A STUDY OF THE IMPACT OF THE EMERGENCE OF QUANTUM COMPUTERS ON SPECIALIZATIONS IN THE FIELD OF CYBERSECURITY

Solodovnyk Ganna
PhD in Technical Sciences, Associate Professor,
Associate Professor of the Department of Cybersecurity
and Information Technologies
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine

Relevance. The development of quantum computers based on the principles of quantum parallelism and quantum entanglement opens new horizons for the modelling and study of complex, multi-component systems, including those similar to biological structures. However, it simultaneously leads to a significant increase in the capabilities for compromising information protection systems, which necessitates the enhancement of information security through the implementation of new technologies within the framework of post-quantum cryptography. The adoption of such technologies requires specialists with appropriate qualifications and expertise; therefore, the emergence of quantum computers fundamentally changes the requirements for professionals in cybersecurity, cryptography, DevOps, financial services, telecommunications, and even risk management.

Literature Review. Today, various Internet standards, such as Transport Layer Security (TLS), S/MIME, and PGP/GPG, employ RSA- and ECC-based cryptography to secure data transmission between smart cards, computers, servers, and industrial control systems. Online banking on “https” websites and the encryption of instant messaging on mobile devices represent the most widespread examples of the application of such data-protection methods. However, if quantum computers become available to malicious actors-machines capable of performing certain computations significantly faster than modern automated systems, a real threat emerges to the security algorithms widely used today [1].

In 2024, the European Union Agency for Cybersecurity published a comprehensive report assessing the state of cybersecurity and analysing the readiness of critical-sector institutions to counter contemporary risks and identify vulnerabilities. The report presents findings on the effectiveness of the existing EU cybersecurity framework and the overall maturity of organisations in the field of information protection. This is the fifth iteration of the report, incorporating data from 1,350 organisations across 27 EU Member States, covering all highly critical sectors as well as the manufacturing sector [2].

The European Union Agency for Cybersecurity (ENISA) is an EU institution responsible for ensuring a high level of cybersecurity across Europe by improving the trustworthiness of software, products, services, and information-telecommunication

processes. The agency was established in 2004 and is governed by the EU Cybersecurity Act. According to ENISA, proactive incident detection presupposes the early identification of malicious activities through internal monitoring tools or external threat-intelligence sources.

Enhancing the effectiveness of network-security incident detection in EU Member States is possible through the wider dissemination of currently developed cybersecurity measures and information resources, the accumulation and distribution of best practices in information protection, and the development and promotion of potential directions for advancing cybersecurity tools. With ENISA's support, joint European cybersecurity exercises have been repeatedly conducted, and their regular implementation has become one of the agency's objectives. Another objective involves the rapid dissemination of information about the state of the EU's information infrastructure and the creation of pan-European certification schemes for trust networks and Internet-of-Things devices across sectors ranging from energy to transportation.

According to ENISA publications, quantum technologies are capable of breaking public-key cryptographic schemes widely used in modern protection systems, such as RSA and ECC, or weakening symmetric encryption algorithms. Therefore, national authorities in various countries are working on identifying appropriate solutions: in 2017, the U.S. National Institute of Standards and Technology (NIST) launched and continues to develop a process for the standardization of several quantum-resistant public-key cryptographic algorithms.

At present, public-key cryptographic algorithms are regulated by the FIPS standards, the Digital Signature Standard, as well as the special publications SP 800-56A Revision 2 with recommendations on discrete-logarithm-based schemes, SP 800-56B Revision 1 with recommendations on integer-factorization-based key establishment schemes. However, such algorithms remain vulnerable to attacks executed by large-scale quantum computers [3].

NIST initiated a process of searching for, evaluating, and standardizing public cryptographic algorithms that would be resistant to attacks by quantum computers and could replace or complement existing algorithms that become vulnerable in the post-quantum era. For this purpose, in 2016–2017 NIST invited researchers in the field of cryptography to submit candidate algorithms for further analysis and evaluation. The proposed algorithms underwent several rounds of assessment based on criteria such as security, efficiency, implementation suitability, and openness of the reference code. As a result, algorithms were selected that demonstrated the best balance between resistance to quantum attacks, performance characteristics, and compatibility with existing systems.

In 2024, NIST released the first official Federal Information Processing Standards (FIPS) for post-quantum cryptography, which define procedures for key exchange and encapsulation, the generation of digital signatures, and alternative or backup signature mechanisms. In 2025, an additional algorithm – Hamming Quasi-Cyclic (HQC), a post-quantum key-encapsulation mechanism (KEM) – was added to the standards. This algorithm was chosen by NIST as a backup option in case vulnerabilities are discovered in the primary ML-KEM scheme [3].

The algorithms approved by NIST represent an attempt to ensure long-term cryptographic resilience in anticipation of the emergence of powerful quantum computers in a five- to ten-year (or longer) timeframe. These standards provide a unified foundation for organisations, governments, and developers to design and deploy information-protection systems capable of withstanding quantum-enabled attacks. Implementing FIPS standards reduces the risk that data encrypted today may be decrypted in the future (a Harvest-Now-Decrypt-Later attack).

Although NIST's post-quantum cryptography standards do not define direct requirements for specialists, they indirectly establish new competencies necessary for professionals in cybersecurity, cryptography, DevSecOps, and system architecture to operate quantum-resilient systems. These considerations substantiate the relevance of studying the impact of emerging quantum computers and the associated development of new standards and technologies for protecting information resources on professional specialisations in the field of cybersecurity.

Main Part. It is important to distinguish between post-quantum cryptography (PQC) and quantum cryptography (QC). PQC encompasses cryptographic methods designed for use on classical computers and assumed to be secure against both classical and quantum cryptanalytic attacks. Quantum cryptography, by contrast, refers to cryptographic solutions that employ physical principles of quantum mechanics to provide security services. A typical example of such methods is quantum key distribution (QKD).

In December 2020, the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, published the EU Cybersecurity Strategy, which addresses information-security issues for critical services such as hospitals, energy grids, and railway systems. The strategy explicitly identifies quantum methods and encryption technologies as key enablers, including those enhanced by artificial-intelligence tools, for achieving resilience, technological sovereignty, leadership, and the promotion of a global and open cyberspace. Another objective defined for these technologies is the enhancement of operational capabilities for preventing, deterring, and responding promptly to cybersecurity threats.

Ideas aimed at increasing information-security resilience laid the foundation for the development of the Open Quantum Safe (OQS) project [4]. This project is open-source software. The primary goals of OQS are the support, development, and prototyping of quantum-resistant cryptographic tools. The project consists of two main components: a library for implementing quantum-resistant algorithms and a suite of applications and protocols designed for integrating prototype solutions [5].

Most modern cryptosystems are built upon the computational hardness of integer factorization and discrete logarithms when solved using classical algorithms; however, such problems are efficiently solvable through Shor's algorithm. The quantum Shor algorithm enables the factorization of an integer M in time $O((\log M)^3)$ using $O(\log M)$ qubits. Consequently, the availability of a quantum computer equipped with several thousand qubits would make it possible to break public-key cryptographic systems. One of the methods for compromising the protection of such systems is the factorization of the public key into prime components. Classical algorithms on

conventional computers allow the security of such systems to be broken in time $O(M^{1/4})$, whereas Shor's algorithm enables the same task to be performed in time comparable to that required for multiplying prime numbers [3]. The task facing NIST developers is the standardisation of new public-key cryptographic methods that introduce several additional non-classified public digital signatures. To address this challenge, NIST researchers collect and analyse comments, requirements, and constraints related to quantum-resistant security mechanisms in order to formulate evaluation criteria for selecting the most suitable alternatives among quantum-resistant methods.

In effect, post-quantum cryptography standards impose on specialists, first and foremost, the requirement to understand the principles of PQC, to recognize the differences between post-quantum and classical algorithms, and to be aware of their vulnerabilities to Shor's and Grover's algorithms. The competencies of modern specialists must include knowledge of lattice-based and hash-based cryptography. Effective performance of a cybersecurity professional in post-quantum conditions presupposes the ability to apply new cryptographic algorithms defined by leading standards – ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+), HQC – which requires familiarity with key structures and sizes, performance limitations, and the parameters of security levels (ML-KEM-512, ML-KEM-768, ML-KEM-1024).

The process of transitioning an organisation from a classical set of cryptographic algorithms, protocols, or key parameters to a post-quantum, more modern, or more secure configuration necessitates the presence of appropriate competencies. According to NIST recommendations, a specialist must be able to:

– conduct cryptographic inventory of systems, i.e., identify all components in which cryptographic algorithms, keys, certificates, libraries, and protocols (TLS, SSH, VPN) are used;

– design flexible cryptographic interfaces (crypto-agility) that require selecting new algorithms, parameters, compatible libraries, and modes of operation capable of combining classical and post-quantum technologies;

– update infrastructures in accordance with the planned transition to post-quantum technologies and perform performance and compatibility testing.

Figure 1 presents a logical diagram illustrating the emergence of a new role for a specialist in the field of cybersecurity.

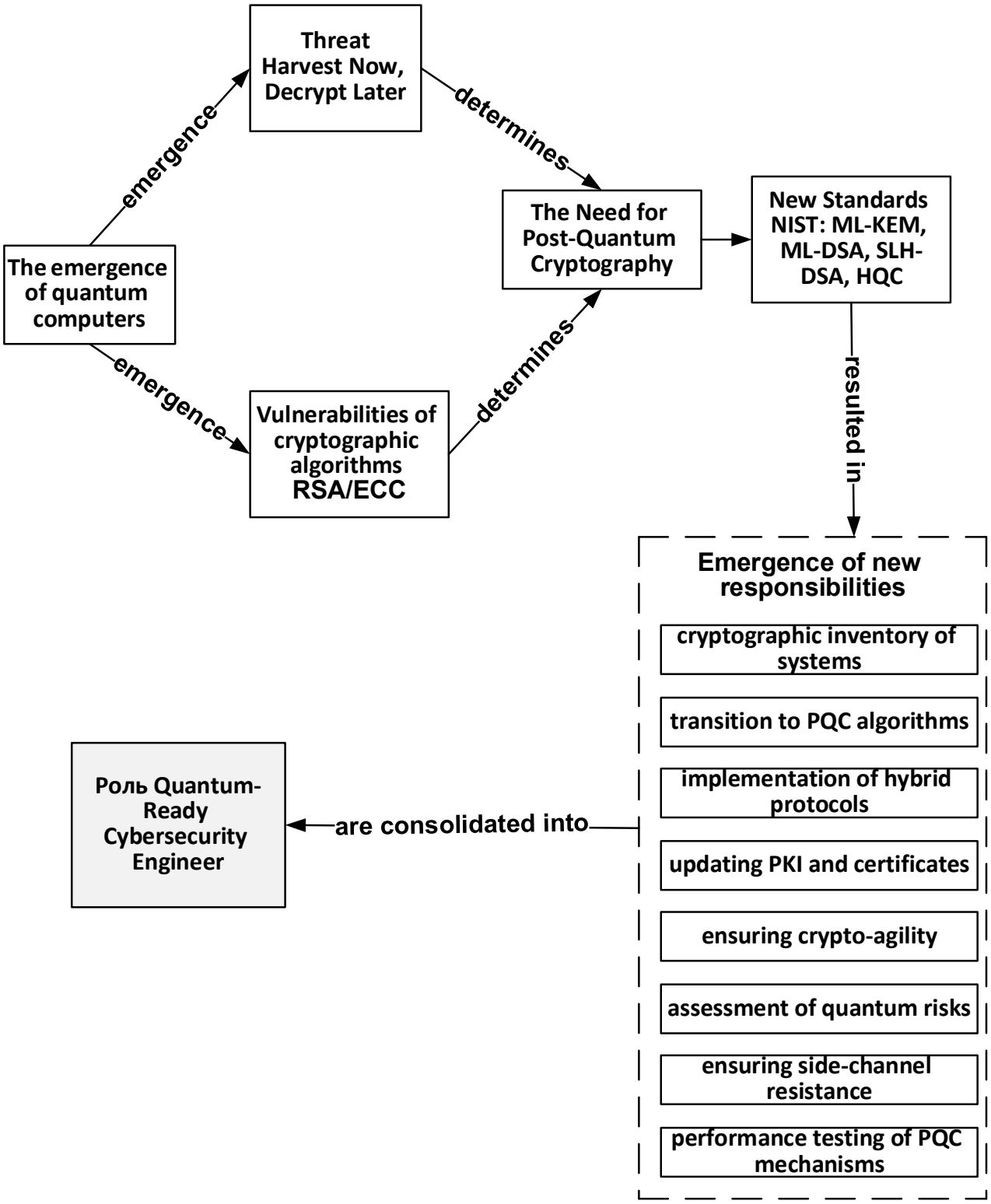

Figure 1 – Diagram of the Emergence of a New Role [author's own development]

These technological and standardisation changes in the field of information protection also affect the work of risk-management specialists. The assessment of risks associated with quantum attacks demands analysis of new threats of the "harvest now, decrypt later" type, evaluation of data age and sensitivity, as well as auditing the general risks of implementing post-quantum technologies in large infrastructures. Another task involves monitoring and verifying the security of post-quantum

technology deployment in specific systems and determining its impact on system performance. A contemporary specialist must be familiar with techniques that render cryptographic implementations resistant to attacks exploiting side-channel leakages, must be able to ensure correctness of implementations (constant-time operations), and recognise common errors in the deployment of post-quantum technologies.

NIST standards contain numerical characteristics of the algorithms; therefore, a specialist must be able to assess the load on the central processing unit and the network, select an appropriate security level in terms of protection strength and system-resource consumption, and test the performance of new protection mechanisms in an industrial (production) environment.

The development of quantum computing and the adoption of new standards within post-quantum cryptography are transforming the role of cybersecurity professionals. Classical cryptography based on RSA or ECC becomes vulnerable to attacks that quantum computers may be capable of executing in the future. A specialist seeking to be prepared for the challenges of the post-quantum era must understand these threats not only at the theoretical level, but also in terms of practical risk auditing and system-migration planning.

According to recommendations presented in professional reviews [6], a modern information-security specialist must be capable of maintaining an inventory of cryptographic assets within an existing system, developing a plan for the gradual transition to PQC algorithms, and rapidly and seamlessly replacing cryptographic algorithms, keys, protocols, and configurations without altering the fundamental architecture and operational logic of the information system.

In addition to purely technical skills, it is essential to be able to consider quantum risks in the context of business, operational, and organisational processes: to assess the impact on long-term confidentiality, data-retention periods, potential migration costs, and to justify investments in system-security upgrades for organisational leadership. This aspect is highlighted in modern cybersecurity development forecasts as a key skill of the future [6].

Another important area of responsibility for the new role of a cybersecurity engineer is the integration of post-quantum algorithms while ensuring compatibility, or the implementation of hybrid solutions during the transition phase, as well as performance testing with consideration of system load. It is necessary to verify the security of implementations, including with respect to side-channel attacks, and to ensure proper key management throughout the entire key-lifecycle process [7].

Conclusions. The study of the impact of quantum-technology development on work in the field of information security has shown that the role of the modern cybersecurity specialist is of strategic importance. Such a specialist is not only expected to respond to current threats, but also to design long-term security architectures for organisations, develop policies, plan migration processes, determine priorities, and coordinate the work of developers, architects, and business units-ensuring the overall readiness of the company for the quantum future.

The spread of quantum threats is shaping a new vector in the development of professions in the field of cybersecurity, requiring specialists to acquire competencies

that previously were not part of standard qualification requirements. Thus, the advancement of post-quantum cryptography necessitates a new type of specialist – quantum-ready engineers with a deep understanding of PQC algorithms. The transition to quantum-resistant encryption mechanisms is impossible without the preparation of personnel capable of conducting cryptographic inventory, dependency assessment, and system-migration planning. Existing IT infrastructures require adaptation to the new conditions, creating high demand for professionals who possess the principles of crypto-agility and hybrid cryptographic schemes. Financial and telecommunication services, as critical sectors, require specialists capable of evaluating the long-term risks of quantum attacks on confidential data. The development of new educational strategies becomes essential, as the preparation of qualified, PQC-oriented personnel is impossible without updating academic curricula.

References

1 Infineon // Post-quantum cryptography. URL:https://www.infineon.com/cms/en/product/promopages/post-quantum-cryptography/

2 European Union Agency for Cybersecurity // NIS360 2024: Assessment of cybersecurity posture and sectoral criticality under NIS2. URL: https://www.enisa.europa.eu/publications/nis-investments-2024

3 Computer Security Resource Center. NIST // Post-Quantum Cryptography Standardization. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

4 Open Quantum Safe // Official project website.URL: https://openquantumsafe.org/

5 IBM Developer // Developing with quantum-safe OpenSSL. URL: https://developer.ibm.com/tutorials/awb-quantum-safe-openssl/

6 Eraneos // Preparing for the Post-Quantum Era: Building Crypto Agility. URL: https://www.eraneos.com/articles/preparing-for-the-post-quantum-era-building-crypto-agility/

7INE // Cybersecurity 2030: Skills That Will Define Careers. URL: https://ine.com/blog/cybersecurity-2030-skills-that-will-define-careers