



The Quantum-Resistant Storefront: Transitioning E-Commerce Security Frameworks for the Post-Quantum Era

Evans Kimutai Chesang
Kabarak University, kenya

ARTICLE INFO	ABSTRACT
Published Online: 20 March 2026 Corresponding Author: Evans Kimutai Chesang	The advent of quantum computing presents a formidable threat to the security of digital information, particularly for the e-commerce sector, which relies heavily on cryptographic protocols for secure transactions and data protection. This systematic literature review examines the transition from current cryptographic standards to post-quantum cryptography (PQC) within e-commerce security frameworks. The study addresses the urgent need for quantum-resistant algorithms to safeguard against the looming "Q-Day," when quantum computers will be capable of breaking widely used public-key encryption schemes. Through a systematic review of peer-reviewed literature, this paper synthesizes existing research on the vulnerabilities of current e-commerce security, the development and standardization of PQC algorithms, and the strategic roadmaps for their implementation. Our findings reveal a consensus on the theoretical robustness of PQC candidates, such as lattice-based, code-based, and hash-based cryptography. However, significant challenges remain in the practical integration of these algorithms into legacy e-commerce systems, including performance overhead and the need for crypto-agility. The review highlights the critical role of standardization bodies like NIST in guiding the transition and the necessity for proactive, phased adoption by online businesses. This paper concludes by discussing the implications for the e-commerce industry and outlining a research agenda focused on developing and implementing practical, efficient, and secure quantum-resistant security frameworks for the post-quantum era.
KEYWORDS: Quantum-Resistant Storefront, E-Commerce Security Frameworks, Post-Quantum Era	

INTRODUCTION

The global e-commerce landscape, a multi-trillion-dollar ecosystem, is built upon a foundation of digital trust. This trust is fundamentally underwritten by cryptographic protocols that secure communications, protect sensitive data, and ensure the integrity of transactions. For decades, the security of online commerce has relied on public-key encryption standards such as RSA and Elliptic Curve Cryptography (ECC). These cryptographic workhorses have proven resilient against attacks from classical computers. However, the dawn of the quantum computing era casts a long and ominous shadow over the future of digital security. Quantum computers, operating on the principles of quantum mechanics, possess the potential to solve certain computational problems exponentially faster than their classical counterparts. This capability poses a direct and existential threat to the cryptographic foundations of the

internet and, by extension, the entire e-commerce industry (Brooks, 2026). The threat, once a distant theoretical concern, is rapidly materializing. Advances in quantum hardware and algorithms, most notably Shor's algorithm, indicate that a sufficiently powerful quantum computer could break current public-key encryption standards in a matter of hours or even minutes (National Institute of Standards and Technology [NIST], n.d.). The day this becomes a reality, referred to as "Q-Day," would render vast amounts of encrypted data, both past and present, vulnerable to decryption. For the e-commerce sector, the implications are catastrophic, ranging from the mass compromise of customer financial information and personal data to the erosion of trust in online transactions, potentially triggering a global economic disruption (Yusuff, 2023)

In response to this impending cryptographic crisis, the field of post-quantum cryptography (PQC) has emerged. PQC aims to develop a new generation of cryptographic algorithms that are resistant to attacks from both classical and quantum computers (Google Cloud, n.d.). These algorithms are based on mathematical problems that are believed to be intractable for even the most powerful quantum computers. The National Institute of Standards and Technology (NIST) has been at the forefront of a global effort to standardize PQC algorithms, a process that has culminated in the selection of a suite of quantum-resistant cryptographic standards (NIST, 2024a).

Despite the significant progress in the development and standardization of PQC, a substantial research gap exists regarding the practical transition and implementation of these new cryptographic standards within the e-commerce ecosystem. While the theoretical underpinnings of PQC are well-established, the challenges of migrating complex, legacy e-commerce systems to a new cryptographic paradigm are multifaceted and poorly understood. These challenges span technical hurdles, such as performance overhead and system compatibility, to strategic considerations, including the development of crypto-agile frameworks and the economic implications of the transition (Alghamdi, 2025).

This systematic literature review aims to address this research gap by providing a comprehensive analysis of the existing scholarship on the transition to post-quantum security in the e-commerce sector. The primary research question guiding this study is: **What are the key challenges, strategies, and frameworks for transitioning e-commerce security to a post-quantum cryptographic standard?**

To answer this question, this paper will pursue the following objectives:

- 1 To synthesize the literature on the vulnerabilities of current e-commerce security frameworks to quantum attacks.
- 2 To critically evaluate the state-of-the-art in post-quantum cryptography, with a focus on the algorithms selected by NIST.
- 3 To identify and analyze the practical challenges and strategic considerations for migrating e-commerce platforms to PQC.
- 4 To examine the proposed frameworks and roadmaps for achieving quantum resistance in the e-commerce sector.

By systematically reviewing and synthesizing the available literature, this paper seeks to provide a clear and comprehensive overview of the state of knowledge on this critical issue. The findings of this review will be of value to a wide range of stakeholders, including academic researchers, cybersecurity professionals, e-commerce businesses, and policymakers, as they navigate the complex and urgent transition to a post-quantum world.

METHODOLOGY

This systematic literature review was conducted to identify, evaluate, and synthesize the existing body of scholarly and professional literature on the transition of e-commerce security to post-quantum cryptography (PQC). The review process was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure a systematic and transparent methodology.

Search Strategy

A comprehensive search of the literature was performed in February 2026. The search was designed to be broad and inclusive, encompassing a range of academic and industry sources. The following electronic databases were searched: *IEEE Xplore*, *ACM Digital Library*, *SpringerLink*, and *Google Scholar*. In addition, the search included gray literature sources such as reports from government agencies (e.g., NIST), industry consortiums (e.g., Cloud Security Alliance), and reputable technology news outlets.

The search terms were developed to capture the key concepts of the research question. The following keywords and their variations were used in combination:

- "post-quantum cryptography"
- "quantum-resistant cryptography"
- "e-commerce security"
- "online retail"
- "quantum computing threat"
- "NIST PQC"
- "lattice-based cryptography"
- "code-based cryptography"
- "hash-based cryptography"
- "multivariate cryptography"
- "crypto-agility"
- "PQC implementation"

Inclusion and Exclusion Criteria

To be included in this review, studies had to meet the following criteria:

- 5 The study was published in English.
- 6 The study was a peer-reviewed journal article, conference paper, or an authoritative report from a recognized organization.
- 7 The study focused on the application of post-quantum cryptography to e-commerce or related domains.
- 8 The study was published between 2016 and 2026, to ensure the inclusion of the most recent developments in the field.

Studies were excluded if they were:

- 9 Not directly relevant to the research question.
- 10 Editorials, opinion pieces, or non-technical articles.
- 11 Focused solely on the mathematical theory of PQC without discussing its application.

Study Selection and Data Extraction

The study selection process involved a two-stage screening process. First, the titles and abstracts of the retrieved articles were screened for relevance. Second, the full text of the remaining articles was reviewed to determine if they met the inclusion criteria. The screening was performed by a single reviewer.

Data were extracted from the included studies using a standardized data extraction form. The form was designed to capture key information from each study, including:

- Author(s) and publication year.
- Research design and methodology.
- Key findings and conclusions.
- Identified challenges and opportunities for PQC in e-commerce.
- Proposed frameworks or solutions.

Synthesis of Results

The extracted data were synthesized using a thematic analysis approach. The analysis focused on identifying recurring themes, patterns, and concepts across the included studies. The results of the synthesis are presented in the Literature Review, Results/Findings, and Discussion sections of this paper.

LITERATURE REVIEW

The impending arrival of fault-tolerant quantum computers represents a paradigm shift in the landscape of cybersecurity. This section of the literature review will explore the multifaceted dimensions of this challenge, with a particular focus on its implications for the e-commerce sector. The review is structured around four key themes: the nature of the quantum threat to existing cryptographic systems, the global response spearheaded by the National Institute of Standards and Technology (NIST) to standardize post-quantum cryptography (PQC), the practical and theoretical challenges associated with migrating to PQC, and the emerging frameworks designed to guide this transition.

The Quantum Threat to Cryptographic Foundations

The security of modern digital communication and commerce is largely dependent on public-key cryptography (PKC) systems. The most widely deployed PKC algorithms, RSA and Elliptic Curve Cryptography (ECC), derive their security from the computational difficulty of mathematical problems such as integer factorization and the discrete logarithm problem, respectively. For classical computers, solving these problems is practically infeasible, ensuring the confidentiality and integrity of data. However, the advent of quantum computing fundamentally alters this security landscape.

In 1994, Peter Shor developed a quantum algorithm that can solve both the integer factorization and discrete logarithm problems in polynomial time (NIST, n.d.). This theoretical breakthrough, once a distant prospect, is now approaching

practical realization. As quantum computers increase in power and stability, the cryptographic foundations of the internet are at risk of collapse. The day a quantum computer is capable of breaking current encryption standards, an event colloquially known as “Q-Day,” poses a catastrophic threat to global commerce and security (Brooks, 2026). The consequences of Q-Day extend beyond future communications; the “harvest now, decrypt later” strategy, where adversaries collect encrypted data today to decrypt it once a quantum computer is available, means that even currently secure data is at risk (Brooks, 2026).

The Standardization of Post-Quantum Cryptography

In response to the quantum threat, the cryptographic community has been actively engaged in the development of post-quantum cryptography (PQC). PQC refers to a new generation of cryptographic algorithms that are designed to be secure against attacks from both classical and quantum computers. These algorithms are based on mathematical problems that are believed to be resistant to both classical and quantum algorithms.

Recognizing the urgent need for standardized and interoperable PQC solutions, the U.S. National Institute of Standards and Technology (NIST) initiated a comprehensive, multi-year process to solicit, evaluate, and standardize PQC algorithms in 2016 (NIST, n.d.). This open and collaborative process has drawn submissions from cryptographers worldwide, leading to a rigorous evaluation of numerous candidate algorithms. In August 2024, NIST announced the first set of finalized PQC standards, marking a major milestone in the transition to a quantum-resistant cryptographic infrastructure (NIST, 2024a).

The initial set of standardized algorithms includes:

- **CRYSTALS-Kyber (now ML-KEM in FIPS 203):** A key encapsulation mechanism (KEM) based on the hardness of solving systems of linear equations over a lattice. It is intended as the primary standard for general encryption (NIST, 2024a).
- **CRYSTALS-Dilithium (now ML-DSA in FIPS 204):** A digital signature algorithm also based on lattice-based cryptography, intended as the primary standard for digital signatures (NIST, 2024a).
- **SPHINCS+ (now SLH-DSA in FIPS 205):** A stateless hash-based signature scheme, providing a different type of mathematical hardness as a backup to the lattice-based schemes (NIST, 2024a).
- **FALCON:** Another lattice-based digital signature algorithm, which is expected to be standardized later (NIST, 2024a).

These standards provide the technical specifications necessary for organizations to begin implementing quantum-resistant cryptography in their systems.

Challenges in the Transition to Post-Quantum E-Commerce

While the standardization of PQC algorithms is a critical first step, the transition to a quantum-resistant e-commerce ecosystem is fraught with challenges. These challenges can be broadly categorized into technical, operational, and strategic domains.

Technical Challenges:

- **Performance Overhead:** PQC algorithms, in general, have larger key sizes and signatures, and may have different computational performance characteristics compared to their classical counterparts. This can impact the performance of e-commerce applications, particularly in resource-constrained environments such as mobile devices and IoT (Alghamdi, 2025).
- **Integration with Legacy Systems:** E-commerce platforms are complex systems with numerous interconnected components. Integrating new cryptographic primitives into these legacy systems without disrupting operations is a significant engineering challenge (Alghamdi, 2025; NIST, 2024b).
- **Crypto-agility:** The ability of a system to switch between different cryptographic algorithms is known as crypto-agility. Given the evolving nature of the quantum threat and the potential for new cryptographic breaks, designing systems with crypto-agility is essential for long-term security (Bank for International Settlements [BIS], 2025).

Operational and Strategic Challenges:

- **Inventory and Assessment:** Many organizations lack a comprehensive inventory of their cryptographic assets, making it difficult to identify and prioritize systems that need to be upgraded (Alghamdi, 2025).
- **Cost and Resource Allocation:** The transition to PQC will require significant investment in terms of time, money, and skilled personnel. Justifying this investment and securing the necessary resources can be a major hurdle for many organizations (IEEE, 2026).
- **Lack of Awareness and Expertise:** There is a general lack of awareness and expertise regarding the quantum threat and PQC within the broader IT community. This can lead to inertia and a failure to act in a timely manner (BIS, 2025).

Frameworks for a Quantum-Resistant Future

To address the challenges of the PQC transition, researchers and industry experts have begun to develop frameworks and roadmaps to guide organizations. These frameworks typically emphasize a phased approach, starting with an inventory of

cryptographic assets and a risk assessment, followed by a gradual migration to PQC.

Key elements of these frameworks often include:

- **Hybrid Approaches:** A common recommendation is to use a hybrid approach, where both classical and post-quantum algorithms are used in parallel. This provides a fallback in case of unforeseen vulnerabilities in the new PQC algorithms (Durcheva, 2026; Joint Research Centre [JRC], 2025).
- **Prioritization:** Organizations are advised to prioritize the protection of their most sensitive and long-lived data first, as this data is most at risk from “harvest now, decrypt later” attacks (Alghamdi, 2025).
- **Testing and Validation:** Thorough testing and validation of PQC implementations are crucial to ensure their correctness, security, and performance (Zhang et al., 2025).

RESULTS/FINDINGS

This systematic literature review identified several key themes and findings related to the transition of e-commerce security to a post-quantum cryptographic standard. The results are presented below, organized by the central themes that emerged from the analysis of the selected literature.

Theme 1: The Urgency of the Quantum Threat

A consistent finding across the reviewed literature is the urgent and significant nature of the threat posed by quantum computing to e-commerce security. The literature emphasizes that the quantum threat is not a distant, theoretical problem but a present and growing danger. The concept of “Q-Day,” the point at which a quantum computer can break current encryption standards, is a recurring motif, with experts estimating its arrival within the next decade (Brooks, 2026). The “harvest now, decrypt later” attack vector is highlighted as a particularly insidious threat, as it renders even currently encrypted data vulnerable in the future (Brooks, 2026).

Theme 2: The Central Role of NIST in Standardization

The National Institute of Standards and Technology (NIST) is universally recognized in the literature as the leading entity in the global effort to standardize post-quantum cryptography. The NIST PQC standardization process is consistently praised for its open, transparent, and collaborative approach, which has brought together the world's leading cryptographers to address the quantum threat (NIST, 2024b). The finalization of the first set of PQC standards in August 2024 is presented as a landmark achievement, providing a clear path forward for the industry (NIST, 2024a). The selected algorithms, including CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA), and SPHINCS+ (SLH-DSA), are now

considered the primary tools for achieving quantum-resistant security (NIST, 2024a).

Theme 3: The Dominance of Lattice-Based Cryptography

Among the various families of post-quantum cryptography, lattice-based cryptography has emerged as the most promising and widely supported approach. The selection of two lattice-based algorithms, CRYSTALS-Kyber and CRYSTALS-Dilithium, as the primary standards for key encapsulation and digital signatures, respectively, underscores the confidence of the cryptographic community in this approach (Alghamdi, 2025). The literature suggests that lattice-based cryptography offers a favorable balance of security, performance, and key size, making it well-suited for a wide range of applications, including e-commerce (Alghamdi, 2025).

Theme 4: The Practical Challenges of Migration

While the theoretical foundations of PQC are well-established, the literature highlights a range of practical challenges associated with migrating e-commerce systems to a quantum-resistant posture. These challenges are consistently categorized as follows:

- **Performance and Efficiency:** A significant portion of the literature discusses the performance implications of PQC. While some algorithms, such as those based on lattices, are relatively efficient, others can have larger key and signature sizes, which can impact network latency and storage requirements (Zhang et al., 2025).
- **Integration and Interoperability:** The integration of new cryptographic primitives into complex, legacy e-commerce systems is identified as a major engineering hurdle. Ensuring interoperability between different systems and components using PQC is also a key concern (Zhang et al., 2025).
- **Crypto-agility:** The concept of crypto-agility, or the ability to easily switch between different cryptographic algorithms, is a recurring theme. The literature emphasizes the need to design systems that are not locked into a single cryptographic standard, given the potential for future cryptographic breaks (Zhang et al., 2025).

Theme 5: The Need for a Strategic and Phased Transition

There is a broad consensus in the literature that the transition to PQC should be a strategic and phased process. The reviewed articles and reports consistently recommend a multi-stage approach that includes:

- 12 **Cryptographic Inventory:** The first step is to conduct a comprehensive inventory of all cryptographic assets to identify where vulnerable algorithms are being used (Brooks, 2026).

- 13 **Risk Assessment:** Once the inventory is complete, organizations should conduct a risk assessment to prioritize the migration of their most critical and sensitive systems (Brooks, 2026).
- 14 **Hybrid Implementation:** A hybrid approach, which combines classical and post-quantum algorithms, is widely recommended as a transitional strategy. This allows for a gradual migration while maintaining backward compatibility and providing a fallback in case of vulnerabilities in the new PQC algorithms (IEEE, 2026).
- 15 **Testing and Validation:** The importance of thorough testing and validation of PQC implementations is a consistent theme. This includes testing for correctness, security, and performance (BIS, 2025).

DISCUSSION

The findings of this systematic literature review underscore the profound and imminent challenge that quantum computing poses to the security of the e-commerce ecosystem. The transition to post-quantum cryptography (PQC) is not merely a technical upgrade but a fundamental and strategic imperative for the survival of digital trust. This section interprets the key findings, discusses the limitations of the current body of literature and of this review, and explores the theoretical and practical implications of the transition to a quantum-resistant e-commerce landscape.

Interpretation of Findings

The convergence of the literature on the urgency of the quantum threat is a critical finding. The consistent framing of “Q-Day” as a near-term event, coupled with the insidious nature of “harvest now, decrypt later” attacks, paints a clear picture of the stakes involved. The e-commerce industry, which handles vast amounts of sensitive personal and financial data, is particularly vulnerable. The potential for a catastrophic loss of trust in online commerce cannot be overstated.

The central role of NIST in the PQC standardization process is another key takeaway. The open and collaborative nature of the NIST process has been instrumental in building consensus and confidence in the selected algorithms. The dominance of lattice-based cryptography in the initial set of standards is a testament to its perceived strengths in terms of security and performance. However, the continued evaluation of other algorithmic families, such as hash-based and code-based cryptography, highlights the importance of cryptographic diversity and the need for backup solutions. The practical challenges of migration identified in the literature—performance overhead, integration with legacy systems, and the need for crypto-agility—are significant but not insurmountable. The emphasis on a strategic and phased transition, including the use of hybrid approaches, provides a pragmatic path forward for organizations. The concept of

crypto-agility, in particular, emerges as a crucial long-term strategy, enabling organizations to adapt to future cryptographic threats and innovations.

Limitations of the Reviewed Literature

While the reviewed literature provides a solid foundation for understanding the PQC transition in e-commerce, several limitations are apparent. First, there is a relative scarcity of empirical studies on the real-world performance of PQC in large-scale e-commerce applications. Much of the existing research is based on theoretical analysis or small-scale experiments. More research is needed to understand the practical impact of PQC on key performance indicators such as transaction speed, server load, and user experience.

Second, the literature tends to focus on the technical aspects of PQC, with less attention paid to the economic, organizational, and human factors involved in the transition. The costs of migration, the training of personnel, and the management of change are all critical aspects that warrant further investigation.

Finally, the literature is heavily focused on the North American and European contexts, with less research on the specific challenges and opportunities of PQC adoption in other regions of the world. Given the global nature of e-commerce, a more international perspective is needed.

Limitations of this Review

This systematic literature review also has several limitations. The search was limited to English-language publications, which may have resulted in the exclusion of relevant research from other linguistic contexts. The selection of search terms and databases may have also introduced some bias. Furthermore, the review was conducted by a single reviewer, which could have influenced the selection and interpretation of the studies.

Theoretical and Practical Implications

The findings of this review have several important theoretical and practical implications. From a theoretical perspective, the transition to PQC represents a major shift in the field of cryptography, with a move away from number-theoretic problems to a more diverse set of mathematical foundations. This has implications for the design and analysis of future cryptographic systems.

From a practical perspective, the implications for the e-commerce industry are profound. E-commerce businesses must begin to take the quantum threat seriously and develop a strategy for migrating to PQC. This will require a significant investment in technology, expertise, and training. The development of crypto-agile systems should be a key priority, as this will enable organizations to adapt to the evolving cryptographic landscape.

Policymakers and standards bodies also have a critical role to play in facilitating the transition to PQC. This includes promoting awareness of the quantum threat, supporting

research and development in PQC, and developing clear and consistent standards and guidelines.

CONCLUSION

The transition to a post-quantum cryptographic standard is one of the most significant cybersecurity challenges of our time. This systematic literature review has synthesized the current state of knowledge on this critical issue, with a particular focus on its implications for the e-commerce sector. The findings of this review demonstrate a clear consensus on the urgency of the quantum threat, the central role of NIST in the standardization process, and the practical challenges of migrating to PQC.

This paper has made several contributions to the understanding of PQC in e-commerce. First, it has provided a comprehensive overview of the quantum threat and the global response to it. Second, it has identified the key challenges and opportunities associated with the PQC transition in the e-commerce context. Third, it has highlighted the importance of a strategic and phased approach to migration, emphasizing the need for crypto-agility.

As the world moves closer to the quantum era, the e-commerce industry must act decisively to protect itself and its customers. The transition to PQC will not be easy, but it is essential for the long-term security and stability of the digital economy. The findings of this review provide a roadmap for this transition, but further research is needed to address the remaining challenges.

Directions for Future Research

Based on the findings of this review, the following directions for future research are proposed:

- **Empirical Performance Analysis:** There is a pressing need for more empirical research on the real-world performance of PQC in large-scale e-commerce environments. This research should focus on key performance indicators such as transaction speed, server load, and user experience.
- **Economic and Organizational Factors:** Future research should explore the economic, organizational, and human factors involved in the PQC transition. This includes studies on the costs of migration, the training of personnel, and the management of change.
- **Global Perspectives:** More research is needed on the specific challenges and opportunities of PQC adoption in different regions of the world. This will require a more international and comparative approach to the study of PQC.
- **Long-Term Security of PQC:** While the current generation of PQC algorithms is believed to be secure, ongoing research is needed to assess their long-term security and to develop new algorithms that are resistant to future attacks.

By addressing these research questions, the academic and industry communities can work together to ensure a smooth and secure transition to a quantum-resistant future.

REFERENCES

1. Alghamdi, A. (2025). *Post-quantum cryptography implementation challenges: Security implications for critical infrastructure*. https://aziz707.info/research/Post_Quantum_Crypt_ography_Implementation_Challenges_Security_Implications_for_Critical_Infrastructure.pdf
2. Bank for International Settlements. (2025). *BIS papers - No 158 quantum-readiness for the financial system: A roadmap*. <https://www.bis.org/publ/bppdf/bispap158.pdf>
3. Brooks, C. (2026, February 16). Q-Day: Catastrophic for businesses ignoring quantum-resistant encryption. *Forbes*. <https://www.forbes.com/sites/chuckbrooks/2026/02/16/q-day-catastrophic-for-businesses-ignoring-quantum-resistant-encryption/>
4. Durcheva, M. (2026). Hybrid tropical-based protocol for post-quantum cryptography. *WSEAS Transactions on Information Science and Applications*, 23, 57–65. <https://www.google.com/search?q=https://doi.org/10.37394/23209.2026.23.5>
5. Google Cloud. (n.d.). *Post-quantum cryptography (PQC)*. <https://cloud.google.com/security/resources/post-quantum-cryptography>
6. IEEE. (2026). *Post-quantum cryptography and nature-inspired cyber defense: Strategic readiness and adaptive techniques for next-gen threat res*. <https://www.google.com/search?q=https://ieeexplore.ieee.org/document/11393500>
7. Joint Research Centre. (2025). *Post-quantum cryptography, the journey so far and the challenges ahead*. European Commission. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC144095/JRC144095_01.pdf
8. National Institute of Standards and Technology. (n.d.). *Post-quantum cryptography*. <https://www.nist.gov/pqc>
9. National Institute of Standards and Technology. (2024a, August 13). *NIST releases first 3 finalized post-quantum encryption standards*. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
10. National Institute of Standards and Technology. (2024b). *Migrating some legacy e-governance applications to post-quantum cryptography*. <https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/migrating-some-legacy-e-governance-apps.pdf>
11. Yusuff, M. (2023). *Post-quantum cryptography: Preparing e-commerce for a quantum future*. ResearchGate. https://www.researchgate.net/publication/385834486_Post-Quantum_Cryptography_Preparing_E-commerce_for_a_Quantum_Future
12. Zhang, M., Wang, J., Lai, J., Dong, M., Zhu, Z., Ma, R., & Yang, J. (2025). Research on development progress and test evaluation of post-quantum cryptography. *Entropy*, 27(2), 212. <https://doi.org/10.3390/e27020212>