ЎЗБЕКИСТОН ҚОНУНЧИЛИГИ ТАҲЛИЛИ

UZBEKISTAN LAW REVIEW

ОБЗОР ЗАКОНОДАТЕЛЬСТВА УЗБЕКИСТАНА

ИЛМИЙ ТАҲЛИЛИЙ ЖУРНАЛ	SCIENTIFIC ANALYTICAL JOURNAL	НАУЧНО АНАЛИТИЧЕСКИЙ ЖУРНАЛ

2024

№4

ТАҲРИР ҲАЙЪАТИ

БОШ МУҲАРРИР:

Гулямов Саид Саидахрарович – юридик фанлари доктори, профессор.

ТАҲРИР ҲАЙЪАТИ АЪЗОЛАРИ:

Рустамбеков Исламбек Рустамбекович – ю.ф.д., профессор.
Хўжаев Шохжахон Акмалжон ўғли – юридик фанлар бўйича фалсафа доктори.
Оқюлов Омонбой – ю.ф.д., профессор.
Эргашев Восит Ёқубович – ю.ф.н., профессор.
Махкамов Отабек Мухтарович – ю.ф.д.
Суюнова Дилбар Жолдасбаевна – ю.ф.д., доц.
Мусаев Бекзод Турсунбоевич – ю.ф.д., доц.
Беков Ихтиёр – ю.ф.д., проф.
Бозоров Сардор Сохибжонович – ю.ф.д., проф. в.б.
Хазратқулов Одилбек Турсунович – юридик фанлари номзоди, доцент.
Самарходжаев Ботир Билялович – ю.ф.д., профессор.
Ходжаев Бахшилло Камалович – ю.ф.д., профессор.
Нарзиев Отабек Саъдиевич – ю.ф.д., проф. в.б.
Жолдасова Шахноза Батировна – юридик фанлар бўйича фалсафа доктори.

Маълумот олиш учун қуйидагиларга мурожаат этиш сўралади:
Гулямов Саид Саидахрарович,
Рустамбеков Исламбек Рустамбекович
ТДЮУ, Халқаро хусусий ҳуқуқ кафедраси,
Ўзбекистон Республикаси, Тошкент ш., 100047,
Сайилгоҳ кўчаси, 35. Тел: 233-66-36

"Ўзбекистон қонунчилиги таҳлили"нинг электрон нусхаси Интернетдаги www.library-tsul.uz ёки www.lawreview.uz сайтида жойлаштирилган.

Журнал 2013 йилдан Ўзбекистон Республикаси Вазирлар Маҳкамасининг Олий Аттестация комиссияси журналлари рўйхатига киритилган.

Ушбу журналда баён этилган натижалар, хулосалар, талқинлар уларнинг муаллифларига тегишли бўлиб, Ўзбекистон Республикаси ёки Тошкент давлат юридик университети сиёсати ёки фикрини акс эттирмайди.

2024 йилда нашр этилди.

Муаллифлик ҳуқуқлари Тошкент давлат юридик университетига тегишли. Барча ҳуқуқлар ҳимояланган. Журнал материалларидан фойдаланиш, тарқатиш ва кўпайтириш Тошкент давлат юридик университети рухсати билан амалга оширилади. Ушбу масалалар бўйича Тошкент давлат юридик университетига мурожаат этилади. Ўзбекистон Республикаси, Тошкент ш., 100047, Сайилгоҳ кўчаси, 35.

ISSN 2181-8118

Масъул котиб: **И. Рустамбеков**
Нашриёт муҳаррири: **Н. Ниязова**
Техник муҳаррир: **Д. Козимов**
Лицензия № 02-0074
Босишга рухсат этилди – 25.12.2024
Нашриёт ҳисоб табоғи – 5
«IMPRESS MEDIA» босмахонасида босилди
Адади – 100 нусха.

ИЛМИЙ-ТАҲЛИЛИЙ ЖУРНАЛ

4/2024

МУНДАРИЖА

Islombek Abdikhakimov
Lecturer of Cyber Law Department
Tashkent State University of Law

QUANTUM COMPUTING AND ITS IMPACT ON CYBERSECURITY: REDEFINING LEGAL FRAMEWORKS FOR A POST-QUANTUM ERA

Abstract. Quantum computing represents a transformative leap in computational capabilities, leveraging quantum mechanics to address complex problems far beyond the scope of classical computing. While this innovation promises breakthroughs in fields such as artificial intelligence and materials science, it simultaneously poses significant challenges to cybersecurity. Quantum algorithms, such as Shor's, threaten to render classical cryptographic methods obsolete, exposing critical vulnerabilities in global digital infrastructure. This paper explores the implications of quantum computing for current cryptographic systems, highlights advancements in post-quantum cryptography (PQC), and underscores the urgent need for updated legal frameworks to address emerging threats. Employing a qualitative methodology, the study integrates technological analysis with legal evaluations to propose actionable solutions for a secure transition to a post-quantum era. The findings emphasize the necessity of international collaboration, adaptive legal standards, and widespread adoption of PQC to mitigate the dual-use risks of quantum technologies and safeguard digital trust.

Keywords: Quantum computing, cybersecurity, cryptography, post-quantum cryptography, Shor's algorithm, legal frameworks, quantum threat, digital infrastructure, cybersecurity law, quantum-resistant encryption.

Аннотация. Квантовые вычисления представляют собой революционный прорыв в вычислительных возможностях, используя квантовую механику для решения сложных задач, выходящих далеко за пределы возможностей классических вычислений. Хотя эта инновация обещает прорывы в таких областях, как искусственный интеллект и материаловедение, она одновременно создает значительные проблемы для кибербезопасности. Квантовые алгоритмы, такие как алгоритм Шора, угрожают сделать классические криптографические методы устаревшими, обнажая критические уязвимости в глобальной цифровой инфраструктуре. В данной статье исследуются последствия квантовых вычислений для современных криптографических систем, освещаются достижения в постквантовой криптографии (PQC) и подчеркивается острая необходимость обновления правовых основ для противодействия возникающим угрозам. Используя качественную методологию, исследование объединяет технологический анализ с правовой оценкой для предложения практических решений по безопасному переходу к постквантовой эпохе. Результаты подчеркивают необходимость международного сотрудничества, адаптивных правовых стандартов и широкого внедрения PQC для снижения рисков двойного использования квантовых технологий и защиты цифрового доверия.

Ключевые слова: квантовые вычисления, кибербезопасность, криптография, постквантовая криптография, алгоритм Шора, правовые основы, квантовая угроза, цифровая инфраструктура, законодательство в области кибербезопасности, квантово-устойчивое шифрование.

Annotatsiya. Kvant hisoblash klassik hisoblash imkoniyatlaridan ancha yuqori bo'lgan murakkab masalalarni hal qilish uchun kvant mexanikasidan foydalangan holda hisoblash qobiliyatlarida transformatsion sakrashni ifodalaydi. Ushbu innovatsiya sun'iy intellekt va materiallar fanida yangi kashfiyotlarni va'da qilsa-da, bir vaqtning o'zida kiberhavfsizlik uchun jiddiy muammolarni keltirib chiqarmoqda. Shor algoritmi kabi kvant algoritmlari klassik kriptografik usullarni eskirgan qilib, global raqamli infratuzilmadagi muhim zaifliklarni ochib bermoqda. Ushbu maqola kvant hisoblashning zamonaviy kriptografik tizimlarga ta'sirini o'rganadi, post-kvant kriptografiyasidagi (PQC) yutuqlarni ta'kidlaydi va yuzaga kelayotgan tahdidlarga qarshi kurashish uchun huquqiy asoslarni yangilashning kechiktirib bo'lmaydigan zaruriyatini ko'rsatadi. Sifatli metodologiyadan foydalangan holda, tadqiqot post-kvant davriga xavfsiz o'tish uchun amaliy yechimlarni taklif qilish maqsadida texnologik tahlil va huquqiy baholashni birlashtiradi. Natijalar xalqaro hamkorlik, moslashuvchan huquqiy standartlar va kvant texnologiyalarining ikki tomonlama foydalanish xavflarini kamaytirish hamda raqamli ishonchni himoya qilish uchun PQCni keng joriy etish zarurligini ta'kidlaydi.

Kalit so'zlar: kvant hisoblash, kiberhavfsizlik, kriptografiya, post-kvant kriptografiyasi, Shor algoritmi, huquqiy asoslar, kvant tahdidi, raqamli infratuzilma, kiberhavfsizlik qonunchiligi, kvantga chidamli shifrlash..

Introduction.

Quantum computing represents a revolutionary leap in computational power, leveraging the principles of quantum mechanics to process information at unprecedented speeds. Unlike classical computers, which rely on bits as the basic unit of information. quantum computers utilize quantum bits, or qubits. Qubits can exist simultaneously in multiple states due to the phenomena of superposition and entanglement, enabling parallel computations that vastly exceed the capabilities of classical systems.[1] Recent advancements in quantum technology by organizations such as IBM, Google, and others suggest that quantum supremacy—the ability of a quantum computer to solve problems that classical computers cannot—is no longer a theoretical milestone but an impending reality. [2]

Cybersecurity, which encompasses practices and technologies designed to protect data, networks, and systems from unauthorized access and attacks, is a cornerstone of modern digital infrastructure. From protecting sensitive government information to ensuring the integrity of financial transactions and personal privacy, cybersecurity underpins trust in the digital age. Traditional cryptographic methods such as RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) are integral to this

trust. However, these methods rely on mathematical problems—like prime factorization and discrete logarithms—that are computationally infeasible for classical computers to solve efficiently. Quantum computers, armed with algorithms like Shor's, could potentially solve these problems in polynomial time, rendering current encryption methods obsolete.[3]

Problem Statement. The rapid development of quantum computing poses both unprecedented opportunities and existential threats to digital security. On one hand, quantum technology holds the promise of breakthroughs in areas like material science, artificial intelligence, and drug discovery. On the other hand, its ability to undermine existing encryption protocols represents a seismic shift in cybersecurity. The current cryptographic landscape, which secures everything from financial transactions to national defense systems, is fundamentally ill-prepared for the quantum threat.

This quantum disruption is exacerbated by the lag in legal and regulatory frameworks, which are not yet equipped to address post-quantum cybersecurity risks. Many nations and organizations remain in the exploratory stages of implementing post-quantum cryptography (PQC) standards, while others lack concrete strategies altogether. Without robust legal mechanisms to enforce the adoption of quantum-resistant technologies, global digital infrastructure may face vulnerabilities that transcend national borders, exposing sensitive data and critical systems to potentially catastrophic breaches.

Objectives. This article aims to achieve the following:

Analyze the implications of quantum computing on current cybersecurity practices, with a specific focus on cryptographic systems.

Explore the emerging field of post-quantum cryptography and its potential to mitigate quantum-induced vulnerabilities.

Propose updates to existing legal frameworks to address the challenges posed by quantum computing in the cybersecurity domain.

By addressing these objectives, the article seeks to provide a comprehensive roadmap for navigating the post-quantum era, balancing technological innovation with the need for robust security and legal safeguards.

Scope. The scope of this study is threefold:

Cryptographic Implications: The article will examine how quantum computing disrupts classical cryptographic systems, focusing on the vulnerabilities of RSA, ECC, and similar protocols. The analysis will also explore NIST's efforts to standardize post-quantum cryptographic algorithms.

Post-Quantum Standards: A review of the emerging field of post-quantum cryptography will highlight viable alternatives to classical encryption. The article will discuss the challenges of implementing these standards at scale, along with the technical, logistical, and policy hurdles that must be overcome.

Legal and Ethical Considerations: This section will evaluate the adequacy of existing cybersecurity laws in addressing post-quantum threats. It will also explore the ethical dimensions of regulating quantum computing, particularly in balancing the promotion of innovation with the need for security and accountability.

In addressing these aspects, this article aims to contribute to the discourse on quantum computing and cybersecurity by proposing actionable solutions for the evolving legal and technological landscape.

Methods. Research Design. This study employs a qualitative research design grounded in an extensive literature review and comparative analysis. The methodological approach focuses on synthesizing current academic, technical, and legal insights to address the implications of quantum computing on cybersecurity and the associated need for legal reforms.

Literature Review:The literature review encompasses a wide array of scholarly articles, technical reports, and institutional white papers that explore advancements in quantum computing, its implications for cryptography, and potential countermeasures. The review includes analyses of milestone studies, such as Shor’s algorithm and its cryptographic implications, as well as ongoing efforts by institutions like the National Institute of Standards and Technology (NIST) to develop quantum-resistant cryptographic algorithms. This ensures a robust understanding of the subject matter and its complexities.

Comparative Analysis: The research compares traditional cryptographic techniques with emerging post-quantum cryptographic approaches. This comparative analysis focuses on evaluating the relative strengths, weaknesses, and vulnerabilities of each method in the context of quantum computational capabilities. The study also examines the feasibility of transitioning to quantum-resistant algorithms in various sectors, from financial systems to national defense.

Data Sources. The data for this study are derived from credible and authoritative sources to ensure the reliability and validity of the findings:

PeerReviewed Journals: Scholarly articles from journals such as Quantum Information Science, Cryptography and Communications, and IEEE Transactions on Information Theory are analyzed to provide insights into both the technical aspects of quantum computing and the advancements in cryptographic research.

Institutional White Papers: Reports published by leading organizations, including NIST, the European Telecommunications Standards Institute (ETSI), and the World Economic Forum (WEF), serve as primary references for the development of quantum-safe standards and frameworks.

Cybersecurity Reports: Industry analyses, such as those from cybersecurity firms (e.g., McAfee, IBM Security), offer practical perspectives on the real-world challenges posed by quantum computing to traditional encryption.

Legal Statutes and Frameworks: Existing laws, policies, and international agreements related to cybersecurity and data protection are reviewed to identify regulatory gaps in the context of post-quantum threats. Sources include the General Data Protection Regulation (GDPR), U.S. cybersecurity legislation, and relevant international conventions.

Framework for Analysis: The study employs a dual-framework approach to analyze both the technological and legal dimensions of quantum computing’s impact:

Technological Assessment: This aspect evaluates the vulnerabilities of traditional encryption methods under quantum computing scenarios. The study examines algorithms such as RSA and ECC, focusing on their computational principles and susceptibility to quantum attacks. Furthermore, the assessment explores the readiness and performance of post-quantum cryptographic solutions, including lattice-based cryptography, hash-based signatures, and multivariate polynomial cryptography.

Legal Gap Analysis: A systematic evaluation of existing cybersecurity laws is conducted to determine their

adequacy in addressing post-quantum risks. This involves identifying gaps in current regulatory frameworks, such as the absence of mandates for quantum-resistant standards or lack of international cooperation on cryptographic policies. The analysis also considers ethical challenges, including the dual-use nature of quantum computing and its potential misuse.

By combining technological and legal analyses, this framework facilitates a comprehensive understanding of the challenges posed by quantum computing and provides actionable insights for developing robust solutions in the post-quantum era.

Methods. This study adopts a multi-faceted research design to comprehensively explore the intersection of quantum computing, cybersecurity, and legal frameworks:

Literature Review: A systematic review of academic articles, industry white papers, and governmental reports was conducted to map the current state of quantum computing and its implications for cybersecurity. Key areas of focus included the development of quantum algorithms, vulnerabilities in traditional cryptography, and advancements in post-quantum cryptography.

Comparative Analysis: A detailed comparison was carried out between traditional cryptographic methods (e.g., RSA, ECC) and emerging quantum-resistant cryptographic techniques. This analysis considered computational complexity, scalability, and potential for integration into existing systems.

Data Sources. Primary sources of data included:

Peer-Reviewed Journals: Scholarly articles from journals such as Quantum Information Processing, Journal of Cybersecurity, and Nature Communications provided foundational insights into quantum computing and cryptographic vulnerabilities.

Institutional White Papers: Reports from leading organizations, including the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI), offered up-to-date information on post-quantum cryptography standardization.[5]

Cybersecurity Reports: Annual threat assessments and technical briefs from cybersecurity firms such as McAfee and Kaspersky were analyzed to identify trends in cyber threats exacerbated by quantum advancements.

Legal Statutes: Existing laws and regulations, such as the General Data Protection Regulation (GDPR) and the U.S. Cybersecurity Information Sharing Act, were evaluated for their relevance to quantum-era cybersecurity challenges.

Framework for Analysis. To address the objectives of this study, two analytical frameworks were employed:

The impact of quantum computing on encryption standards was evaluated by examining the computational feasibility of quantum algorithms such as Shor's and Grover's. This analysis included projected timelines for quantum computing milestones and their correlation with cybersecurity risks.

The adequacy of existing legal frameworks in addressing post-quantum challenges was assessed by comparing current laws to the needs of a quantum-secure infrastructure. Particular attention was paid to gaps in international coordination and the absence of enforceable post-quantum standards.

Shor’s Algorithm and Its Implications:

Shor's algorithm demonstrates the potential for quantum computers to efficiently solve problems like integer factorization and discrete logarithms, which are foundational to RSA and ECC encryption. For instance, a sufficiently powerful quantum computer could, in theory, decrypt RSA-encrypted data by factoring large integers exponentially faster than classical algorithms. This capability renders current encryption methods vulnerable once practical quantum computers are available.

NIST’s Post-Quantum Cryptography Initiatives:

In response to the looming threat, NIST has spearheaded efforts to standardize post-quantum cryptographic algorithms. Algorithms under consideration include lattice-based, hash-based, and code-based cryptographic techniques, which leverage problems believed to be resistant to quantum attacks. Among the candidates, schemes such as Kyber (lattice-based) and SPHINCS+ (hash-based) have emerged as frontrunners, emphasizing computational efficiency and security.

Emerging Threat Landscape.

Quantum Computing as a Dual-Use Technology:

Quantum computing’s dual-use nature presents unique challenges. While it can advance fields like medicine and climate modeling, it simultaneously enables state and non-state actors to exploit encryption vulnerabilities. Nations investing in quantum technologies, such as China and the U.S., are at the forefront of both development and potential misuse.

Cybersecurity Vulnerabilities:

Harvest Now, Decrypt Later Attacks: Adversaries are increasingly adopting strategies where encrypted data is harvested now with the expectation that future quantum computers will decrypt it. This tactic poses a significant threat to long-term data confidentiality, particularly in industries like healthcare and defense.

Insecure Transition Periods: The transition to post-quantum cryptography is fraught with challenges, including the compatibility of quantum-resistant algorithms with existing systems, creating windows of vulnerability during implementation.

Legal Deficiencies. Limitations of Existing Cybersecurity Laws:

Most current cybersecurity laws focus on classical threats, offering little to no guidance on mitigating risks associated with quantum computing. For example, while GDPR emphasizes data protection, it does not mandate quantum-safe encryption practices, leaving a significant gap in long-term data security. [4]

Lack of International Consensus: A fragmented global approach to post-quantum cybersecurity creates inconsistencies and vulnerabilities. While initiatives like NIST’s PQC standardization are commendable, their adoption varies widely across regions. This lack of consensus delays the global implementation of quantum-resistant systems, increasing the collective risk.

Discussion. The advent of quantum computing introduces profound challenges for cybersecurity, necessitating immediate and coordinated action to safeguard global digital infrastructure.

Urgency of Transitioning to Quantum-Safe Cryptographic Methods:

The potential of quantum computers to undermine widely used cryptographic protocols like RSA and ECC underscores the critical need for quantum-resistant encryption. Organizations and governments must accelerate the transition to post-quantum cryptographic (PQC) standards, particularly in sectors where long-term confidentiality is essential, such as healthcare, finance, and national security. Proactive measures, including the integration of quantum-safe cryptographic systems into critical infra-

structure, must occur before quantum computers achieve widespread operational capabilities.[5]

Challenges in Deploying Post-Quantum Algorithms at Scale:

Technical Hurdles: Many PQC algorithms are computationally intensive, posing challenges for devices with limited processing power, such as Internet of Things (IoT) devices. Moreover, ensuring backward compatibility with existing systems further complicates deployment.

Resource Constraints: Transitioning global cryptographic infrastructure is a resource-intensive endeavor requiring significant financial investment, technical expertise, and organizational commitment. Small and medium-sized enterprises (SMEs), in particular, may struggle to adopt PQC standards without external support.

- Coordination Across Stakeholders: Achieving a smooth transition requires cooperation among governments, private organizations, and technology providers to develop, implement, and standardize quantum-resistant algorithms effectively. [6]

Ethical Considerations. Addressing Ethical Challenges in Dual-Use Quantum Technologies: Quantum computing is inherently a dual-use technology with both beneficial and malicious applications. The ethical implications of its misuse require immediate attention. [7]Policies should include mechanisms to regulate the development and deployment of quantum technologies while ensuring accountability. Additionally, there is a moral imperative to ensure that quantum computing advancements are not monopolized by a few powerful nations or corporations, to prevent exacerbating global inequalities. [8]

Balancing Innovation and Regulation: Over-regulation could stifle innovation, hindering the development of quantum computing's beneficial applications, such as advances in climate modeling or healthcare. Striking a balance between fostering innovation and ensuring security is crucial. Adaptive regulatory frameworks that evolve alongside technological advancements can help achieve this equilibrium. Regulatory sandboxes, for instance, can provide controlled environments for testing quantum technologies under regulatory supervision without impeding their growth.[9]

Conclusion. Summary of Findings. Quantum computing is poised to transform the technological landscape, offering unparalleled computational capabilities that could drive significant advancements across industries. However, its potential to undermine existing cryptographic systems represents a critical threat to global cybersecurity. Algorithms such as Shor's have demonstrated the feasibility of quantum attacks on widely-used encryption methods, exposing vulnerabilities in the digital infrastructure that underpins commerce, healthcare, defense, and governance.

The analysis has highlighted the inadequacy of existing cybersecurity frameworks in addressing post-quantum challenges. While the development of post-quantum cryptographic (PQC) algorithms is underway, the absence of widespread implementation, coupled with fragmented global regulatory efforts, exacerbates vulnerabilities. The findings emphasize the urgency of transitioning to quantum-safe cryptographic methods and updating legal frameworks to account for quantum computing's disruptive impact. A coordinated approach that integrates technological innovation with robust regulation is essential for securing a quantum-resilient future.

Recommendations. Adoption and Enforcement of Post-Quantum Standards:

Global stakeholders, including governments, private organizations, and international bodies, must prioritize the adoption of PQC algorithms. Regulatory mandates should enforce the implementation of quantum-safe encryption in critical sectors, supported by incentives to encourage early adoption. International standardization efforts must ensure interoperability and compatibility across borders to prevent fragmented responses to quantum threats.

Establishment of International Collaboration Frameworks:

The harmonization of post-quantum cybersecurity measures requires active participation from international organizations such as the United Nations (UN), International Organization for Standardization (ISO), and International Telecommunication Union (ITU). These entities should lead efforts to create universal standards, share knowledge, and provide technical assistance to nations and industries with limited resources.

Investment in Research and Development:

Further research into quantum computing and post-quantum cryptography is imperative. Governments and private enterprises should increase funding for research programs to refine PQC algorithms, optimize their scalability, and address integration challenges. This investment should also include interdisciplinary studies that explore the ethical and legal dimensions of quantum technology.

Creation of Adaptive Legal Frameworks:

Legal reforms must be forward-looking, incorporating quantum-resilient principles while remaining flexible enough to adapt to future advancements. Policymakers should introduce sandbox frameworks to allow controlled testing of quantum technologies while enforcing accountability and security measures.

Public Awareness and Workforce Development:

Raising awareness of quantum computing's implications and developing a skilled workforce are essential for a secure transition to the post-quantum era. Educational initiatives should target professionals in cybersecurity, law, and technology to equip them with the expertise needed to navigate this emerging landscape.

The convergence of quantum computing and cybersecurity presents a critical juncture for technological and legal innovation. By acting decisively, global stakeholders can mitigate risks, leverage quantum computing's potential for societal benefit, and ensure the resilience of digital systems in the post-quantum world.

References

1. Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

2. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., … & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

3. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

4. European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

5. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-

Quantum Cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

6. National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

7. National Security Agency (NSA). (2016). NSA's Cybersecurity Perspective on Post-Quantum Cryptography. Retrieved from https://www.nsa.gov

8. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

9. Vogelsang, K., Kainz, M., & Hofmann, M. (2021). Challenges of quantum-resistant cryptography in large-scale networks. Journal of Cybersecurity, 7(1), tyab007. https://doi.org/10.1093/cybsec/tyab007