sjst.scst.edu.ly

Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)

مجلة صرمان للعلوم والتقنية
Vol 7, No.2. Jun. – Dec. 2025
Pages: 343 ~ 354

Post-Quantum Cryptography and the Future of Data Security: Challenges, Migration Readiness, and Strategic Protection of Information Systems

Seham Ahmed Daraz[1], Ziaulhaq Dhau Obeid[2]
[1]Almustaqbal college, Misrata, Libya
[2]College of Technical Science, Bani Walid, Libya

hayat9374@gmail.com[1], Ziaulhaq.obeid@yahoo.com[2]

Abstract

This study examines post-quantum cryptography as a future-oriented approach to protecting data security against the expected risks of quantum computing. It explains that current public-key cryptographic systems, such as RSA and elliptic-curve cryptography, may become vulnerable when powerful quantum computers are developed.

The study highlights that organizations need to prepare early for migration to quantum-resistant cryptographic systems. This preparation requires more than technical updates; it involves cryptographic inventory, risk assessment, cybersecurity governance, vendor coordination, staff training, and strategic planning.

The main focus of the study is to analyze how organizational readiness affects the successful adoption of post-quantum cryptography. The proposed framework includes factors such as awareness of quantum threats, maturity of cryptographic inventory, governance readiness, vendor readiness, technical infrastructure flexibility, and cybersecurity expertise.

The study concludes that post-quantum cryptography is essential for protecting sensitive data in the future. Successful migration depends on early planning, institutional readiness, and the adoption of NIST-approved post-quantum standards.

Submitted: 22/10/2025 *Accepted: 26/12/2025*

الملخص

تدرس هذه الدراسة تشفير ما بعد الكم (Post-Quantum Cryptography) كنهج موجه نحو المستقبل لحماية أمن البيانات ضد المخاطر المتوقعة للحوسبة الكمومية. وتوضح الدراسة أن أنظمة التشفير الحالية ذات المفتاح العام، مثل (RSA) وتشفير المنحنى الإهليلجين(Elliptic-Curve Cryptography) ، قد تصبح عرضة للاختراق عند تطوير أجهزة كمبيوتر كمومية قوية.

وتسلط الدراسة الضوء على حاجة المؤسسات للاستعداد المبكر للانتقال إلى أنظمة التشفير المقاومة للكم. ويتطلب هذا الاستعداد ما هو أكثر من مجرد تحديثات تقنية؛ إذ يشمل جرد أدوات التشفير، وتقييم المخاطر، وحوكمة الأمن السيبراني، والتنسيق مع الموردين، وتدريب الموظفين، والتخطيط الاستراتيجي.

ينصب التركيز الرئيسي للدراسة على تحليل كيفية تأثير الجاهزية المؤسسية في الاعتماد الناجح لتشفير ما بعد الكم. ويتضمن الإطار المقترح عوامل مثل: الوعي بالتهديدات الكمومية، ونضج جرد أدوات التشفير، وجاهزية الحوكمة، وجاهزية الموردين، ومرونة البنية التحتية التقنية، والخبرة في مجال الأمن السيبراني.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 7, No.2. Jun. – Dec. 2025
Pages: 343 ~ 354

وتخلص الدراسة إلى أن تشفير ما بعد الكم يعد أمرًا أساسيًا لحماية البيانات الحساسة في المستقبل. ويعتمد الانتقال الناجح على التخطيط المبكر، والجاهزية المؤسسية، واعتماد معايير ما بعد الكم المعتمدة من المعهد الوطني للمعايير والتكنولوجيا.(NIST)

Background of the Study

Data security has become a strategic priority for modern organizations because digital services, cloud computing, electronic payments, government platforms, healthcare records, and corporate systems all depend heavily on cryptographic protection. Public-key cryptography is especially important because it supports secure communication, digital signatures, identity verification, software updates, and key exchange across the internet and enterprise systems.

However, the development of cryptanalytically relevant quantum computers creates a future risk to many existing public-key cryptographic systems. CISA, NSA, and NIST warn that a sufficiently capable quantum computer could break public-key systems currently used to protect information systems, including algorithms based on RSA, elliptic-curve Diffie-Hellman, and elliptic-curve digital signatures. They also warn that attackers may collect encrypted data now and decrypt it later when quantum capabilities become available, a risk often described as “harvest now, decrypt later.”

Post-quantum cryptography refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers. Unlike quantum key distribution, which requires special quantum communication infrastructure, post-quantum cryptography is based on mathematical algorithms that can be deployed in conventional digital systems. In August 2024, NIST released its first principal post-quantum cryptography standards: FIPS 203 for ML-KEM, FIPS 204 for ML-DSA, and FIPS 205 for SLH-DSA. These standards cover key establishment and digital signatures designed to resist future quantum attacks.

This study is important because the transition to post-quantum cryptography is not merely a technical update. It requires institutional planning, cryptographic inventory, risk assessment, vendor coordination, governance, budget allocation, system testing, policy revision, and long-term security strategy. NIST has stated that organizations should begin migrating to quantum-resistant cryptography, identify where vulnerable algorithms are used, and plan to replace or update them.

Statement of the Problem

Although large-scale quantum computers capable of breaking today’s widely used public-key cryptography are not yet generally available, organizations cannot wait until the threat becomes immediate. Many types of data, such as government records, financial information, medical records, intellectual property, legal documents, and national security information, require confidentiality for many years. If such data is captured today, it may become exposed in the future when quantum computing capabilities advance.

The problem is that many organizations still lack clear readiness for post-quantum cryptography migration. They may not know where quantum-vulnerable cryptography is embedded in their systems, applications, network protocols, cloud services, software libraries, hardware devices, or vendor products. CISA, NSA, and NIST emphasize that organizations often lack visibility into the

full scope of public-key cryptography used in operational environments, which makes migration difficult and increases future risk.

Therefore, the research problem can be formulated as follows:

Organizations face increasing future data security risks due to the potential ability of quantum computers to break current public-key cryptographic systems, while many institutions remain insufficiently prepared to migrate toward post-quantum cryptographic solutions.

Main Research Question

How can post-quantum cryptography contribute to the future protection of data security, and what factors influence organizational readiness to migrate from traditional cryptographic systems to quantum-resistant cryptography?

5. Sub-Questions of the Study

1. What is post-quantum cryptography, and how does it differ from traditional cryptographic approaches?
2. What types of data security risks are created by future quantum computing capabilities?
3. What are the main NIST-approved post-quantum cryptography standards and their security functions?
4. What is the role of cryptographic inventory in post-quantum migration readiness?
5. How do organizational awareness, governance, vendor readiness, and technical infrastructure affect post-quantum migration?
6. What are the main challenges organizations face when adopting post-quantum cryptography?
7. What strategic roadmap can organizations follow to prepare for a quantum-safe security environment?

Objectives of the Study

The study aims to:

1. Explain the concept, importance, and scope of post-quantum cryptography.
2. Analyze the future threat posed by quantum computing to current public-key cryptography.
3. Identify the main post-quantum cryptography standards issued by NIST.
4. Examine the role of post-quantum cryptography in protecting long-term sensitive data.
5. Assess the importance of cryptographic inventory, risk assessment, and vendor coordination in migration readiness.
6. Identify organizational and technical challenges that may delay post-quantum cryptography adoption.
7. Develop a practical research-based framework for improving organizational readiness for post-quantum data security.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 7, No.2. Jun. – Dec. 2025
Pages: 343 ~ 354

Significance of the Study

Scientific Significance

This study contributes to the academic literature on cybersecurity, information systems, cryptography, and digital risk management by examining an emerging security challenge that will shape the future of data protection. It links post-quantum cryptography with organizational readiness, which allows the topic to be studied not only as a technical cryptographic issue but also as a management and governance challenge.

Practical Significance

The study can help organizations understand how to prepare for the post-quantum transition. It highlights practical steps such as building a cryptographic inventory, identifying systems that depend on quantum-vulnerable algorithms, engaging vendors, prioritizing critical systems, and developing migration roadmaps. CISA, NSA, and NIST specifically recommend that organizations begin preparing by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments, and engaging technology vendors.

Security Significance

The study is significant for long-term data protection. Sensitive data that must remain confidential for many years may be exposed to future quantum decryption if organizations do not prepare early. Post-quantum cryptography therefore represents a strategic layer of protection for future confidentiality, integrity, authentication, and trust in digital systems.

Scope of the Study

Subject Scope

The study focuses on post-quantum cryptography, data security, cryptographic migration, organizational readiness, and future quantum-related cybersecurity risks.

Technical Scope

The study focuses mainly on public-key cryptography, key establishment, digital signatures, cryptographic inventory, migration planning, and NIST post-quantum standards.

Institutional Scope

The study may be applied to organizations that depend heavily on digital systems, such as banks, universities, government institutions, healthcare organizations, telecommunications companies, and cloud-based service providers.

Time Scope

The study focuses on the current transition period following the release of NIST's first post-quantum cryptography standards in 2024 and the recommended preparation period for migration toward quantum-resistant cryptography. NIST indicates that organizations should begin migration planning and that quantum-vulnerable algorithms are expected to be deprecated and ultimately removed from NIST standards by 2035, with high-risk systems transitioning earlier.

Key Terms of the Study

Post-Quantum Cryptography

Cryptographic algorithms designed to remain secure against both classical computers and future quantum computers.

Quantum-Vulnerable Cryptography

Cryptographic systems that may be broken by future quantum computers, especially systems based on integer factorization or discrete logarithm problems, such as RSA and many elliptic-curve systems.

Cryptographic Inventory

A documented list of cryptographic algorithms, protocols, certificates, keys, applications, devices, and systems used within an organization. This inventory helps identify where quantum-vulnerable cryptography is used.

Quantum Readiness

The organizational ability to identify, assess, prioritize, and migrate systems from quantum-vulnerable cryptography to quantum-resistant solutions.

Harvest Now, Decrypt Later

A threat model in which attackers collect encrypted data today and store it until future quantum computers become capable of decrypting it.

Proposed Conceptual Framework

The study may be built around the following model:

Independent Variables

1. Organizational awareness of quantum threats
2. Cryptographic inventory maturity
3. Cybersecurity governance and policy readiness
4. Vendor and supply-chain readiness
5. Technical infrastructure flexibility
6. Availability of cybersecurity expertise and training

Mediating Variable

Post-quantum cryptography migration readiness

Dependent Variable

Future data security protection

Conceptual Relationship

The study assumes that organizations with higher awareness, better cryptographic inventories, stronger governance, better vendor coordination, and more flexible infrastructure will have greater readiness to adopt post-quantum cryptography. This readiness is expected to improve future data security by reducing exposure to quantum-vulnerable cryptographic systems.

Research Hypotheses

For an applied quantitative study, the following hypotheses may be used:

H1: There is a statistically significant relationship between organizational awareness of quantum threats and post-quantum cryptography migration readiness.

H2: Cryptographic inventory maturity has a statistically significant effect on post-quantum cryptography migration readiness.

H3: Cybersecurity governance has a statistically significant effect on post-quantum cryptography migration readiness.

H4: Vendor and supply-chain readiness has a statistically significant effect on post-quantum cryptography migration readiness.

H5: Technical infrastructure flexibility has a statistically significant effect on post-quantum cryptography migration readiness.

H6: Post-quantum cryptography migration readiness has a statistically significant effect on future data security protection.

H7: Post-quantum cryptography migration readiness mediates the relationship between organizational preparedness factors and future data security protection.

Literature Review Structure

Cryptography and Data Security

This section discusses the role of cryptography in protecting confidentiality, integrity, authentication, and non-repudiation. It explains how traditional cryptographic systems support secure communication, digital signatures, certificates, software updates, online transactions, and identity management.

Quantum Computing as a Future Security Threat

This section explains how future quantum computers may threaten current public-key systems. It should discuss why organizations must prepare before the threat becomes operational, especially when data has a long secrecy lifetime. CISA, NSA, and NIST emphasize that early planning is necessary because migration takes time and because attackers may already be collecting data that will remain sensitive in the future.

Post-Quantum Cryptography

This section explains the concept of post-quantum cryptography and its role in resisting future quantum attacks. It should include the major NIST standards: ML-KEM for key encapsulation, ML-DSA for digital signatures, and SLH-DSA for stateless hash-based signatures. NIST also notes that ML-KEM, ML-DSA, and SLH-DSA are expected to provide the foundation for most post-quantum cryptography deployments and can be put into use now.

Post-Quantum Cryptography Standards

This section discusses the three initial NIST standards:

Standard	Algorithm	Function
FIPS 203	ML-KEM	Key establishment / key encapsulation
FIPS 204	ML-DSA	Digital signatures
FIPS 205	SLH-DSA	Stateless hash-based digital signatures

NIST states that FIPS 203 specifies a key encapsulation mechanism derived from CRYSTALS-KYBER, while FIPS 204 and FIPS 205 specify digital signature schemes derived from CRYSTALS-Dilithium and SPHINCS+, respectively.

Cryptographic Inventory and Migration Readiness

This section discusses the importance of identifying where quantum-vulnerable algorithms are used. The literature review should explain that cryptographic discovery should include network protocols, end-user systems, servers, applications, libraries, firmware and software updates, and CI/CD development pipelines. CISA, NSA, and NIST recommend that organizations create inventories to identify quantum-vulnerable cryptography and prioritize migration based on risk.

Vendor and Supply-Chain Readiness

This section examines the role of technology vendors, cloud providers, and commercial off-the-shelf systems in the migration process. Organizations are encouraged to engage vendors about their quantum-readiness roadmaps and to consider contract changes so that future products support post-quantum cryptography.

Challenges of Post-Quantum Migration

This section analyzes expected challenges, including:

1. Lack of visibility into cryptographic assets
2. Legacy systems and embedded cryptography
3. Compatibility with existing applications and protocols
4. Performance and implementation concerns
5. Vendor dependency
6. Cost and resource limitations
7. Shortage of specialized expertise
8. Governance and policy gaps
9. Difficulty prioritizing high-risk systems

Future of Data Security

This section explains how future data security will increasingly depend on crypto-agility, continuous risk assessment, quantum-safe algorithms, and institutional readiness. The discussion should connect post-quantum cryptography to broader cybersecurity strategies such as zero trust, secure software development, risk management, and supply-chain security.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 7, No.2. Jun. – Dec. 2025
Pages: 343 ~ 354

Research Methodology

Research Approach

The study may use a descriptive analytical approach because it aims to describe post-quantum cryptography, analyze its role in future data security, and examine readiness factors that influence adoption.

A stronger version of the study may use a mixed-methods approach, combining:

1. Document analysis of NIST, CISA, NSA, and cybersecurity standards.
2. Survey research targeting IT and cybersecurity professionals.
3. Interviews with cybersecurity managers or information security officers, if available.

Research Design

The proposed research design is an applied cybersecurity readiness study. It examines how organizational factors affect post-quantum cryptography migration readiness and how this readiness contributes to future data security protection.

Population of the Study

The population may include:

1. Cybersecurity professionals
2. IT managers
3. Network administrators
4. Information security officers
5. Digital transformation staff
6. Risk management officers
7. Cloud and infrastructure engineers
8. Software development and DevOps staff

Sample of the Study

A suitable sample may range from 50 to 150 respondents, depending on access to organizations. If the study is conducted in one sector, such as banking or telecommunications, the sample should include employees who work directly with IT infrastructure, cybersecurity, risk management, or digital systems.

Data Collection Tools

The study may use a questionnaire divided into the following sections:

1. Demographic and professional information
2. Awareness of quantum computing threats
3. Current use of public-key cryptography
4. Cryptographic inventory readiness
5. Governance and policy readiness
6. Vendor and supply-chain readiness

7. Technical readiness for post-quantum migration
8. Perceived future data security protection

Measurement Scale

A five-point Likert scale may be used:

1. Strongly disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly agree

Data Analysis Methods

The study may use:

1. Frequencies and percentages
2. Means and standard deviations
3. Cronbach's Alpha for reliability
4. Pearson correlation analysis
5. Simple and multiple regression analysis
6. Mediation analysis, if migration readiness is treated as a mediating variable

Qualitative thematic analysis for interview responses, if interviews are used

Proposed Questionnaire Dimensions

Dimension 1: Awareness of Quantum Threats

Sample items:

1. The organization understands the future risks of quantum computing to current encryption systems.
2. IT staff are aware of the concept of post-quantum cryptography.
3. Management recognizes the importance of preparing early for quantum-related cybersecurity risks.

Dimension 2: Cryptographic Inventory

Sample items:

1. The organization has identified where public-key cryptography is used.
2. The organization maintains an inventory of cryptographic algorithms, protocols, and certificates.
3. The organization can identify systems that depend on RSA, ECDH, or ECDSA.
4. The organization classifies data according to sensitivity and required confidentiality lifetime.

Dimension 3: Governance and Policy Readiness
Sample items:

1. The organization has cybersecurity policies that address future cryptographic risks.
2. Post-quantum migration is included in cybersecurity planning.
3. Senior management supports long-term data protection initiatives.
4. Risk assessment processes include future cryptographic threats.

Dimension 4: Vendor and Supply-Chain Readiness
Sample items:

1. The organization discusses post-quantum readiness with technology vendors.
2. Vendor contracts include security upgrade requirements.
3. Cloud providers are evaluated based on their quantum-readiness roadmaps.
4. The organization considers supply-chain dependencies in cryptographic migration planning.

Dimension 5: Technical Infrastructure Flexibility
Sample items:

1. Existing systems can be updated to support new cryptographic algorithms.
2. The organization has technical expertise to test post-quantum algorithms.
3. Legacy systems may create challenges for post-quantum migration.
4. The organization supports crypto-agility in system design.

Dimension 6: Future Data Security Protection
Sample items:

1. Post-quantum cryptography will improve long-term confidentiality of sensitive data.
2. Migration to quantum-resistant algorithms will reduce future cybersecurity risk.
3. Post-quantum cryptography will strengthen trust in digital services.
4. Quantum-safe security planning will improve organizational resilience.

Expected Findings

The study is expected to find that post-quantum cryptography is essential for long-term data security, particularly for organizations that store or transmit sensitive information with long confidentiality requirements. It is also expected to show that organizational readiness depends on awareness, cryptographic inventory, governance, vendor coordination, technical infrastructure, and cybersecurity expertise.

The study may also find that many organizations are still at an early stage of post-quantum readiness, especially in relation to cryptographic discovery and vendor coordination. This would align with the concern raised by CISA, NSA, and NIST that organizations often lack full visibility into their dependency on public-key cryptography.

sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol 7, No.2. Jun. – Dec. 2025
Pages: 343 ~ 354

Expected Contribution of the Study

This research is expected to contribute in four main ways:

1. It provides a structured academic explanation of post-quantum cryptography and its importance for future data security.
2. It links technical cryptographic standards with organizational readiness and cybersecurity governance.
3. It offers a practical framework for evaluating institutional preparedness for post-quantum migration.
4. It supports decision-makers in planning a gradual and risk-based transition toward quantum-resistant security.

Research Gap

Most discussions of post-quantum cryptography focus on the technical design of algorithms or the mathematical strength of quantum-resistant schemes. However, fewer applied studies examine how organizations can actually prepare for migration in real operational environments. The transition requires more than selecting algorithms; it requires cryptographic inventory, governance, vendor readiness, technical testing, budget planning, system modernization, and staff awareness.

Therefore, the research gap lies in examining organizational readiness for post-quantum cryptography adoption as a key factor in protecting future data security. This study addresses the gap by connecting post-quantum cryptography standards with practical institutional readiness and long-term data protection.

Proposed Post-Quantum Readiness Roadmap

A practical roadmap for organizations may include the following stages:

1. Awareness Stage: educate management and IT teams about quantum risks and post-quantum cryptography.
2. Inventory Stage: identify cryptographic assets, protocols, certificates, applications, and systems.
3. Risk Classification Stage: prioritize systems based on data sensitivity, confidentiality lifetime, and operational importance.
4. Vendor Engagement Stage: ask vendors and cloud providers about their post-quantum migration roadmaps.
5. Testing Stage: test post-quantum algorithms in non-production environments.
6. Policy Stage: update cybersecurity policies, procurement rules, and software development standards.
7. Implementation Stage: migrate high-risk systems first, followed by broader organizational deployment.

8. Monitoring Stage: continuously review standards, vulnerabilities, performance, and compliance requirements.

Conclusion

Post-quantum cryptography represents one of the most important future directions in data security. The threat is not only technical but also strategic, because organizations must prepare before quantum computers become capable of breaking current public-key cryptography. The release of NIST's post-quantum standards provides a foundation for migration, but successful adoption depends on organizational awareness, cryptographic inventory, governance, vendor readiness, and technical flexibility. This research plan provides a comprehensive framework for studying how post-quantum cryptography can protect future data security and how organizations can prepare for a quantum-safe digital environment.

References

1. CISA, NSA, & NIST. (2023). Quantum-readiness: Migration to post-quantum cryptography. Cybersecurity and Infrastructure Security Agency.
2. NIST. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology.
3. NIST. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology.
4. NIST. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology.
5. NIST CSRC. (2024). Announcing approval of three Federal Information Processing Standards for post-quantum cryptography. National Institute of Standards and Technology.
6. NIST CSRC. (2025). Post-Quantum Cryptography Project. National Institute of Standards and Technology.