and memory overhead (Cohn-Gordon, K., and Brierley, H, 2019). Embedded systems are being specially focused upon by the Internet Engineering Task Force (IETF) and NIST's Lightweight Cryptography Project as the develop pertinent guidelines and libraries.

An emerging trend is the development of hybrid encryption stacks for cloud and IoT systems that combine existing RSA or ECC protocols with post-quantum counterparts. With regard to future-

safe architectures, this layered methodology offers quantum-elusive protection while still sustaining backward adaptability.

Academic and Research Institutions. Scholarly pursuits focus on advancing the frontiers of quantum and post-quantum cryptography. University and national laboratory collaborative projects have developed experimental quantum networks in Vienna, Tokyo, and Geneva where QKD and quantum repeaters are tested in live environments. These testbeds yield valuable data concerning photon loss, synchronization errors, and system resilience.

Moreover, leading universities are at the forefront of cryptanalysis, where newly developed post-quantum schemes are benchmarked against classical and quantum contenders. The MIT, ETH Zurich, KU Leuven, and University of Waterloo actively participate in algorithm design and review for the NIST PQC competition.

These efforts in practice illustrate the progress, albeit inconsistent in speed and scale, towards a globally integrated quantum-safe cryptography infrastructure.

5. Quantum cryptography: Future directions

The shift from theoretical models to functional quantum computers marks a new chapter for the field of cryptography, presenting it with one of the greatest challenges and unparalleled opportunities. Addressing challenges of post-quantum computing not only entails implementing novel algorithms and systems, but demands a fundamental restructuring of security frameworks, trust models, and coordination on technology around the world.

Thus, among the most important research and development directions, the following can be mentioned:

1. *Total standardization and implementation of post-quantum cryptographic algorithms*. Once NIST selects the finalist algorithms CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, among others, NIST released, on August 13, 2024, final versions of the first three Post Quantum Crypto Standards: FIPS 203, FIPS 204, and FIPS 205 (NIST, 202ab), (NIST, 2024). These standards will facilitate cross adoption throughout government, military, industry, and civilian entities. Simultaneously, IETF, ISO/IEC and other standardization bodies are also modifying and developing certain protocols such as TLS, VPNs, and SSH to accommodate PQC.

2. *The design of quantum-resistant systems and their components*. In addition to cryptographic primitives, system design must also account for larger key sizes, new certificate formats, and hybrid methods of authentication. This includes software such as OpenSSL and BoringSSL, operating systems, and secure hardware like Trusted Platform Modules and HSMs.

3. *The issues of identity and authentication from the quantum viewpoint*. Proven challenges and relevant research are being done as regards to authentication, especially with zero-knowledge proofs, biometrics, and quantum-resistant identity-based encryption. Blockchain identity solutions also face revision, as existing systems rely heavily on ECDSA and other vulnerable schemes.

4. *Development of quantum cryptographic networks and their hardware*. Quantum hardware innovations such as quantum repeaters, photonic chips, and room temperature single-photon detectors will enhance the accessibility and scalability of quantum communications. Quantum router, entanglement distribution, and quantum internet architectures are imminent areas of research that will redefine secure communication networks of the future.

5. *Global cooperation and policy alignment*. Due to the cross-border nature of digital communications, the open world society needs to establish common cryptographic frameworks for

international interoperability, trade controls, and collaborative research and development policies. Effective cyber diplomacy and information-sharing amongst the quantum leadership consortium (U.S., EU, China, Japan) will be essential to prevent fragmented or insecure transitions.

6. *Education and development of the workforce*. With the advancement of cryptographic systems, designing, implementing, and auditing such systems will require increasingly sophisticated skills. While universities are starting to create programs in quantum cybersecurity, organizations like ENISA and CISA have launched targeted campaigns focused on raising awareness and developing relevant competencies (ENISA, 2021). Bridging the talent gap in quantum-safe security is as crucial as the technologies themselves.

CONCLUSIONS

Quantum computing has the capacity to advance science, medicine and artificial intelligence; however, it poses an immediate, direct existential risk to traditional cryptographic systems. The sustained progress being made in quantum hardware brings with it the need to accelerate the adaptation of existing frameworks.

Symmetric cryptography, which is only moderately impacted by Grover's algorithm, can be defended against with greater key lengths in conjunction with proper cryptographic design. As for asymmetric cryptography, it is under immediate threat and must adapt a structured transition to quantum-safe substitutes without delay.

In response to the consequences of quantum technologies, two options are emerging: the theoretical securitization guarantees of quantum cryptography, such as QKD, and the more practical, scalable defence provided by post-quantum algorithms. It seems likely that both options will be present in future systems, each fulfilling different functions depending upon the system's sensitivity, size, and implementation expense.

The shift to a quantum-resilient cryptographic backbone will move through stages of development and refinement, research and testing, standardization, and the education of specialists in the field. This transition will take time and cannot be done overnight. It is equally important to realize that the consequences of inaction are profound. The time to act is now. By adopting post-quantum and quantum-cryptography technologies, we would be able to bolster global digital ecosystems in order to ensure privacy, integrity, and authenticity as fundamental guarantees even in the age of quantum technology.

REFERENCES

1. ABN AMRO, 2019. *Uses Quantum Key Distribution for Secure Bank Communication*. Available at: https://www.abnamro.com [Accessed 22.03.2025].
2. Bennett, C. H., Bernstein, E., Brassard, G. and Vazirani, U., 1997. The strengths and weaknesses of quantum computation. *SIAM Journal on Computing*. 26 (5), pp. 1510–1523.
3. Bennett, C.H. and Wiesner, S.J., 1992. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States. *Physical Review Letters*, 69, pp. 2881-2884.
4. CISA Insights, 2022. *Preparing Critical Infrastructure for Post-Quantum Cryptography*. Available at: https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf [Accessed 11.04.2025].
5. Cohn-Gordon, K., and Brierley, H, 2019. Lightweight Cryptography for the Internet of Things. *Proceedings of the IEEE European Symposium on Security and Privacy*, pp. 321-332.

6. ENISA, 2020. *Quantum-Safe Cryptography and Post-Quantum Cryptographic Algorithms*. Available at: https://www.enisa.europa.eu/publications/quantum-safe-cryptography [Accessed 09.04.2025].
7. ENISA, 2021. *Quantum Cryptography and Security Challenges in Europe*. Available at: https://www.enisa.europa.eu/publications/quantum-cryptography-in-europe [Accessed 12.11.2024].
8. European Commission, 2020. *EuroQCI: European Quantum Communication Infrastructure*. Available at https://ec.europa.eu/digital-strategy/our-policies/european-quantum-communication-infrastructure_en, [Accessed 07.02.2025].
9. Google Security Blog, 2022. *Chrome's Implementation of Post-Quantum Cryptography*. Available at https://security.googleblog.com/2022/06/chromes-post-quantum-cryptography-pilot.html, [Accessed 22.04.2025].
10. Liao, S. K., Cai, W. Q. , Liu, W. Y. *et al*., 2017. Satellite-to-ground quantum key distribution, *Nature*, 549(7670), pp. 43–47.
11. Lyubashevsky, V., Peikert, C., and Regev, O., 2010. On the hardness of ideal lattice problems. *Journal of the ACM (JACM)*, 62(6), pp. 1-50.
12. NIST, 2018. NISTIR 8267: *Quantum Key Distribution and its Use in Secure Communications*. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8267.pdf [Accessed 22.10.2024].
13. NIST, 2022a. *Post-Quantum Cryptography Project*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography [Accessed 03.11.2024].
14. NIST, 2022b. *Post-Quantum Cryptography Standardization: Finalists*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions [Accessed 03.11.2024].
15. NIST, 2024. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards [Accessed 03.11.2024].
16. Peikert, C., 2016. Lattice cryptography for the masses. *Communications of the ACM*, 59(5), pp. 45-52.
17. Shor, P. W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134.
18. US DOE, 2020. *The Quantum Internet Blueprint: Building a Secure Quantum Network*. Available at: https://www.energy.gov/science/quantum-internet-blueprint [Accessed 13.04.2025].
19. Vidaković, M., and Miličević, K., 2023. Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments. *Algorithms*, 16(11), 518.
20. Weger, V., Gassner, N. and Rosenthal, J., 2024. *A Survey on Code-based Cryptography*. Available at https://arxiv.org/pdf/2201.07119, [Accessed 22.04.2025].
21. Gentry, C., and Peikert, C., 2010. Approximating the Shortest Vector Problem in Lattices. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pp. 237-246.