Vol. 7, No. 4, December 2025

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Quantum Computing Cryptography: A Systematic Review of Innovations, Applications, Challenges, and Algorithms

Peter Maitireni[1], Vusumuzi Ncube[2], Belinda Ndlovu[3], Thando Sibanda[4]

[1,2,3,4]Informatics Analytics Department, National University of Science and Technology, Bulawayo, Zimbabwe

Email: pamitireni@gmail.com[1], vusncube@gmail.com[2], belinda.ndlovu@nust.ac.zw[3], catherinethandosibanda@gmail.com[4]

Received: Oct 11, 2025

Revised: Nov 5, 2025

Accepted: Nov 24, 2025

Published: Dec 10, 2025

Corresponding Author

Author Name*:

Belinda Ndlovu

Email*:

belinda.ndlovu@nust.ac.zw

DOI:

10.63158/journalisi.v7i4.1331

Abstract. This study explores how to build quantum-resistant systems to safeguard digital infrastructure in the post-quantum era by uncovering the innovations, applications, algorithms, and challenges of Quantum Computing cryptography. Utilizing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses approach a search was conducted across the following databases for the years 2021–2025: PubMed, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. We shortlisted 15 studies from 519 screened articles for a comprehensive evaluation based on their relevance. Findings show strong adoption in finance, healthcare, IoT, cybersecurity, and e-government, with lattice-based PQC emerging as the most dominant cryptographic family, followed by QKD and hybrid PQC–QKD models. The review highlights key obstacles, including transition complexity, lack of global standards, high implementation costs, and integration difficulty. The study contributes by providing the first sector-aligned synthesis of innovations, identifying algorithmic trends, and mapping global research disparities through a conceptual model. It also presents a structured set of future research directions to guide policymakers, cryptographers, and practitioners preparing for quantum-enabled threats.

Keywords: Post-Quantum Cryptography, Quantum Computing Cryptography, Quantum Key Distribution, Quantum-Safe Blockchain, Quantum Machine Learning

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

Quantum computing is a cutting-edge technology based on the principles of quantum mechanics to handle information. It utilizes quantum bits (qubits), which can be in multiple states simultaneously, rather than conventional bits (0 or 1) as in classical computing. A qubit can be in multiple states at the same time because of quantum superposition and entanglement. As a result, data processing can be performed in a single step, providing significant computational power for complex tasks [1].

Quantum cryptography is the ultimate way of protection in the future, when cybercrime will be at an even higher level, where hackers with quantum computers could decrypt some historically used cryptographic systems [2]. This area comprises two major parts: Post-Quantum Cryptography (PQC), which focuses on developing classical algorithms that can withstand quantum attacks [3], and Quantum Key Distribution (QKD), which leverages quantum effects to establish secure communication channels. As quantum computers become increasingly capable of solving complex problems, classical cryptographic systems will become less effective, and new quantum-resistant cryptographic protocols will need to be developed [4].

The lack of a shared understanding of innovations, applications, challenges, and algorithms makes it difficult to place different approaches in context and compare them, hindering the easy identification of the most suitable ones for particular cases. Moreover, there is a lack of interdisciplinary collaboration between quantum cryptography and other emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), and Blockchain to create quantum-secured ecosystems [5], [6], [7]. Deploying quantum cryptography requires significant infrastructure investment, training, and standardization, which is daunting for most organizations [8], [9]. The lack of hybrid cryptographic solutions, such as combining PQC and QKD, warrants further research [10]. Hybrid solutions can be stronger and more versatile, but their strengths and weaknesses are not examined in-depth [11].

Although there are several reviews, no consolidated systematic literature review (SLR) exists in the quantum cryptography sector that reports on innovations, applications, algorithm families, and adoption challenges within a coherent analytical framework. Some

existing reviews either focus on quantum algorithm development or on experimental QKD deployments, leaving a yawning gap in understanding the foci of these technological threads, the situated adoption, and the international systemic blocks that remain. This review aims to bridge this gap by synthesizing all evidence generated since 2021–2025, which also saw a rapid upsurge in quantum hardware. Over this cycle, an elaboration of the National Institute of Standards and Technology (NIST) PQC standard was set, preparing this interim as an equally interesting moment to capture remarkable progress. In its kind, this SLR, unlike its antecedents, blends algorithmic, sectoral, and deployment challenges within a single analytical framework.

Research Questions

1. What are the most recent significant innovations in quantum computing cryptography?
2. In which application areas is quantum computing cryptography being deployed or planned?
3. What are the primary challenges faced when integrating quantum computing with existing cryptographic systems?
4. Which quantum and post-quantum algorithms are central to current cryptographic developments?
5. What future research directions are required to advance scalable, interoperable, and sector-specific quantum-safe cryptographic systems?

2. METHODS

This Systematic Literature Review (SLR) will follow established guidelines, such as the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [12]. The review aims to consolidate current information on applications, innovations, challenges, and algorithms in Quantum Computing Cryptography (QCC).

2.1. Database Search Strategy

The investigations were conducted across digital libraries using the following query: ("quantum computing cryptography") AND ("innovations" OR "applications" OR "challenges" OR "algorithms"). The search was executed across five digital libraries: PubMed (n=92), SpringerLink (n=25), IEEE Xplore (n=20), ScienceDirect (n=13), and Google Scholar (n=369).

A total of 519 studies were examined, and 15 studies were chosen for the final SLR table using inclusion and exclusion criteria.

2.2. Inclusion and Exclusion Criteria

Five digital libraries were explored to find the current status of quantum computing cryptography. The search was restricted to peer-reviewed English-language papers from 2021 to 2025. The period between 2021 and 2025 was chosen mainly because it matches the peak of the NIST PQC standardization activities, quite a few QKD pilot projects, and a significant increase in mixed PQC–QKD research. Previous studies do not take into account the recent progress, while future ones are still emerging. Only studies with valid literature on QCC focusing on innovations, applications, challenges, and algorithms were included. Studies on programming or development of cryptographic algorithms were excluded.

2.3. Screening

Among the 253 examined studies, a full-text review was conducted that encompassed not only theoretical developments in quantum cryptography but also the emergence of cryptographic protocols tailored for quantum security, the implementation of quantum-safe encryption algorithms, and the challenges posed by gaps in post-quantum security models. At this level, 238 manuscripts were dismissed on various grounds. The reasons included (1) SLRs, (2) works in other focus areas either in development or programming, (3) lack of data about innovations, applications, algorithms, and challenges, (4) unavailability of full text, and some were in non-English languages. Three reviewers, working independently, reviewed all titles, abstracts, and the entire text. Any differences in opinions were resolved through discussion until an agreement was reached, thereby assuring the reliability of the methodology. During the pilot screening, Cohen's kappa was calculated to check the consistency, after which screening of the remaining papers with consensus resolution continued.

2.4. Included

Only 15 studies that matched the predefined inclusion criteria were included. While some papers, such as SLRs, were excluded, they will be useful in providing relevant literature for the ultimate understanding of Quantum computing cryptography.

2.5. Quality Assessment

The determination of the academic quality and integrity of the chosen studies was an indispensable factor in the reliability of this systematic literature review. The quality appraisal phase assumed a multi-criteria position based on established SLR traditions, particularly those derived from PRISMA and cryptographic research standards. The appraisal process was guided by five dimensions: proximity to the underlying research questions, peer-review status, accessibility of the methodology, theoretical and practical contributions, and authors' institutional credibility. The first step in the study selection was to ensure that the studies addressed the four main topics of the review: innovations, applications, challenges, and algorithms in quantum computing cryptography.

To maintain academic credibility, only peer-reviewed journal articles or papers presented at reputable conferences from 2021 to 2025 were included. Methodological transparency was another key factor for study inclusion; all studies were required to state their research method, whether empirical, theoretical or simulation-based, to help in the process of reproducibility and deep analysis. Moreover, papers that presented new frameworks, quantum-resistant protocols, or practical applications were given priority as a way of capturing the contemporary state of the art in the field. The last level of filtering was checking the authors' credentials and institutional affiliations to ensure that there was representation from recognized thought leaders and institutions that are actively involved in the field of quantum cryptography.All fifteen studies selected for synthesis satisfied at least four of these five standards, attesting to the rigour and representativeness of the review corpus. This systematic assessment worked to bring together a body of research that is both methodologically sound and strategically relevant in arriving at an understanding of the quantum security paradigm. Table 1 presents the quality assessment.

Table 1. Quality Assessment Criteria

Assessment Criterion	Description	Quality Indicators	Included Studies (n = 15)
Relevance to Research Questions	Degree to which each study aligns with innovations, applications,	Clear research focus; explicit cryptography/quantum themes	All 15 studies (100%) directly addressed ≥2 thematic pillars

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Assessment Criterion	Description	Quality Indicators	Included Studies (n = 15)
	challenges, and algorithms in QCC		
Peer-Review Status	Publication in a peer-reviewed journal or reputable conference	Journal-indexed, Scopus/IEEE/Springer, formally reviewed	15/15 (100%) were peer-reviewed conference/journal papers
Methodological Transparency	Clarity of methods, models, simulations, or theoretical analysis used	Detailed methodology, reproducibility, clear assumptions	12 studies (80%) had clear methodological detail; 3 (20%) limited
Theoretical & Practical Contribution	Contribution toward PQC, QKD, hybrid systems, or sector-specific deployment	New frameworks, algorithms, analyses, or real-world relevance	11 studies (73%) offered strong contributions; 4 (27%) moderate
Institutional Credibility	Reputation of authors or institutions in cryptography/quantum research	Affiliation with universities, labs, or national agencies	13 studies (87%) from recognised research institutions
Clarity of Reporting	Organisation, coherence, and use of figures/tables	Clear visualisations and reporting structures	10 studies (67%) highly clear; 5 studies (33%) acceptable clarity
Algorithmic Rigor	Soundness of cryptographic analysis, PQC/QKD evaluation	Proper cryptographic assumptions and proofs used	9 studies (60%) high rigour; 6 (40%) preliminary or conceptual
Use of Empirical or Simulation Evidence	Experiments, pilot deployments, performance tests	Datasets, simulations, hardware tests	7 studies (47%) empirical; 8 (53%) theoretical
Discussion of Limitations	Transparency regarding constraints or future challenges	Hardware limits, scalability, cost, SNDL, standardisation	11 studies (73%) explicitly discussed limitations

3. RESULTS AND DISCUSSION

The graphical PRISMA flow diagram in Figure 1 provides a visual representation of the studies that met the inclusion criteria outlined in Table 2. This diagram helps illustrate the selection process, ensuring transparency in identifying the relevant research articles for further analysis.

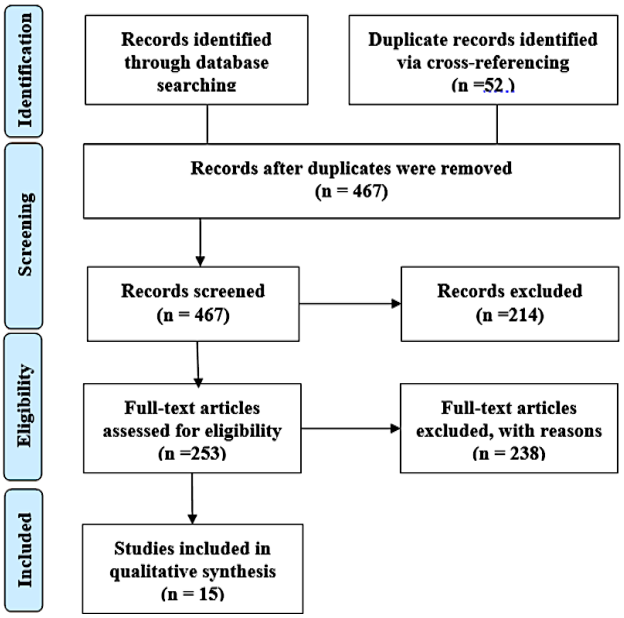

Figure 1. PRISMA Flow Diagram

Table 2 presents a comprehensive summary of 15 studies that satisfied the inclusion criteria for this review. The table outlines the key innovations, application areas, challenges faced, and the specific algorithms employed in each selected study. By synthesizing these aspects, we can better understand the diverse approaches being used in post-quantum cryptography and related fields.

Table 2 also highlights the geographical distribution of the studies, with research originating from a variety of countries including Liberia, India, Bangladesh, Nigeria, the USA, the UK, and others. The selected studies focus on several advanced cryptographic techniques, such as post-quantum cryptography, quantum key distribution, hybrid cryptography, and quantum machine learning. These innovations are applied across various domains, including finance, cybersecurity, healthcare, telecommunications, blockchain, and e-governance. In addition to showcasing the application areas, Table 2

identifies common challenges that researchers face, including transition complexities, standardization issues, scalability problems, and integration difficulties. These challenges underscore the importance of overcoming existing limitations to ensure the broader adoption of quantum-safe cryptographic methods. Table 2 also details the algorithms used in each study, such as lattice-based methods, Shor's algorithm, Grover's algorithm, and code-based algorithms. These algorithms are central to the proposed solutions in the context of post-quantum cryptography and related applications.

Table 2. Summary of Selected Studies

Source	Country	Innovations	Applications Areas	Challenges	Algorithm used
[13]	Liberia.	• Post Quantum Cryptography • Quantum Key Distribution • Hybrid Cryptography • Quantum Machine Learning • Quantum-secure Blockchain • Quantum Random Number Generation	• Finance • Blockchain • Cybersecurity	• Transition Complexity • Standardization Issues • Integration Issues • Security Concerns	• Lattice-based • Shor's Algorithm • Grover's Algorithm • Code-based • Multivariate Based
[14]	India	• Post Quantum Cryptography • Quantum Machine Learning • Hybrid Cryptography • Quantum-secure Blockchain	• Telecommunications • Healthcare • Finance • Cybersecurity • Blockchain	• Transition Complexity • Standardization issues • Integration Issues • Scalability Issues	• Lattice-based • Shor's Algorithm • Grover's Algorithm • Code-based Multivariate-based
[15]	Bangladesh	• Post Quantum Cryptography • Quantum Security	• E-Governance • Cybersecurity • Defence • Finance	• Integration Issues • Technological Limitations	• Lattice-based • Shor's Algorithm • Grover's Algorithm • Hash-based

Source	Country	Innovations	Applications Areas	Challenges	Algorithm used
[16]	Nigeria	• Post Quantum Cryptography • Hybrid Cryptography	• E-Governance • Finance • Telecommunications	• Transition Complexity • Standardization Issues	• Shor's Algorithm • Grover's Algorithm
[17]	India	• Post Quantum Cryptography • Quantum Key Distribution	• Finance • Telecommunications • Defence • Cybersecurity • E-Governance	• Standardization Issues • Scalability Issues • Security Concerns • High Costs • Technological Limitations	• Shor's Algorithm • Grover's Algorithm • BB84 Protocol
[18]	USA	• Post Quantum Cryptography • Quantum Key Distribution	• Healthcare • Internet of Things • E-Government • Finance	• Transition Complexity • Standardization Issues • Implementation Issues	• Lattice-based • Shor's Algorithm. • Grover's Algorithm
[19]	USA	• Post Quantum Cryptography • Quantum Key Distribution • Quantum Security	• Healthcare • Internet of Things • E-Government • Defence • Blockchain	• Transition Complexity • Standardization Issues • Integration Issues • Breaking Classical Encryption	• Lattice-based • Shor's Algorithm • Grover's Algorithm • Code-based
[20]	UK	• Hybrid Cryptography • Quantum Machine Learning • Quantum Digital Signatures	• Healthcare • Finance • Defence • E-Government • Blockchain • Cybersecurity	• Transition Complexity • Scalability Issues • High Costs	• Shor's Algorithm • Grover's Algorithm • Quantum Approximate Optimization Algorithm (QAOA)
[21]	USA	• Quantum Key Distribution	• Finance • Cybersecurity • Security	• Transition Complexity	• The Rawal Liang and

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Source	Country	Innovations	Applications Areas	Challenges	Algorithm used
		• Industry 4.0 Technologies	• E-Commerce	• Security Concerns • High costs • Implementation issues	Peter (RLP) Protocol • BB84 Protocol • TS-QKD Protocol
[22]	India	• Post Quantum Cryptography	• Finance • Internet of Things • Infrastructure • Telecommunications • Cloud computing • Quantum-safe Blockchain	• Transition complexity • Standardization Issues • Implementation issues • Performance Trade-Offs	• Lattice-Based • Code-Based • Multivariate-based • Hash-Based
[23]	Australia	• Post Quantum Cryptography	• Finance • Defence • Cloud computing.	• Integration Issues • Security concerns • Breaking Classical Encryption	• Lattice-based • Code-Based • Multivariate-based • Hash-Based
[24]	India	• Post Quantum Cryptography • Quantum Key Distribution • QNP	• Healthcare • Finance • Machine Learning • Telecommunications	• Transition Complexity • Integration Issues • Scalability Issues	• Lattice-Based • Multivariate-Based • Isogeny-Based
[25]	Japan	• Hybrid Cryptography • Quantum Digital Signatures	• Telecommunications • Infrastructure • Security	• Integration Issues • Scalability Issues • Security Concerns • Implementation Issues • Technological Limitations.	• Hybrid Cryptographic techniques

Source	Country	Innovations	Applications Areas	Challenges	Algorithm used
[26]	USA	• Post Quantum Cryptography • Hybrid Cryptography	• Healthcare • Security • Blockchain • Infrastructure • E-Commerce	• Standardization Issues • Integration Issues • High costs • Policy Issues • Technological Limitation • Performance Trade-Offs	• Lattice-based • Multivariate-Based • Code-Based • Hash-Based
[27]	Vietnam	• Post Quantum Cryptography	• Internet of Things • Cloud computing • Security	• Transition Complexity • Standardization Issues • High Costs • Performance Trade-Offs	• Lattice-based • Multivariate-based • Code-based • Hash-Based • Hybrid Cryptographic techniques

3.1. Publications by continent

Figure 2 shows the comparison of studies by continent. The systematic literature review of QCC reveals a significant geographic disparity in the number of publications. Asia leads with 46% of the publications, primarily driven by India, Bangladesh, Japan, and Vietnam, reflecting a high level of investment and interest in quantum cryptography, which is likely driven by research capacity and technological advancements. The orientation of research in this continent is towards practical applications, such as quantum-resistant blockchain and sectoral solutions in finance and healthcare, indicating the region's commitment to harnessing quantum technology for real-world impacts.

America follows at 27%, led by the USA, where research is focused on theoretical developments, policy proposals, and quantum-safe migrations, reflecting a solid foundation. Africa stands at 13%, reflecting increasing interest in quantum technologies. Europe and Australia each contributed 7% towards overall publications, suggesting that research activity in these regions, while present, is less concentrated compared to Asia and America. Combined, the findings identify Asia as a prominent hub of innovation and

contribution towards quantum cryptography, highlighting the global disparities in research ventures.

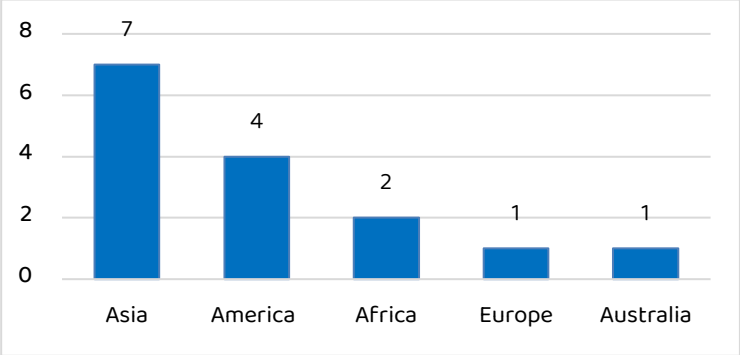

Figure 2. Comparison of studies by continent

3.2. Highlighted Innovations and their Frequencies

Figure 3 emphasizes the development of PQC algorithms (12 articles), QKD (6 articles), and a combination of these two approaches (hybrid systems) (6 articles) as the leading innovations in quantum computing cryptography.

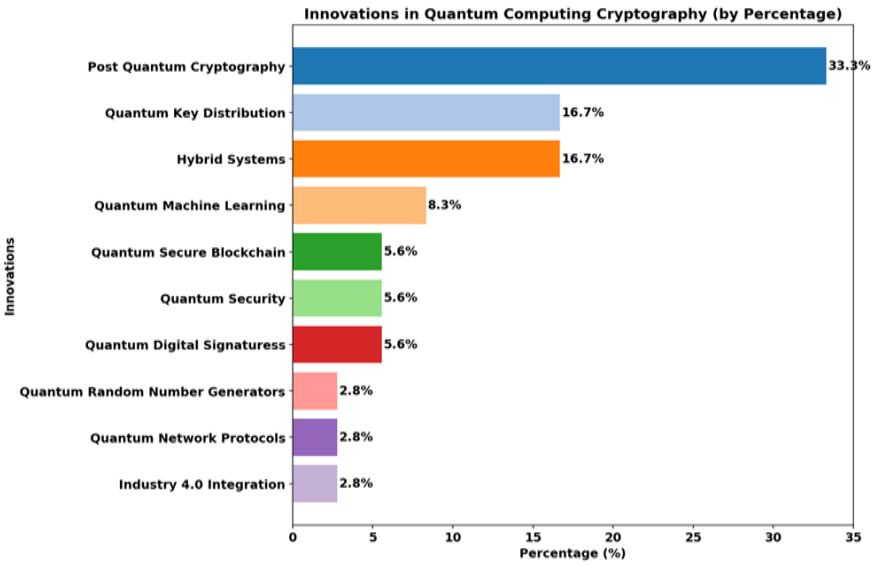

Figure 3. Innovations in Quantum Computing Cryptography

There is also a clear trend towards integrating these cryptographic solutions with other advanced technologies, such as AI and ML, in Quantum Machine Learning (QML) (3 articles) and Blockchain (2 articles). A multi-layered security framework integrating quantum security encryption with two components, Quantum Digital Signatures (QDS) (2 articles)

and Quantum Random Number Generators (QRNG), has been studied. The Quantum Network Protocol (QNP) integrates with Industry 4.0 technologies.

3.3. Highlighted Applications and their Frequencies

The primary areas of application for quantum computing cryptography, including finance (11 times) and healthcare (7 times), where strong data security and secure transaction systems are in high demand, as shown in Figure 4. Other significant areas are e-government, blockchain, telecommunications, and cybersecurity (6 each), wherein the shared demand is to secure data transmission and integrity. Defence (5 times) and the Internet of Things (IoT) (4 times) follow, reflecting the applicability of quantum cryptographic techniques in protecting critical military data and networked devices.

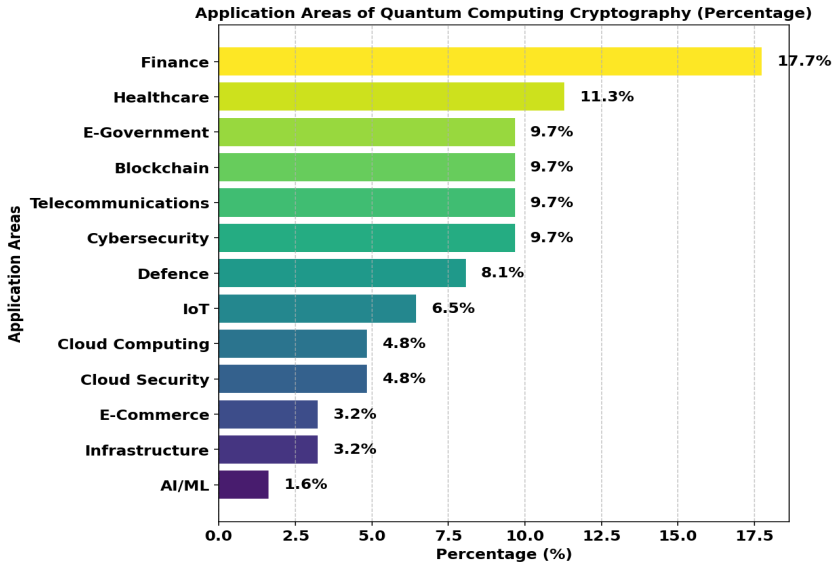

Figure 4. Distribution of Major Application Sectors

Cloud computing and security (three times each) reflect an embryonic interest in protecting distributed computing environments, while e-commerce and infrastructure (two times each) reflect initial experimentation with quantum-secure architectures for electronic commerce and critical infrastructures. Finally, Artificial Intelligence and Machine Learning (1 mention) is an evolving technology with expectations of embedding quantum cryptography in next-generation intelligent data-driven systems. Cumulatively, these findings present a wide and expanding breadth of applications across the real world, led by finance and healthcare as early adopters of quantum-secure technology.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

3.4. Highlighted Challenges and their Frequencies

The most significant issues of quantum computing cryptography, as shown in Figure 5. At the top of the list, a count of 10 is attributed to transition complexity, which can be viewed as a huge task of transitioning computer systems from classical to quantum-proof in terms of infrastructure and technical incompatibilities. Standardization (9 counts) and integration issues (8 counts) follow, highlighting the current lack of comprehensive frameworks and the challenge of integrating quantum cryptographic solutions with existing digital infrastructures. Scalability, security, and cost (each of which is a factor of 5) confirm once more that, even if quantum technologies are very attractive, their worldwide application is restricted by both economic and technical aspects. Additionally, the barriers consist of technological and implementation obstacles (four times), performance trade-offs (three times), and fears regarding attacks on classical encryption (two times). These barriers are less common but still significant, including continuous technological progress, slow user acceptance, quantum coherence issues, high error rates, and policy loopholes, which indicate that the situation is still evolving. Overall, the research reaches a similar conclusion: quantum cryptography may eventually revolutionize the field, but currently, it is hindered by significant technical, economic, and regulatory challenges.

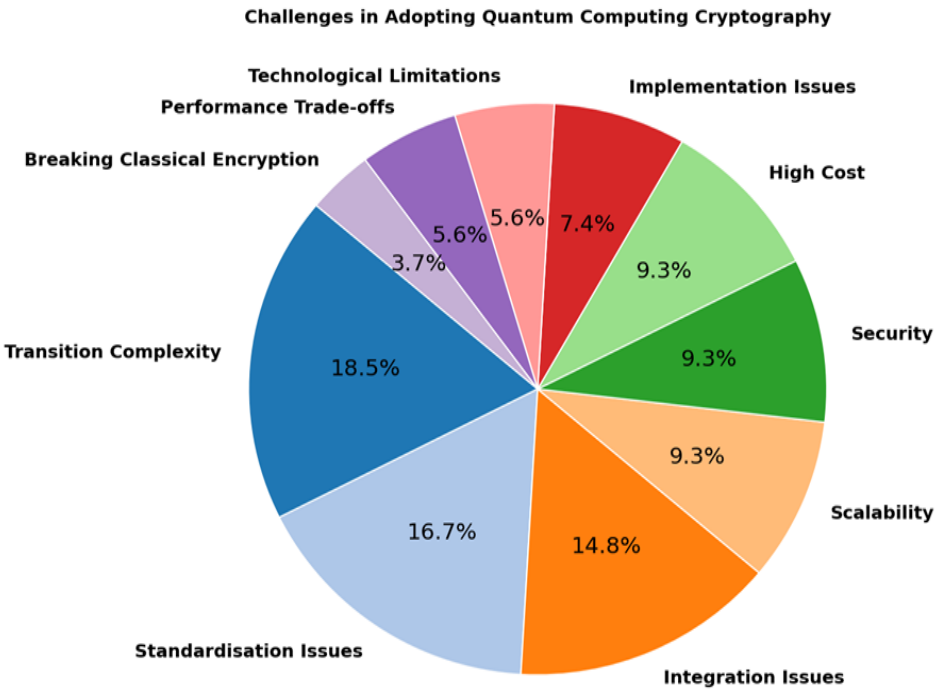

Figure 5. Breakdown of major Challenge Areas

Table 3. Summary of Key Challenges in Quantum Cryptography

Challenge	Affected Areas	Example	Impact
Transition Complexity	Deployment, Operations	Metropolitan QKD network costs	High barrier to entry
Standardization Gaps	Policy, Development, Compliance	Multiple competing PQC algorithms	Slows adoption, risks interoperability
Store Now, Decrypt Later	Data Longevity, Privacy	Long-term health or financial records	Encourages proactive quantum readiness
Efficiency and Scalability	IoT, Mobile Devices	McEliece key sizes	Limits usability on constrained devices
Integration	Enterprise IT, Internet Infrastructure	TLS stack upgrades	Costly transitions
Skill Shortages	Workforce Development	Lack of trained quantum engineers	Delays in project deployment
Legal and Regulatory Uncertainty	Governance, International Standards	Absence of enforcement laws	Stalls' investment and implementation plans

3.5. Highlighted Algorithms Used in Quantum Computing Cryptography

The majority of studies on quantum cryptographic algorithms are directed towards the PQC area, particularly lattice-based cryptography, which has the highest number of citations, at 9, as shown in Figure 6. This is the most favorable option because it offers the highest level of quantum resistance and is also the most practical to implement. Among the QKD protocols, those related to Shor's and Grover's algorithms (8) are given special status, marking their origins in quantum communication security. Out of the various types of PQC, multivariate-based (7), code-based (6), and hash-based cryptography (5) are steadily gaining interest, with a focus on ongoing experimentation with different algorithmic families to make them quantum-resistant. Additionally, BB84

and hybrid cryptography methods, which attempt to combine classical and quantum security mechanisms for greater durability, attract considerable attention. For example, newer algorithms such as the Quantum Approximate Optimization Algorithm (QAOA), Rawal Liang and Peter (RLP), TS-QKD, and isogeny-based cryptography (each with a count of 1) are paving the way for higher efficiency and adaptability in future quantum-safe systems. Thus, the research reveals an active deepening through traditional and new algorithmic paradigms for enhancing cryptographic security in the quantum era.

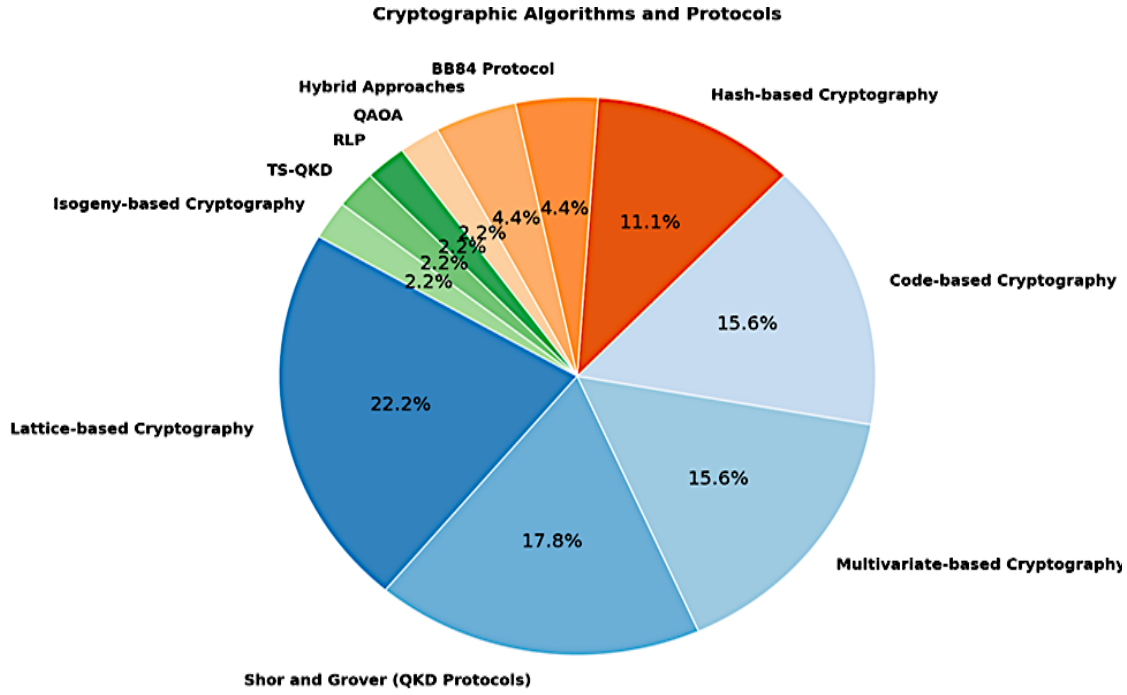

Figure 6. Highlighted Algorithms in Quantum Cryptography

This section presents a discussion addressing the research questions directly, utilizing the findings from this SLR to map the rapidly evolving field. Quantum technologies are advancing rapidly, and there's real pressure now to adopt quantum-safe cryptography, not someday, but immediately. Here, we synthesize the implications of these findings, outlining how they may inform theory, practice, and even policy.

3.6. Comparative Analysis of Cryptographic Approaches

Table 4 presents a comparative analysis of the major quantum cryptographic techniques. The methods are evaluated according to their readiness for practical application, and the support of specific industries by the existing infrastructure is clearly illustrated so that

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

one knows the current situation and what needs to be done. Such a comparison acknowledges lattice-based PQC as the most promising option for the NIST standardization process, the secure performance ratings, and the historical equipment cross-backing to the large-scale quantum-safe transition [28]. However, the diversity of algorithms needs to be hedged against future threats. Hence, continued funding in code-based, hash-based, and multivariate methodologies remains essential. QKD provides provable security for high-value applications, regardless of infrastructure costs and distance limitations. At the same time, hybrid systems are the standard for the highest security requirements, regardless of complexity and cost [25].

Table 4: Comparative Analysis of Quantum Cryptography Approaches

Approach	Security Basis	Deployment Readiness	Infrastructure Requirements	Performance Characteristics	Sector Suitability
Lattice-based PQC	Computational hardness (LWE, RLWE)	High (NIST standardized)	Compatible with existing systems	Moderate key sizes, efficient operations	Universal application
Code-based PQC	Decoding random linear codes	Medium (McEliece mature, large keys)	Compatible with existing systems	Large public keys, fast encryption	High-security applications
Hash-based PQC	Hash function security	High (SPHINCS+ standardized)	Compatible with existing systems	Large signatures, state variants	Long-term archival, firmware signing
Multivariate PQC	MQ problem hardness	Medium (some schemes broken)	Compatible with existing systems	Small signatures, vulnerable history	Constrained devices (with caution)
QKD (BB84, E91)	Quantum mechanics laws	Medium (limited deployments)	Requires quantum hardware, optical infrastructure	Distance limited (~100-400 km terrestrial), detector vulnerabilities	Government, Defence, and critical finance
Hybrid (PQC + QKD)	Layered security combining both	Low (experimental, few deployments)	Requires both quantum and classical infrastructure	Combines the benefits and complexities of both	Maximum security requirements

3.7. A Phased Pathway to Quantum Resilience

Obtaining quantum security is not a one-time action but a gradual and methodical process. The following flowchart shows an intelligent and phased approach for enterprises. The first step is to evaluate your current situation. Next, you enter a hybrid phase, and lastly, you fully integrate. This plan is not just a concept; it provides groups with a tangible and practice-oriented method to enhance their protections, thereby preparing them for current hazards and upcoming quantum trials.

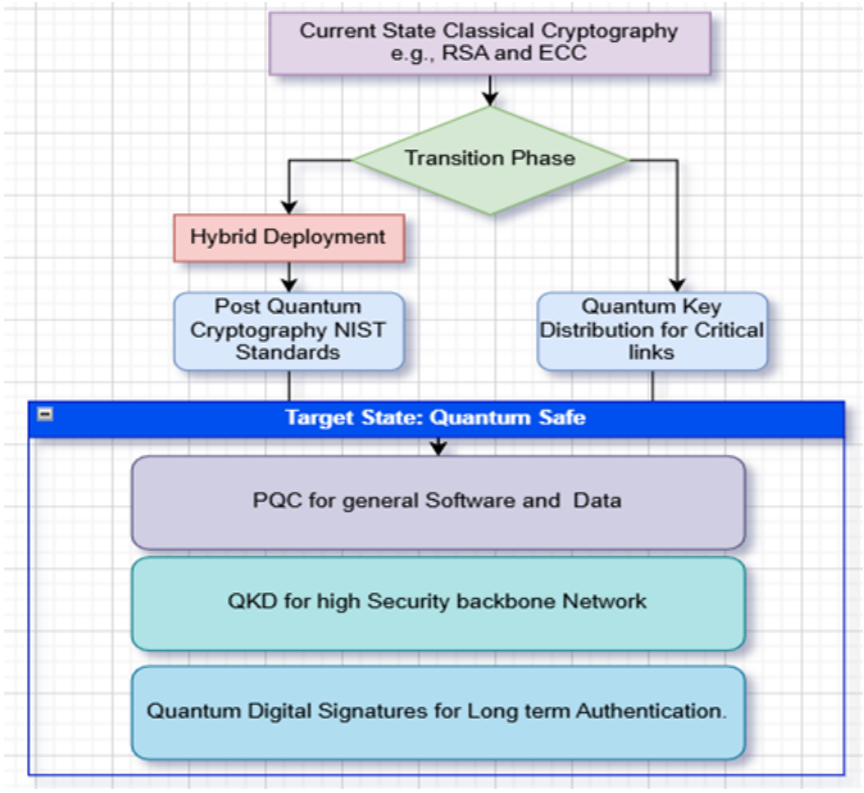

Figure 7. Transitioning from Classical to Quantum Resistant Systems

3.8. Innovations in quantum computing cryptography

Innovation in quantum computing cryptography incorporates the development of new cryptographic measures and methods that specifically aim at the weaknesses of traditional cryptography that have been broken by quantum computing. The ellipse of algorithmic remedies and methodological solutions covers the quantum-secure architecture and hybrid cryptographic systems. In other words, this is the place where the new era of cybersecurity starts, with cryptographic science and quantum mechanics joining forces to overcome the weaknesses of the quantum-enabled attacks. The

mentioned technologies, among others, such as post-quantum cryptography (PQC), quantum key distribution (QKD), hybrid systems, and quantum machine learning (QML), constitute a chain of interlinked defenses that will continue to protect the digital infrastructures even in the age of computational disruption [25].

3.8.1. Post-quantum cryptography

PQC refers to a set of quantum and classical computer-resistant cryptographic algorithms. PQC is less resource-intensive than QKD because it does not require hardware infrastructure. PQC can be directly injected into existing digital infrastructure. The most well-known PQC algorithm families, according to the literature reviewed, are:

1. Lattice-Based Cryptography**:** CRYSTALS-Kyber (for key agreement) and CRYSTALS-Dilithium (for signatures) stand out due to their performance and strong security proofs based on the Learning with Errors (LWE) problem [29]. Studies by [22] and [23] emphasize the compatibility between performance and security, making them suitable for a wide range of applications.
2. Code-Based Cryptography: The McEliece cryptosystem, which is based on the intractability of decoding random linear codes, has so far withstood cryptanalysis for decades. However, its large public key size is still a powerful deterrent to universal adoption [20].
3. Hash-Based & Multivariate-Based Cryptography: SPHINCS+, a hash-based signature, offers secure but conservative security owing to the properties of the hash function, but yields larger signatures [19]. Multivariate cryptography, promising as it has been for digital signatures, has been marred by setbacks, such as the cryptanalysis of the Rainbow scheme, necessitating periodic security evaluations.

3.8.2. Quantum key distribution

QKD opens the door to key exchange between parties that is theoretically unbreakable, leveraging the principles of quantum mechanics. Among others, BB84 and E91 are the most often employed protocols [10], [13]. The method is based on the idea that an eavesdropper can be detected because the quantum state has been disturbed. It finds applications in finance, e-government, healthcare, and military communications [13], [25], [24]. Nonetheless, despite its theoretical security advantages, QKD still has practical limitations such as high infrastructure costs, limited distances, and difficulties in scaling up, making it less attractive [13], [18].

3.8.3. Hybrid Cryptographic Systems

Lately, people are paying more attention to hybrid models that blend PQC with QKD [18], [26]. These models help us transition toward quantum-safe encryption without abandoning existing networks immediately. You can keep the old connections running while adding tougher quantum security on top. Take the Muckle++ protocol, for example. It uses FPGA-based modules and taps into quantum randomness, giving you both forward secrecy and post-compromise recovery features that matter when dealing with industrial automation or protecting critical infrastructure[25].

3.8.4. Quantum Secure Blockchain and Quantum Machine Learning

Quantum-safe blockchain is a type of technology that utilizes techniques of quantum-resistant cryptography to create blockchain networks that are resistant to future attacks on computers based on quantum processing [14]. In place of insecure cryptographic approaches like Elliptic Curve Digital Signature Algorithm (ECDSA), quantum-resistant ones are used along with QKD for secure key exchange [30]. These are the most appropriate options for managing public and private healthcare data and financial sectors [14]. The field of application is very broad, including finance through healthcare, IoT, and supply chains [13], [14], [21]. Existing and future platforms for blockchain technologies (Bitcoin, Ethereum, etc.) heavily rely on ECDSA and SHA-256, two of the most common blockchain cryptography algorithms. Cryptanalysis, aided by quantum computers, will render both of them vulnerable. Shor's Algorithm will overpower ECDSA by breaking the logarithms. Grover's Algorithm, on the other hand, will only reduce the strength of SHA-256 by half; that is, it will compromise its collision resistance and allow others to find the same hash for the messages. All this creates an outright need for the quantum-hardening of the blockchain infrastructures before the critical junctures of quantum hardware. Different proposals suggesting ways to secure distributed ledgers against quantum attacks include Post-Quantum Signature Schemes, Quantum-Safe Consensus Protocols, and modification of Proof-of-Work or Proof-of-Stake to the extent of including either PQC or QKD so that secure node-to-node communication is enabled. The deployment faces a few hurdles, such as resource-intensive, a lack of proper standards, and scalability issues. At the same time, QML offers cryptographic flexibility, including real-time anomaly detection and dynamic key management, enabling it to effectively cope with evolving cyber threats [6]. QML combines the concepts of quantum computing with machine learning algorithms to accelerate data-driven insights. [6], delves

into the alliance of AI and quantum cryptography, pointing out that AI approaches contribute to the efficiency and robustness of the cryptographic methods.

It leverages quantum properties, such as superposition and entanglement, to enhance classification, clustering, and pattern recognition tasks. When applied to cybersecurity, QML is a powerful tool for quantum-sensitive anomaly detection, intrusion detection systems (IDS) with quantum enhancement, and cryptographic key classification. Combined with AI, it facilitates dynamic threat modelling, cryptographic decision-making, and system optimisation in post-quantum environments. It is applied to anomaly detection and cyber threat litigation [14] and [13] for enhancing zero-day attack prediction, real-time intrusion detection, and adaptive security frameworks in quantum-resilient networks. These models beat traditional systems by identifying subtle patterns from enormous quantum-encrypted traffic. QML potentially reduces training time for complex models used in encrypted environments. Limitations of QML include hardware restrictions, i.e., quantum processors with sufficient qubits and low error rates exist on paper and in simulation, but are awaiting testing.

3.8.5. Industry 4.0

Industry 4.0 is characterized by integrating digital, physical, and biological systems using Industrial IoT, AI, ML, and collaborative robotics, Blockchain, and digital twins [21], [31]. Some revolutionary technologies include the Industrial Internet of Things (IIoT), which connects devices, sensors, and equipment on factory floors, enabling real-time data gathering for predictive maintenance and remote monitoring. An example is that smart sensors on the manufacturing floor can detect faults before they occur, thereby reducing downtime. AI and ML facilitate intelligent automation, quality inspection, and demand planning [32], [33]. An AI-powered visual inspection system reduces defects and enhances yield. Supply chain and energy consumption are optimized in real-time through ML algorithms. Cyber-Physical Systems integrate computation, networking, and physical processes, facilitating autonomous decision-making in robotics and intelligent machinery [34].

3.9. Emerging Enablers

Quantum digital signatures, quantum network protocols, and quantum random number generators are among the technologies that enhance the system's authenticity,

transmission security, and entropy generation [34]. These are the main features of Quantum Security Architectures (QSAs) that Industry 4.0 requires, where machines must communicate with high security and low latency [31]. These innovations are changing the trust in the digital world and pushing it towards environments resistant to quantum attacks. The effects of this shift are already evident in banking, healthcare, defense, and smart manufacturing, with data confidentiality and integrity being crucial for the success of these sectors. However, scalability, standardization, and hardware limitations still significantly impede the realization of the quantum security transition. Therefore, the future of quantum technologies should be grounded in theory, yet also highly practical, where the transition to quantum security is both affordable and equitable across all industries.

3.10. Application areas of Quantum Computing Cryptography

This section presents the application areas of Quantum Computing Cryptography.

3.10.1. Sector Specific Applications and Real-World Relevance

Cryptography based on Quantum Computing is gradually moving from the domain of speculation to that of practical usage, shielding the very basis of digital trust in essential areas. QCC makes sure that quantum-proof security is available against cyberattacks in the era of quantum computing, covering sectors like finance, healthcare, military, and e-governance. Nevertheless, high scalability, lack of standardization, and high cost are the main challenges. The ongoing pilot testing by IBM, Google, BT, and NATO, however, indicates a major breakthrough towards a quantum-safe digital future. Quantum-resilient encryption may sound like a theory but its application is entwined with the continued security of the most critical areas.

1) Finance

Applications of quantum computing cryptography are being employed within various high-risk sectors. The most widely mentioned use is Financial Services. [13], [14], [15] propose deploying a quantum-resistant Blockchain to protect financial transactions from quantum-based threats. A few more highlights include secure transactions with quantum-resistant encryption methods [16], [22]. Meanwhile, [26] summarizes the threat of "Store Now, Decrypt Later" attacks on financial data, and [13] addresses quantum-resistant blockchain in cryptocurrency. The protection of confidential conversations and

other critical infrastructures is among the top concerns of the Government and the Defense Sector. For instance, JPMorgan Chase and IBM have tested out quantum-safe Blockchain ledgers armed with Kyber-based encryption. Moreover, digital currencies like Bitcoin and Ethereum are trying out post-quantum digital signatures to further secure their ledgers against any possible changes. Online sales sites like Shopify and PayPal are also looking into PQC-shielded transactions and quantum-proof receipts [35].

2) Blockchain

Blockchain is a tamper-proof digital record that is transparent and cryptographically secure with consensus mechanisms [13], [14], [36]. Blockchain use cases are beyond cryptocurrency, including financial, supply chain, health care, and voting systems[37],[38],[39]. Blockchain is being re-designed with PQC and QKD to be quantum-resistant.

3) Cybersecurity

Cybersecurity protects computer systems from unauthorized access and sabotage, guaranteeing information confidentiality, integrity, and availability [18],[40]. Quantum-age protection mechanisms involve AI-based anomaly detection, Zero Trust Architecture, and PQC deployment. QML and AI-based threat prediction are utilized to defend against SNDL attacks [13], [26].

4) Telecommunications

Telecom networks embrace quantum technologies for safer operations, including implementing QKD on fibre-optic and satellite links [24]. Specific protocols like Time-Sensitive-QKD (TS-QKD) guarantee real-time data safeguarding in Industry 4.0 applications [21], while post-quantum TLS handshakes and T12 protocols secure internet sessions from quantum attacks [19], [25].

5) Healthcare

Healthcare infrastructure has profound vulnerabilities, ranging from sensitive patient data to the increasing digitization through telemedicine and IoT monitoring [19], [14], [41], [42]. Deployments of PQC through lattice-based and hash-based constructions protect Electronic Health Records (EHRs) in cloud infrastructure. QML models detect anomalies and insider attacks in healthcare data systems [13]. The sensitivity and confidentiality of

EHRs make healthcare an ideal application area. PQC is being tested to encrypt EHRs in cloud storage. At the same time, QKD is being planned to protect data links between hospitals and research labs [14]. Hospitals and research networks are deploying PQC and QKD to secure EHRs and genomic data. The Swiss Quantum Initiative successfully transmitted patient data using QKD between hospitals in Geneva. Quantum Random Number Generators are also being embedded in Internet of Medical Things (IoMT) devices to enhance encryption strength and prevent spoofing [19].

6) Internet of Things (IoT)

The Internet of Things involves ubiquitous connected systems leveraging sensors and actuators[43]. IoT is a massive cybersecurity problem with billions of resource-limited devices vulnerable to quantum attacks [20], [14], [21]. The solutions include lightweight PQC algorithms, such as NTRU and FrodoKEM, for device security, and QKD for edge-to-cloud communication in Industrial IoT networks. Applications are also seen in healthcare wearables, industrial sensors, and smart city infrastructure.

7) Cloud Computing

Cloud infrastructure is vulnerable to quantum attacks due to its centralized architecture and classical encryption vulnerabilities. Countermeasures include incorporating PQC into TLS 1.3 through Kyber-based exchanges, Post-Quantum VPNs, and QKD for interconnecting data centers [19]. Vendors are adopting cryptographic agility and a hybrid protocol for seamless migration [26].

3.11. Machine Learning and Artificial Intelligence

Artificial Intelligence refers to computer programs that simulate human intelligence to achieve functions such as reasoning, learning, and decision-making [44]. At the same time, Machine Learning, a subset of AI, enables systems to learn automatically and improve performance without explicit programming [45]. AI and ML have dual roles as vulnerabilities and defence mechanisms in quantum-resilient systems. Uses of QML include intrusion detection, encrypted traffic classification, and quantum cryptanalysis [13]. Cross-industry uses cover healthcare diagnostics, financial fraud detection, manufacturing automation, and telecommunications routing.

1) Infrastructure

Critical infrastructures face heightened quantum vulnerabilities due to digitization and long-term confidentiality requirements [3]. Industry 4.0 networks, smart grids, and SCADA systems are adopting PQC and QKD to safeguard PLCs and IIoT devices [21]. Uses under national security include Defence Industrial Base protection and satellite command systems with QKD and QDSs [24].

2) Security

Quantum attacks undermine data integrity and authentication in all sectors by breaching RSA, ECC, and AES through Shor's and Grover's algorithms [35]. PQC utilizes lattice and code-based challenges for classical infrastructure compatibility [27], [46]. Quantum-secure messaging, post-quantum cloud storage, and quantum-resistant blockchain networks are practical applications [13].

3) E-Commerce

E-commerce requires quantum-resistant security for authentication and payment [19]. Solutions are quantum-secure web protocols, PQC-based protection of smart contracts, and QKD-enabled high-value transactions [35], [13] [20]. Industry trends focus on cryptographic agility in TLS protocols and digital receipts that are quantum-proof [26]. E-commerce platforms like Shopify and PayPal are experimenting with PQC-protected transactions and quantum-secure receipts [35].

4) E-Government

E-government platforms manage sensitive national data vulnerable to quantum-improved cyberattacks and SNDL attacks [3]. PQC applications based on Dilithium and SPHINCS+ schemes secure national IDs, e-passports, and digital certificates, instead of insecure RSA and ECC authentication mechanisms [20], [46], [19], [24].

5) Defense

National defense organizations are at the forefront of adoption. NATO and member states invest in PQC for command-and-control infrastructure and QKD for the security of satellite and diplomatic communications, viewing quantum resilience as a strategic autonomy issue [24], [17]. National defence systems use QKD and PQC to secure military communications and logistics. NATO's Quantum-Resilient Communication Programme

and the USA DoD's PQC pilot projects embed NIST-approved algorithms into C4ISR systems. Toshiba's QKD satellites are employed in space defense for secure command and control links. Governments are piloting quantum-secure ID systems and QKD-protected election data transmission. Estonia and South Korea are leading the deployment of quantum-safe digital governance frameworks.

Table 5. Summary of Applications in Quantum Computing Cryptography

Sector	Applications	Core Quantum Technologies	Benefits	Challenges
Finance	Secure transactions, quantum-safe blockchain	PQC, QKD	Prevents SNDL attacks, enhances trust	High implementation costs
Blockchain	Decentralized tamper-proof ledgers	PQC, QKD, Lattice Signatures	Transparency, security	Interoperability issues
Cybersecurity	Threat detection, PQC firewalls	PQC, QML, QKD	Predictive Defence	Expensive, hardware limits
Telecom	Secure 5G & satellite links	QKD, PQC TLS	Secure national communications	Infrastructure upgrade cost
Healthcare	Protects EHRs, IoMT	PQC, QKD, QRNG	Data integrity & privacy	Ethical & cost issues
IoT	Secure smart devices & IIoT	PQC (NTRU, FrodoKEM), QRNG	Lightweight quantum-safe security	Scalability & energy limits
Cloud Computing	Post-Quantum VPNs, Hybrid Clouds	PQC, QKD	Data-at-rest & in-transit protection	Migration complexity
AI/ML	Intrusion detection, cryptanalysis	QML, PQC	Adaptive Cyber Defence	Bias & hardware immaturity
Infrastructure	SCADA, grids, defence logistics	PQC, QKD	Critical system security	Legacy system constraints

Sector	Applications	Core Quantum Technologies	Benefits	Challenges
Security	General quantum-resistant protocols	PQC, QKD, QDS	Forward secrecy, resilience	Standardization
E-Commerce	Secure payments, quantum-proof receipts	PQC, QKD, QRNG	Customer data protection	Latency & cross-compatibility
E-Government	Quantum-safe ID & records	PQC, QKD, QDS, Blockchain	Trust, transparency	Cost & scalability
Defence	Battlefield & C4ISR systems	PQC, QKD, QDS	Military data security	Hardware & latency issues

3.12. Challenges of Quantum Computing Cryptography

Quantum-secure communications are both theoretically and practically challenged, as Figure 8 graphically illustrates. In the middle is the ultimate security based on quantum physics. This system ranges from a total lack of knowledge to complete knowledge, and depends on observability. Real challenges in concentric circles surround it: technical, infrastructural, economic, and policy. In a nutshell, QCC is based on Post-Quantum Cryptography and Quantum Key Distribution and is regarded as being impervious to quantum computer attacks. QKD can reveal tampering mainly through disturbance of the system's state; however, such systems are not dependable beyond laboratory settings [1], [47]. The gap between quantum theory and real-world reliability is the first and most important limitation. The qubit vulnerability, low error rates, and unripe hardware problem characterize the technological aspect. Reliable photon sources, detectors, and repeaters are continually improving. At the same time, PQC algorithms typically require disproportionately high computational resources, which limits their use in smaller systems [47], [27]. Hence, these traps pose a significant engineering challenge to scalability and stability in QCC. A major infrastructure issue working outward is incorporating quantum-resistant technology into the current digital architecture. To accommodate quantum-secure encryption, current protocols, such as SSL and TLS, will need to undergo a complete revamp [3].

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

On top of that, the quantum signals lose quality as they travel, which in turn requires the use of expensive repeaters and the creation of hybrid networks [14]. This scenario makes the entire adoption process not only a technical challenge but also a financial one. The major drawbacks of using edge beams at the macro level are related to insufficient funding, the unavailability of skilled labor, and poor global coordination. The quantum hardware is still very costly, and there is a lack of quantum staff, so the progress is slow [15]. Moreover, the existence of different global standards worsens the situation by creating non-interoperability and unreliability problems [13]. This model illustrates the layered dependency between hardware readiness, cost, regulatory maturity, and engineering feasibility, showing why practical quantum security cannot advance without coordinated progress across these layers.

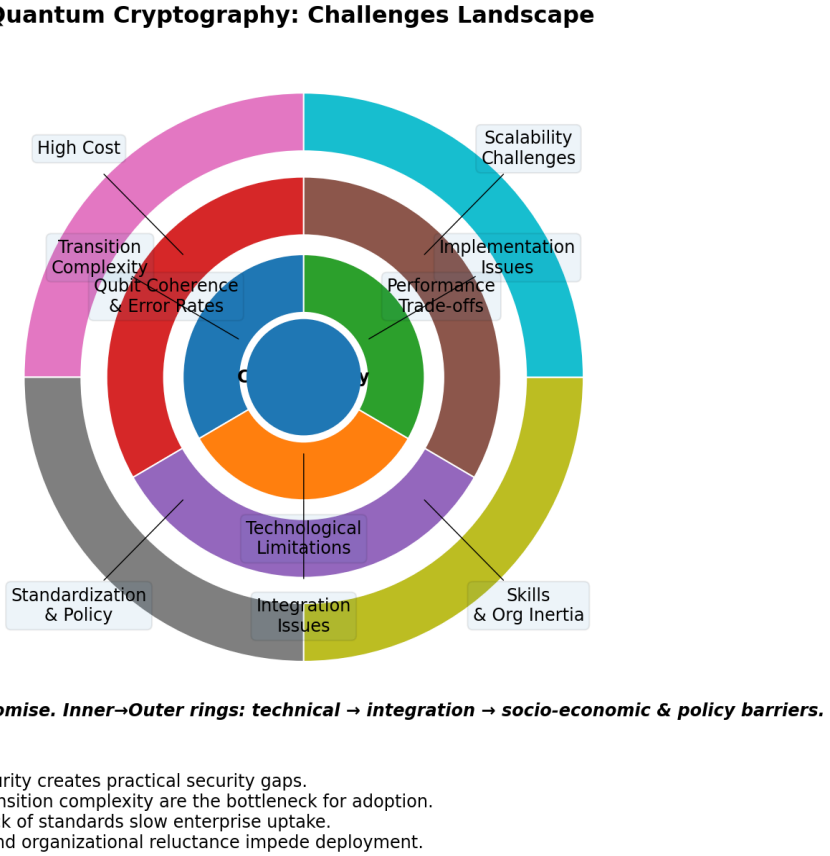

Figure 8. Quantum Computing Challenges Landscape

In general, the infographic clearly illustrates the interrelations among these problems: high-tech restrictions increase expenses, high expenses discourage investments, and weaknesses in regulations hinder progress. A comprehensive approach based on tech

innovation, infrastructure, human resource development, and international standards is required to solve them. Quantum Computing Cryptography could be transformative, yet it is hindered by existing systems. Surmounting the barriers between theory and practice relies not just on scientific progress but also on unified global initiatives to make quantum security attainable and fair.

1) Algorithms and Their Cryptographic Role

Quantum computing has effectively reshaped cryptographic discourse by implementing algorithms that can potentially compromise classical systems while pushing new paradigms in cryptography. The algorithms, ranging from quantum to post-quantum and hybrid schemes, collectively represent a landscape of threat space and response mechanisms for digital security moving forward.

2) Quantum Threat Algorithms: Shor and Grover

Shor's and Grover's algorithms are at the center of the quantum threat. The former, Shor's algorithm [2], is the only one that guarantees the notorious polynomial-time factorization of large numbers and discrete logarithms, which is a direct threat to RSA, DSA, and ECC, among others [13], [18]. It obliges the implementation of PQC by practically eradicating the current asymmetric systems from the circuit. Conversely, Grover's Algorithm [48], enables unstructured searches with a quadratic acceleration, effectively reducing the key size of symmetric ciphers such as AES-128 to AES-64 [23]. The solution is simple: the key size has to be doubled, but it may also have far-reaching impacts on cryptography and password security [19]. In this light, Shor's Algorithm compromises the security against the use of asymmetric encryption methods, while Grover's reduces the reliance on symmetric methods. However, their combined effect is to draw a line between the two worlds, i.e., the classical and the post-quantum. This line is the primary reason why research on PQC is conducted.

3) Post-Quantum Algorithms: Building Quantum-Resistant Systems

Rystals, Kyber, and Dilithium are leading PQC schemes in the standardization process at NIST [27], and lattice-based cryptography [49] is particularly well-known for its balance between implementability and security. Code-based cryptography based on McEliece is quantum-resistant in the long term. However, it has significant implications from a deployment perspective [23]. Multivariate-based solutions are efficient digital signatures

for resource-constrained setups. However, they are prone to vulnerabilities, as witnessed in the recent break of the Rainbow algorithm [50].

Hash-based cryptography, specifically SPHINCS+, is among the most conservative and stable post-quantum signature approaches, but has larger key and signature sizes [27], [15]. Isogeny-based SIDH/SIKE schemes had promised small keys. However, they were struck by crippling cryptanalytic breaks [51], which illustrates the volatility of PQC research. Lattice- and hash-based schemes continue to show the highest readiness for deployment.

4) Hybrid and Quantum-Enhanced Models

The BB84 protocol [52] and its derivatives, like the Time-Sensitive QKD (TS-QKD), are the leading solutions for hardware-based quantum communication security. The RLP cryptosystem, a combination of QKD and PQC, is an example of how these technologies can be applied together in critical areas, such as IIoT. Likewise, the Muckle++ Protocol [25] integrates Kyber, AES-Poly1305, and PUFs to provide crypto-agility against the "Store Now, Decrypt Later" (SNDL) threat. Hybrid solutions bridge the divide between quantum theory and applied cybersecurity, providing interim architectures while full quantum networks are still in development.

Table 5: Comparative Evaluation of Algorithms

Algorithm Category	Representative Algorithms	Primary Role	Strengths	Weaknesses
Quantum Threat	Shor, Grover	Break classical cryptosystems	Theoretical proof of quantum superiority	Destructive to current cryptography
Lattice-Based PQC	CRYSTALS-Kyber, Dilithium	Encryption & Signature	High security, NIST standard	Implementation complexity
Code-Based PQC	McEliece	Encryption	Proven resistance	Huge key sizes
Multivariate-Based PQC	Rainbow, Unbalanced Oil-Vinegar	Signatures	Lightweight	Vulnerable to new attacks

Algorithm Category	Representative Algorithms	Primary Role	Strengths	Weaknesses
Hash-Based PQC	SPHINCS+	Signatures	Minimal assumptions, secure	Large signature sizes
Isogeny-Based PQC	SIDH, SIKE	Encryption	Small keys	Recently broken
Hybrid Models	RLP, Muckle++	Integrated systems	Backward compatible, quantum-secure	Integration cost, standardization gaps

3.13. Real-World Deployments and Case Studies from Theory to Practice

Quantum cryptography's theoretical potential is now being claimed in pilot tests and field operations. These field deployments demonstrate feasibility and provide crucial insights into integration problems and performance.

1) National and Government Infrastructure

The Chinese Micius satellite has already conducted intercontinental QKD, encrypting video conferences between Vienna and Beijing. The pioneering project shows that space-based global quantum networks are feasible [53]. Ground-based QKD links are being deployed by the UK's Quantum Network (UKQN) and the European Quantum Communication Infrastructure (EuroQCI) program to secure government and strategic national infrastructure communications. EuroQCI will serve all EU member states by 2027.

2) Financial Sector Pilots

JPMorgan Chase and Toshiba have experimented with QKD to protect trading data between their data centers in Singapore. The pilot addresses the urgent "Store Now, Decrypt Later" threat for financial institutions, demonstrating a quantum-safe backbone for high-value transactions.

3) NATO's Quantum Defence Posture

The alliance recognized quantum technologies as a strategic priority for defense. It initiated various trials involving QKD in its communication networks to protect sensitive

information and command-and-control systems against future quantum decryption, constituting a new military doctrine for cybersecurity.

4) Integration with Telecom and Cloud

Leading cloud providers like Amazon Web Services (AWS) and Microsoft Azure offer hybrid key exchange in their VPN services, combining legacy and NIST-selected PQC algorithms (e.g., Kyber). Telecom leaders BT and Telefónica are testing the integration of QKD-over-fibre into their operational networks to offer "Quantum-Secure-as-a-Service" to business customers. These case studies confirm that quantum cryptography is transitioning from the lab to operational technology, albeit in specialized, high-security uses.

The Policy and Standardization Imperative: Creating a Global Quantum-Safe Framework

Policy, legal, and standardization issues are deeply intertwined with the technical problems of quantum cryptography. A global framework is necessary for adoption at a global level.

3.14. The NIST Standardization Process

The single most significant international effort to date is the NIST PQC standardization effort. Its selection of CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures provides us with a baseline list of adopted algorithms [29]. However, the process does locate a structural issue, the risk of becoming stuck with a limited number of algorithms, which would be a structural flaw if it were ever compromised.

1) Regulatory and Compliance Environments

Regulations are being rolled out by governments all over the world that mandate the transition to a new technology or system. The U. S. has enacted the Quantum Computing Cybersecurity Preparedness Act that mandates the entire federal government to switch to PQC. The European Commission's EuroQCI project, on the other hand, is a combination of technical adoption and policymaking. The lack of global regulatory harmonization is the most critical gap that could result in multinational companies facing trade barriers and compliance issues.

2) Addressing Sovereignty and Legal Challenges

The physical basis of QKD, which necessarily involves either direct fiber links or satellite connections, is to some extent the cause of raising data sovereignty and legal intercept questions. What about the scenario in which a quantum key is transferred through satellite and the cross-border data transfer rules have to be imposed? The answer will require the formation of new paradigms for the quantum age through the concerted efforts of international collaboration involving not only technologists, but also policymakers and lawyers.

3) The Way Forward

To meet these challenges, governments and standards bodies must:

a) *Advocate Crypto-Agility:* Policy must insist not just on the specification of actual algorithms, but also on being prepared to move between them with ease.

b) *Guarantee Interoperability Testing:* Finance trials that test interoperability between different vendors' QKD and PQC implementations.

c) *Form International Consortia:* Promote multi-stakeholder bodies, such as the International Telecommunication Union (ITU), to create global quantum security standards and prevent a fragmented technology ecosystem.

3.15. The Quantum Cryptography Ecosystem and Research Pathways Model

The research presented here provides a comprehensive ecosystem view that shapes the technological, sectoral, and algorithmic dimensions of quantum cryptography into a systematic conceptual model shown in Figure 9. The model encompasses five pillars of innovation: Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), combined PQC–QKD solutions, quantum-secure blockchain, and Quantum Machine Learning (QML) as rising grounds influencing the future of quantum-safe infrastructures.

The mentioned technologies serve as a liaison for cross-sector applications that include finance, Internet of Things (IoT), healthcare, e-government services, telecommunication, and cybersecurity. The major advancements in this study are the demonstration of interplay of technological convergence, domain-specific deployments, and algorithmic advances which together dictate the trajectory of real-world quantum security development, unlike previous reviews that considered quantum techniques separately or only compared algorithmic families.

Figure 9: Quantum Cryptography Unified Technological Convergence Ecosystem

The model also shows that the convergence is impacted by the barriers in the ecosystem, such as the gaps in standardization, the limitations in scalability, the high cost of implementation, the complexity of integration, the inadequacy of technical skills, and the threat of Store-Now-Decrypt-Later (SNDL). These barriers are associated with algorithmic conditions, mainly the exposure of weaknesses due to Shor's and Grover's algorithms and the consequent development of cryptographic primitives based on lattices, multivariate, codes, and hash functions. By interlinking technological innovation, deployment barriers,

and algorithmic foundations, the model provides a systematic rationale for the emergence of hybrid PQC-QKD security, QML-driven threat prediction, and crypto-agility as the priority directions for installations that are both scalable and future-proof.

3.16. Comparison with Prior Systematic Literature Reviews

Several recent systematic reviews (e.g., Exploring Post Quantum Cryptography: Review and Directions for the Transition Process 2024 [53]; Post Quantum Distributed Ledger Technology: A Systematic Review 2023 [54]; Quantum Computing and Cybersecurity: A Rigorous Systematic Review of Emerging Threats, Post Quantum Solutions, and Research Directions 2025) [55] are giving us valuable information but at the same time they differ from the current study in major aspects. To illustrate, [54] is mainly focused on post-quantum cryptography (PQC) algorithms and transition strategies. In contrast, the sectors and deployment challenges are hardly mentioned. [55] talks about PQDLTs in the context of blockchain but ignores the issue of cross-sector adoption and the synthesis of an algorithmic barrier. [56] give a broad overview of the situation, including emerging threats and post-quantum solutions; however, their attention is on threat classification and solution cataloguing rather than on creating an integrated ecosystem framework that connects innovation, applications, barriers, and algorithm foundations. This review, however, provides a convergent ecosystem model that integrates and synthesizes PQC, QKD, blockchain, and QML, assesses sector-specific adoption, charts algorithmic families, identifies system barriers, and outlines future pathways (RQ5). The use of this integrated method enhances novelty by transitioning from separate technique evaluations to a view of the whole ecosystem and deployment readiness.

3.17. Novelty of the Contribution

By means of a consolidated sectoral and algorithmic synthesis this study provides an extension to the already existing quantum-cryptography reviews. The global move towards NIST-approved schemes is the reason for the dominance of lattice-based cryptography. The strong representation of Asia, however, indicates the quickening of quantum-safe infrastructure investments. Our findings reveal a wider convergence of hybrid cryptography, industry-specific deployments, and the advent of QML-enhanced security, as compared to the previous SLRs that strictly focus on PQC. Integration problems, lack of standards, and the dangers associated with “Store-Now-Decrypt-Later” continue to pose significant challenges.

a) Thus, this work is among the first SLRs to present quantum cryptography as an ecosystem of convergence rather than a set of isolated security mechanisms. It contrasts with prior literature by:
b) Unifying innovation, application, barriers, and algorithms into one ecosystem logic, rather than treating them as separate research strands
c) Framing real-world adoption as a function of algorithmic evolution, not only industry needs or cryptographic performance
d) Positioning hybrid PQC-QKD and QML-driven automation as ecosystem necessities, rather than optional enhancements.

The conceptual model offers several actionable insights:

a) Policy makers must prioritise global standardisation and governance aligned with PQC–QKD interoperability.
b) Industry sectors should adopt hybrid quantum-safe architectures rather than rely on a single cryptographic solution.
c) Researchers must direct efforts towards optimisation for constrained IoT, edge and cloud environments.
d) System architects should embed AI/QML-based automation to support adaptive key management and threat intelligence.
e) Educators and training bodies need to address the critical skills gap hindering quantum adoption.

3.18. Future Research Directions and Recommendations

The results from the 15 studies included in this review indicate several future research directions necessary for the development of quantum-safe cryptographic systems. The first point is that there is a need to test hybrid PQC-QKD deployments in real-world, empirical settings; the current literature is mostly conceptual and does not provide performance benchmarks for operational settings. The second point is that the development of cross-sector optimization strategies, especially for IoT, IIoT, and cloud environments where resources are limited, has not advanced much, even though they are very important for the large-scale adoption of quantum-safe cryptography. The third point is the establishment of interoperability and crypto-agility frameworks, which are deemed an urgent need, enabling effortless migration among diverse PQC families and minimizing long-term vendor lock-in risk. The fourth point is that more research is

needed on integrating AI and QML models to automate post-quantum threat detection, key management, and anomaly recognition, as the existing work is still at the experimental stage. The last point is that deeper research into policy, governance, and standardization is necessary to synchronize technical advancement with global regulatory expectations. All of these gaps in understanding suggest a collaborative, interdisciplinary research agenda that would not only advance the technical foundations but also the policy foundations of quantum-safe infrastructure.

4. CONCLUSION

Quantum Computing Cryptography is among the main contestants in the technological revolution that will probably decide the future of digital security. A systematic literature review offers an exhaustive synthesis of the current state of innovations, areas of discussion, problems, and algorithms in the field. The two different approaches of QKD and PQC are both hopeful. Nevertheless, they eventually result in the development of quantum-resistant crypto systems by different means. Thus, the hybrid solutions that combine the advantages of both paradigms are the ones to lead the transition. Cryptographic applications secured by quanta are slowly but surely entering the market across sectors such as finance, healthcare, and the Internet of Things. The main factors preventing the full use of this tech are the high price, the weaknesses of the current infrastructure, the lack of experts, and the ongoing uncertainty about legal matters. The quantum-breaking vs. quantum-resistant algorithm race shows the dependency on the ongoing research, crypto-agility, and interdisciplinary collaborations. The industry should shift from innovative breakthroughs in isolation to the deployment of complete, scalable, and legal architectures that ensure a secure future against the quantum threats. Education, standardization, and hybrid pilots with broader applications are vital measures. This SLR not only strengthens the knowledge base necessary for such activities but also lays down a strategic foundation for the future of quantum cryptography that covers research, development, and regulation.

Moreover, the review identifies and prioritizes several directions for future research in response to RQ5, including empirical hybrid PQC–QKD pilot deployments, sector-specific optimization for constrained IoT and cloud infrastructures, and the development of interoperability and crypto-agility frameworks that enable smooth migration across PQC

families. Besides that, advancing AI- and QML-enabled quantum threat detection and conducting deeper research on standardization and governance will be equally necessary for establishing a globally aligned, scalable, and resilient quantum-safe ecosystem.

ACKNOWLEDGMENT

We want to thank the publishers and organizations that maintain the scholarly databases (IEEE Xplore, ScienceDirect, SpringerLink, etc.), which were essential for this study. The peer reviewers have provided us with insightful critiques that have helped us refine our arguments, and we are truly grateful for that.

REFERENCES

[1] Durr-E-Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum Cryptography for Future Networks Security: A Systematic Review," *IEEE Access*, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3504815.

[2] P. W. Shor, T. B. Labs, M. Ave, and M. Hill, "Algorithms for Quantum Computation : Discrete Log and Factoring Extended Abstract 1 Introduction," *Proc. 35th Annu. Symp. Found. Comput. Sci.*, p. 124, 1994.

[3] M. Mosca, "Cybersecurity in a quantum world: will we be ready?," *Nist*, no. April, pp. 13–16, 2015, [Online]. Available: csrc.nist.gov/groups/ST/post-quantum…/session8-mosca-michele.pdf

[4] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: applications and future prospects," *Front. Phys.*, vol. 12, no. August, pp. 1–13, 2024, doi: 10.3389/fphy.2024.1456491.

[5] D. Boscovic, *A Survey on Quantum-safe Blockchain System*, vol. 1, no. 1. Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/nnnnnnn.

[6] P. Radanliev, "Artificial intelligence and quantum cryptography," *J. Anal. Sci. Technol.*, vol. 15, no. 1, 2024, doi: 10.1186/s40543-024-00416-6.

[7] Z. Z. Sun *et al.*, "Quantum Blockchain Relying on Quantum Secure Direct Communication Network," *IEEE Internet Things J.*, no. May, 2025, doi: 10.1109/JIOT.2025.3526443.

[8] T. M. Fernandez-Carames, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, 2020, doi: 10.1109/JIOT.2019.2958788.

[9] L. Gyongyosi and S. Imre, "A Survey on quantum computing technology," *Comput. Sci. Rev.*, vol. 31, pp. 51–71, 2019, doi: 10.1016/j.cosrev.2018.11.002.

[10] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, p. 1012, 2020, doi: 10.1364/aop.361502.

[11] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, and A. Erbad, *A Survey and Comparison of Post-Quantum and Quantum Blockchains*, vol. 26, no. 2. IEEE, 2024. doi: 10.1109/COMST.2023.3325761.

[12] David Moher, "PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) Checklist Title 1 Identify the report as a systematic review, meta-analysis, or both," pp. 4–6, 2009, [Online]. Available: www.prisma-statement.org

[13] C. Gilbert and M. A. Gilbert, "Investigating the Challenges and Solutions in Cybersecurity using Quantum Computing and Cryptography," no. December 2024.

[14] N. P. Yvr, D. Choudhury, M. Ambika, and S. Kannadhasan, "Quantum Computing Paradigms Implications for Cryptography and Data Security in Information Systems," vol. 05005, pp. 1–8, 2025.

[15] M. R. Masum, "Quantum Computing for Cryptography and Post-Quantum Security Training," no. January, pp. 2–5, 2025, doi: 10.13140/RG.2.2.27793.95842.

[16] A. Colwill and J. Scott, "Quantum Computing and Its Transformative Effects on Cryptography and Data Security," no. March, pp. 3–5, 2025.

[17] W. Poincaré and M. Hamilton, "Exploring the Potential of Quantum Computing in Cryptography," pp. 43–51, 2024.

[18] C. Easttom, "Quantum Computing and Cryptography," *Mod. Cryptogr.*, no. March, pp. 397–407, 2022, doi: 10.1007/978-3-031-12304-7_19.

[19] D. Kumari, A. Namburi, K. Tanuj, R. Rangu, N. K. Muniswamy Naidu, and M. Mahmoud, "Quantum Computing in Cryptography," *Proc. - 2023 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2023*, pp. 490–495, 2023, doi: 10.1109/CSCI62032.2023.00086.

[20] A. Rayhan, "The Quantum Computing Revolution : Challenges and Opportunities," no. May, 2024, doi: 10.13140/RG.2.2.12467.85283.

[21] B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," *Cyber Secur. Appl.*, vol. 1, no. February, 2023, doi: 10.1016/j.csa.2023.100019.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[22] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel, and Atul, "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research," 2022.

[23] B. Long, "Classical Solutions for Quantum Challenges: An Introduction to Postquantum Cryptography," *ACM SIGCAS Comput. Soc.*, vol. 52, no. 2, pp. 23–25, 2023, doi: 10.1145/3656021.3656030.

[24] V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Comput. Commun.*, vol. 176, no. February, pp. 99–118, 2021, doi: 10.1016/j.comcom.2021.05.019.

[25] L. Garms *et al.*, "Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem," *Adv. Quantum Technol.*, vol. 7, no. 4, pp. 1–8, 2024, doi: 10.1002/qute.202300304.

[26] D. Joseph *et al.*, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022, doi: 10.1038/s41586-022-04623-2.

[27] D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham, and T. T. Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, pp. 1–18, 2023, doi: 10.3390/cryptography7030040.

[28] G. Alagic, C. Bai, J. Katz, and C. Majenz, "Post-Quantum Security of the Even-Mansour Cipher," in *Advances in Cryptology -- EUROCRYPT 2022*, O. Dunkelman and S. Dziembowski, Eds., Cham: Springer International Publishing, 2022, pp. 458–487.

[29] E. Alkim, P. S. L. M. Barreto, N. Bindel, J. Krämer, P. Longa, and J. E. Ricardini, "The Lattice-Based Digital Signature Scheme qTESLA," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12146 LNCS, pp. 441–460, 2020, doi: 10.1007/978-3-030-57808-4_22.

[30] P. Thanalakshmi, A. Rishikhesh, J. Marion Marceline, G. P. Joshi, and W. Cho, "A Quantum-Resistant Blockchain System: A Comparative Analysis," *Mathematics*, vol. 11, no. 18, pp. 1–19, 2023, doi: 10.3390/math11183947.

[31] J. Oosthuizen and B. C. Campus, "Expanding Schwab ' s Four-type Intelligence Proposition to Meaningfully Address the Challenges of the Fourth Industrial Revolution '," no. September 2016, 2024.

[32] V. R. Krishna, R. K. Jalli, and K. N. V. P. S. B. Ramesh, "Quantum Computing : Implications for Artificial Intelligence and Machine Quantum Computing : Implications for Artificial Intelligence and Machine Learning," no. March, 2025.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[33] A. Lohia, "Quantum Artificial Intelligence: Enhancing Machine Learning with Quantum Computing," *J. Quantum Sci. Technol.*, vol. 1, no. 2, pp. 6–11, 2024, doi: 10.36676/jqst.v1.i2.9.

[34] L. Monostori, "Cyber-physical production systems: Roots from manufacturing science and technology," *At-Automatisierungstechnik*, vol. 63, no. 10, pp. 766–776, 2015, doi: 10.1515/auto-2015-0066.

[35] Y. Ruan, H. Chen, J. Tan, and X. Li, "Quantum computation for large-scale image classification," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 4049–4069, 2016, doi: 10.1007/s11128-016-1391-z.

[36] V. A. Muderere, B. Ndlovu, and K. Maguraushe, "Blockchain Adoption in Healthcare : Enhancing Interoperability , Security and Data Exchange," *J. Inf. Syst. Informatics*, vol. 7, no. 3, pp. 2939–2977, 2025, doi: 10.51519/journalisi.v7i3.1267.

[37] R. Sibanda, B. Ndlovu, S. Dube, and K. Maguraushe, "Towards Health 4.0 : Blockchain-Based Electronic Health Record for Care Coordination," pp. 712–720, 2024, doi: 10.34190/ecie.19.1.2606.

[38] P. Jhamba, B. Ndlovu, S. Dube, M. Muduva, and F. Jacqueline, "A Blockchain-based Patient Portal for Mental Health Management," 2024, doi: 10.46254/AF05.20240251.

[39] H. B. Ncube, B. M. Ndlovu, S. Dube, and Maguraushe Kudakwashe, "Blockchain-Based Fraud Detection System for Healthcare Insurance Claims," no. 2023, pp. 540–547, 2024, doi: 10.34190/ecie.19.1.2558.

[40] B. Mutunhu, S. Dube, N. Ncube, and S. Sibanda, "Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology," *Proc. Int. Conf. Ind. Eng. Oper. Manag. Nsukka, Niger.*, pp. 5–7, 2022.

[41] B. Mutunhu, B. Chipangura, and S. Singh, "Towards a quantified-self technology conceptual framework for monitoring diabetes," *South African J. Sci. Technol.*, vol. 43, no. 1, pp. 69–84, 2024, doi: 10.36303/SATNT.2024.43.1.970.

[42] B. Mutunhu, B. Chipangura, and H. Twinomurinzi, "Internet of Things in the Monitoring of Diabetes," *Int. J. Heal. Syst. Transl. Med.*, vol. 2, no. 1, pp. 1–20, 2022, doi: 10.4018/ijhstm.300336.

[43] S. Chishakwe, N. Moyo, B. M. Ndlovu, and S. Dube, "Intrusion Detection System for IoT environments using Machine Learning Techniques," *2022 1st Zimbabwe Conf. Inf. Commun. Technol. ZCICT 2022*, pp. 1–7, 2022, doi: 10.1109/ZCICT55726.2022.10045992.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[44] B. Ndlovu and K. Maguraushe, "Balancing Ethics and Privacy in the Use of Artificial Intelligence in Institutions of Higher Learning: A Framework for Responsive AI Systems," *IJIE (Indonesian J. Informatics Educ.*, vol. 9, no. 1, p. 39, 2025, doi: 10.20961/ijie.v9i1.100723.

[45] S. Hadebe, B. Ndlovu, and K. Maguraushe, "Managing Diabetes Using Machine Learning and Digital Twins," *Indones. J. Innov. Appl. Sci.*, vol. 5, no. 2, pp. 145–162, 2025, doi: 10.47540/ijias.v5i2.1981.

[46] N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, and E. Persichetti, "Tighter Proofs of CCA Security in the Quantum Random Oracle Model," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11892 LNCS, pp. 61–90, 2019, doi: 10.1007/978-3-030-36033-7_3.

[47] S. J. Devitt, "Performing quantum computing experiments in the cloud," *Phys. Rev. A*, vol. 94, no. 3, pp. 1–29, 2016, doi: 10.1103/PhysRevA.94.032329.

[48] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proc. Annu. ACM Symp. Theory Comput.*, vol. Part F1294, pp. 212–219, 1996, doi: 10.1145/237814.237866.

[49] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016, doi: 10.1561/0400000074.

[50] W. Beullens, S. Dobson, S. Katsumata, Y. F. Lai, and F. Pintore, "Group signatures and more from isogenies and lattices: generic, simple, and efficient," *Des. Codes, Cryptogr.*, vol. 91, no. 6, pp. 2141–2200, 2023, doi: 10.1007/s10623-023-01192-x.

[51] W. Castryck, "An efficient key recovery attack on SIDH," no. 101020788, pp. 1–26, 2020.

[52] C. H. Bennett and G. Brassard, "Some of the Most Fundamental Principles," pp. 475–480, 1985.

[53] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, pp. 1–68, 2020, doi: 10.1103/REVMODPHYS.92.025002.

[54] Dekkaki, K. C., & Tasic, I. (2024). *Exploring Post-Quantum Cryptography : Review and Directions for the Transition Process*.

[55] Parida, N. K., Jatoth, C., Reddy, V. D., Hussain, M., & Faizi, J. (2023). Post - quantum distributed ledger technology : a systematic survey. *Scientific Reports*, 1–23. https://doi.org/10.1038/s41598-023-47331-1

[56] Barrett-danes, F., & Ahmad, F. (2025). *Quantum computing and cybersecurity : a rigorous systematic review of emerging threats , post-quantum solutions , and research directions (2019 – 2024). 5.*