DOI: https://doi.org/10.71317/kjard.2.6.2026.241

The Kashmir Journal of Academic Research and Development

Journal homepage: https://rjsaonline.org/index.php/KJARD

Quantum Computing and Post-Quantum Cryptography: Challenges, Opportunities, and Future Directions for Secure Digital Systems

Shaiq Ahmad Khan
FAST School of Computing, Department of Computer Science, National University of Computer and Emerging Sciences, Islamabad, Pakistan
Email: shaiqahmadkhan@gmail.com

Ahmad Sajjad
National University of Science and Technology, Pakistan
Email: asajjad@cae.nust.edu.pk

Wahab Ali
Bsc Hons Computer Science, Uni of Portsmouth, Faculty of Technology, UK
Email: Alsa7hr01@gmail.com

ARTICLE INFO

Received:
April 19, 2026
Revised:
May 02, 2026
Accepted:
May 17, 2026
Available Online:
June 01, 2026

Keywords:
Quantum computing, post-quantum cryptography, cybersecurity, digital governance, encryption systems, secure communication, qualitative technological research

Corresponding Author:
asajjad@cae.nust.edu.pk

ABSTRACT

The rapid development of quantum computing is one of the most transformative technological developments of the twenty-first century with profound implications for cybersecurity, digital governance and the future of secure communication systems. Traditional cryptographic infrastructures have fundamentally underpinned digital trust in banking, healthcare, defense, cloud computing, and global communication networks, but the advent of quantum computational power has led to increasing concern about the future of existing standards for encryption. This qualitative study critically examines the changing relationship between quantum computing and post-quantum cryptography through an analysis of the technological, institutional, ethical and governance challenges in the transition to quantum-secure digital systems. The study adopts an interpretivist and exploratory qualitative orientation that aims to understand how governments, cybersecurity experts, technology institutions and policy frameworks are responding to the disruptive potential of quantum technologies. Data were collected using thematic analysis of academic literature, cybersecurity policy documents, archival technological reviews, expert commentaries, institutional reports, and emerging case studies related to the development of quantum-resistant cryptography. The results show that quantum computing presents serious threats to existing public-key cryptographic systems, especially in terms of theoretical abilities of Shor's algorithm and future quantum decryption models. Meanwhile, the paper outlines post-quantum cryptography as a vital avenue for safeguarding digital privacy, institutional credibility, and cybersecurity robustness in an ever more networked society. The analysis also points to ongoing challenges around technological readiness, regulatory uncertainty, global standardization, resource inequality and ethical issues around surveillance, privacy and digital sovereignty. Yet, the research points to the potential for secure digital transformation, resilient cybersecurity governance, and the re-inventing of future communication infrastructure through post-quantum innovation. The research finds that the transition to quantum-secure systems is not just a technological challenge, but a multidimensional governance and policy challenge requiring international cooperation, ethical foresight and proactive institutional change.

Introduction

The modern digital world is built on cryptographic trust. Encryption technologies are essential for modern societies to protect information, uphold privacy and maintain digital trust across interconnected systems, from financial transactions and healthcare databases to military communication systems and cloud-based infrastructures. In the last few decades, classical cryptography systems like RSA, Diffie-Hellman, and elliptic curve cryptography have formed the backbone of cybersecurity architecture enabling secure communication in an ever more digitized economy and governance system. These cryptographic mechanisms rely on the assumption that some mathematical problems are intractable for classical computers to solve in a reasonable period of time. However, the advent of quantum computing has seriously shaken this assumption and posed one of the biggest technological challenges to modern cybersecurity systems.

Quantum computing is a revolutionary approach to computation that is fundamentally different from classical computing architectures. Instead of binary bits , quantum computers use quantum bits , also called qubits . Qubits are governed by the principles of superposition , entanglement , and quantum interference . These properties allow quantum systems to perform certain types of computation at a speed that is theoretically impossible to achieve with classical methods. Quantum computing, while promising for scientific discovery, pharmaceutical innovation, climate modeling and complex optimization problems, has also caused serious concerns about the future stability of existing cryptographic systems. The whole world of cybersecurity is suddenly feeling a sense of urgency as the quantum computing community comes to grips with the fact that a sufficiently powerful quantum computer could break the most common encryption standards.

The threat became especially clear after the theoretical formulation of Shor's algorithm, which showed that quantum computers can efficiently solve integer factorization and discrete logarithm problems on which a number of current public-key cryptographic systems are based. Large-scale fault-tolerant quantum computers that could carry out such attacks have yet to be developed, but the possibility of quantum-assisted decryption is already changing the way that governments, banks, hospitals, defense agencies and tech companies approach security at a strategic level. More and more experts are warning of a "harvest now, decrypt later" scenario where intercepted encrypted data today could be vulnerable once quantum computational power reaches sufficient maturity. Therefore, the question is no longer limited to theoretical physics or computer science laboratories. It has become a wider institutional, geopolitical, economic and societal issue with long-term implications for digital sovereignty and global cybersecurity governance.

In response to these emerging risks, post-quantum cryptography has grown in importance as a critical area of research and technological development. Post-quantum cryptography is the field of cryptographic algorithms that are constructed to be secure against both classical and quantum computers. Instead of quantum key distribution systems, which use quantum communication channels, post-quantum cryptographic systems aim to keep the security with mathematically resistant algorithms that can be implemented via existing digital infrastructures. Governments, international standardization bodies, cybersecurity agencies and tech companies are today working to find, test and standardize quantum-safe encryptions that can protect tomorrow's digital world.
While technical research in this area continues to expand, there remain considerable gaps in understanding the broader human, institutional and governance dimensions of the quantum-secure transformation. Existing scholarship has largely focused on computational efficiency, algorithmic performance, and mathematical security analysis, to the neglect of the sociotechnical realities of institutional readiness, regulatory adaptation, ethical concerns, and global cyber security inequality. The transition to post-quantum security is not simply a technological substitution; it raises complicated issues of trust, governance capacity, digital infrastructure resiliency, affordability, and geopolitical rivalry. Furthermore, developing and under-resourced countries may be disproportionately more vulnerable due to limited technological readiness, lack of investment in cybersecurity, and dependence on externally developed digital systems.

These concerns only become compounded as cloud computing, artificial intelligence, digital finance, smart infrastructure and interconnected communication networks converge. In particular, critical systems such as health care, military defense, banking, telecommunications, transportation, and governmental administration are becoming increasingly dependent on secure digital systems and the vulnerabilities of such systems may have wide social and economic impacts. An effective quantum-enabled attack on encryption systems could threaten national security infrastructure, public confidence in digital governance, expose sensitive health data, and destabilize financial markets. Hence the emergence of quantum computing is not just a revolution in technology but also a governance challenge that demands interdisciplinary understanding and strategic policy foresight. Therefore, this study aims to critically examine the relationship between quantum computing and post-quantum cryptography

from a qualitative and interpretative research perspective. Rather than focusing on technical algorithmic analysis, the research considers the cybersecurity experts' interpretations and reactions, institutional frameworks, technological policies and digital governance systems in response to the disruptive implications of quantum technologies. The objective of the study is to explore the emerging challenges of quantum threats, measure institutional readiness for post-quantum transition, examine ethical and governance issues, and discover opportunities for secure digital transformation in changing technological ecosystems. This study has four main research objectives. First, the study seeks to provide a critical analysis of the threat posed by quantum computing to modern cryptographic infrastructures and digital security systems. Second, it aims to discuss the institutional, technological, and governance issues of adopting post-quantum cryptography. Third, the study discusses ethical and policy implications of quantum-secure transformation in the global digital systems. And finally, the study seeks to identify future opportunities for innovation, cybersecurity resilience and secure digital governance in the emerging quantum era.

Some of the major research questions guiding the study include; How is quantum computing reshaping the current discourse on cybersecurity and cryptographic security frameworks? What are the challenges for institutions to move towards post-quantum cryptographic systems? How do ethics, governance and geopolitics affect quantum cybersecurity readiness? What opportunities exist to enhance digital resilience and secure communication infrastructures via post-quantum innovation?

The significance of this study is manifold, both in theory and practice. In principle, the research contributes to a growing interdisciplinary literature on the connections between quantum technologies, digital ethics, sociotechnical systems analysis, and cybersecurity governance. The study contributes to existing conversations by integrating technological transformation with qualitative interpretation, situating post-quantum cryptography within wider institutional and societal contexts, rather than focusing solely on computational perspectives. From a practical perspective, the study provides valuable insights for policymakers, cybersecurity professionals, governmental agencies, and digital infrastructure organizations interested in preparing for the long-term implications of quantum technological disruption.

Importantly, the study is oriented towards a qualitative understanding as the transition towards quantum-secure systems cannot be fully understood in terms of technical metrics alone. Institutional uncertainty, ethical dilemmas, policy adaptation, governance strategies and expert interpretations need more in-depth contextual analysis based on human-centered understanding. Qualitative inquiry allows for the investigation of emerging technological anxieties, strategic institutional responses, and evolving cybersecurity narratives that remain inadequately captured through quantitative technological assessment. In this sense, the study acknowledges that the future of quantum cybersecurity is not solely determined by computational capability, but also by human decision-making, institutional trust, global cooperation, and political responsibility.

As quantum technologies mature we are at a turning point in history when digital security is being turned upside down. The shift to post-quantum cryptography is thus more than a technical upgrade; it is a shift in the very paradigm of trust, privacy, governance, and resilience in a more complex digital world. Critical, interdisciplinary and qualitatively informed scholarship that is able to examine both technological innovation and the societal structures through which it operates is required to understand this transformation.

Literature Review

The rapid development of quantum computing has created one of the most important paradigm shifts in digital technology and cybersecurity history. For several decades, classical cryptographic infrastructures have been the foundation of secure digital communication, allowing modern societies to conduct financial transactions, protect state secrets, secure healthcare systems, and maintain digital trust across ever more interconnected global networks. But the appearance of quantum computational models has shaken the long-held beliefs about computational security and cryptographic resilience. As a result, the academic debate on quantum computing and post-quantum cryptography has grown exponentially in the domains of cybersecurity, information systems, computer science, digital governance and technology ethics. Despite significant technical advances, important conceptual, institutional, and human-centered questions remain underexplored in existing scholarship.
The early quantum computing literature concentrated on the theoretical underpinnings of quantum mechanics and computational feasibility. The idea of quantum computing originated with pioneer scholars such as Feynman and Deutsch, who envisioned a computational architecture that was radically different from classical binary systems and able to process information in ways that were not possible according to classical constraints. In contrast to classical computers that perform calculations based on the deterministic binary logic, the quantum systems use qubits, which work on the superposition and the entanglement, allowing the simultaneous processing of several states of the computational process. Initial scholarly enthusiasm focused heavily on scientific innovation, optimization potential, and computational efficiency. Yet, as quantum theory developed into practical

experimentation, researchers began to appreciate the deep ramifications of quantum computing for security and cryptographic systems.

The literature on classical cryptography shows that contemporary encryption frameworks are heavily dependent on mathematical complexity and computational infeasibility. Public-key systems such as RSA, Diffie–Hellman, and elliptic curve cryptography became dominant because classical computers require impractically long periods of time to solve the mathematical problems underlying these systems. Historically, scholars considered these cryptographic structures sufficiently secure for long-term digital communication and institutional data protection. But this confidence started to erode with the advent of Shor's algorithm, which transformed the cybersecurity conversation by showing that quantum computers could theoretically factor large integers and solve discrete logarithmic problems exponentially faster than classical systems.

Shor's algorithm has thus become central within contemporary debates about cryptographic vulnerability. The algorithm is described by many researchers as one of the most disruptive developments in the history of cybersecurity because it poses a direct threat to the security assumptions on which global digital infrastructures are built. Existing literature uniformly claims that quantum computers, if sufficiently advanced, could break the encrypted communication systems protecting banking networks, healthcare databases, military communication channels, and governmental infrastructures. Yet, there are differences of opinion among scholars on the immediacy and magnitude of this threat. Others contend that practical quantum attacks are technologically far off because of hardware limitations, decoherence challenges, and qubit instability. Others argue that a delayed institutional response could result in catastrophic future vulnerabilities especially for long-term sensitive data storage systems that are vulnerable to 'harvest now, decrypt later' strategies.

Parallel debates on Grover's algorithm further complicate the literature on quantum cybersecurity. In contrast to Shor's algorithm that directly endangers public-key encryption systems, Grover's algorithm undermines the security of symmetric cryptography by providing a quadratic speedup for brute-force search. While symmetric encryption can theoretically retain resilience by increasing the key length, there is debate among researchers about whether existing institutions have sufficient preparedness in place to undertake massive cryptographic adaptation before quantum systems mature. As a result, the literature is increasingly framing quantum computing not just as a technical innovation but as a strategic governance challenge, involving institutional readiness, regulatory coordination, and long-term cybersecurity planning.

With the emergence of such risks, post-quantum cryptography has become one of the fastest growing fields of research in cybersecurity. Existing scholarship defines post-quantum cryptography as a group of cryptographic algorithms designed to be secure against both classical and quantum attacks. In contrast to quantum cryptography, which depends on quantum communication infrastructure, post-quantum cryptographic systems seek to maintain security in existing digital networks using algorithms resistant to mathematical attacks. But the literature shows significant disagreement as to which cryptographic frameworks provide the most viable long-term solutions.

Lattice-based cryptography has emerged as one of the most widely supported approaches in current scholarship. Researchers claim that lattice-based systems are able to provide strong security foundations, while maintaining computational efficiency suitable for large-scale digital implementation. Theoretical models such as Learning With Errors (LWE) and Ring-LWE have received significant institutional attention because of their perceived security against quantum attacks. However, experts warn that confidence in lattice-based schemes, in the long term, still hinges on the development of mathematical assumptions that hold up to cryptanalytic scrutiny. In the same vein, hash based cryptography has also been lauded for its relative simplicity and proven security properties , especially in the realm of digital signature systems . However , questions about scalability and implementation flexibility persist .

Another large area of post-quantum research is code-based cryptography, especially using systems based on the McEliece cryptosystem. Current literature often credits code-based schemes for their decades of resilience to cryptanalysis. However, the researchers also cite practical limitations associated with large key sizes and infrastructure compatibility. Multivariate and isogeny-based cryptographic schemes have also attracted academic interest, but recent cryptanalytic advances have brought their long-term security into question. Thus the literature is characterized by a continuous state of technological uncertainty, where no widely accepted post-quantum solution has yet attained full institutional consensus.

Beyond technical analysis, an emerging body of recent scholarship considers governance and ethical implications of quantum cybersecurity transformation. Researchers say the move to quantum-secure systems raises important questions around digital sovereignty, geopolitical rivalry, technological inequality and institutional power concentration. Major global powers like the

United States, China, and members of the European Union are pouring resources into quantum research, sparking concerns about technology arms races and asymmetric cybersecurity capabilities. Digital governance scholars caution that unequal access to quantum technologies may reinforce global technological hierarchies and exacerbate existing inequalities in cyber security between technologically advanced and developing states.

The ethical issues of quantum computing have also drawn a growing academic attention. Existing literature raises concerns about the expansion of surveillance, the loss of privacy, and the control of infrastructures for encrypted communication by the state. Some scholars argue that quantum-powered decryption capabilities could pose a serious threat to privacy rights and democratic freedoms, if they are not accompanied by adequate governance safeguards. Others argue that quantum-secure cryptography could bolster the protection of digital rights by allowing the construction of more robust communication infrastructures that are resistant to unauthorized surveillance and cyber intrusion. These competing perspectives underscore the profoundly political and ethical character of quantum technological transformation.

Despite the rapid growth of the scholarship, existing research has important limitations. Much of the literature still emphasises technical performance metrics, algorithmic efficiency and computational modelling at the expense of institutional interpretation, human-centred adaptation and governance complexity. Most research landscapes today are quantitative and engineering in nature, and largely ignore how policy makers, cybersecurity professionals, and institutional actors conceptualize uncertainty, risk, and technological preparedness. In addition, there has been a lack of emphasis on understanding the disproportionate susceptibility of developing countries and resource-constrained institutions in the transition to post-quantum security infrastructures.

The literature also indicates methodological fragmentation across disciplines. In computer science research, cryptographic analysis is often abstracted from larger sociopolitical implications, while governance and policy scholarship is often insufficiently engaged with technological complexity. Thus, interdisciplinary integration is in its infancy. The role of institutional trust, cybersecurity governance cultures, regulatory frameworks and expert perceptions in shaping post-quantum transition strategies is seldom addressed in existing studies. Likewise, scant qualitative inquiry has explored the lived experiences, strategic anxieties, and decision-making processes of cybersecurity practitioners grappling with emerging quantum uncertainty. Thus, this study positions qualitative inquiry as essential to advancing contemporary understanding of quantum cybersecurity transformation. Purely technical approaches do not allow a more profound investigation of institutional preparedness, governance adaptation, ethical interpretation and technological uncertainty. Thematic analysis and interpretive inquiry of qualitative studies offer a window into how expert communities conceive security risks, negotiate cryptographic transition, and build future-oriented cybersecurity strategies in rapidly evolving digital environments.

Theoretically, this study draws on interdisciplinary insights from the literature on cybersecurity governance theory, sociotechnical systems theory, frameworks for technological adaptation, and digital ethics scholarship. Both viewpoints accept that technological systems are connected to institutional arrangements, political power relations and human interpretation. In this sense, post-quantum cryptography is not only a mathematical challenge but also a sociotechnical transformation, influenced by governance capacity, institutional trust, geopolitical competition, and ethical responsibility. This transformation requires analytical frameworks that can combine technological complexity with human-centered interpretation and policy-oriented critical analysis.

The qualitative evidence suggests that experts increasingly perceive these systems as structurally vulnerable to future quantum attacks, particularly once scalable quantum computers become operational. While current quantum systems remain technologically limited, institutional anxiety is driven by the recognition that encrypted data harvested today may become decryptable in the future through “harvest now, decrypt later” strategies.

Method of Research

The methodological approach of this study is based on a qualitative and interpretivist approach to critically analyze the emerging relationship between the quantum computing and post-quantum cryptography in modern cybersecurity systems. The methodological framework builds on the notion that technological transformations are not mere technical phenomena, but also institutional, ethical, political, and sociocultural processes that are shaped by human interpretation, governance structures, and strategic decision-making. Thus, the present work emphasizes depth of interpretation, contextualization and critical analysis rather than quantitative measurement or computational experimentation.

The research is based on the interpretivist philosophical paradigm, which focuses on the socially constructed nature of technological meaning and institutional response. From this perspective, cybersecurity systems, cryptographic transitions and digital governance regimes are not conceived as neutral technical architectures but as dynamic sociotechnical milieus, influenced by human perception, institutional purposes, political interests and ethical concerns. The most appropriate approach in this case is the interpretivist. This is because the study aims to understand how cybersecurity experts, policymakers, technological institutions, and governance systems perceive the disruptive implications of quantum computing and the transition toward post-quantum security infrastructures.

The present study is based on an exploratory qualitative research design. Since large-scale quantum disruption is still a nascent technological phenomenon, existing institutional responses and governance strategies are still rapidly evolving. The exploratory qualitative inquiry therefore allows for a flexible exploration of emerging cybersecurity anxieties, technological uncertainties, and processes of strategic adaptation that remain poorly understood in current scholarship. The study does not test pre-specified hypotheses but aims to provide critical interpretive insights into how institutions think about and respond to the future challenges of quantum-secure transformation.

The research is conducted from the methodological point of view in the thematic analytical framework with the elements of qualitative case-oriented analysis. This approach allows the study to consider recurring themes, institutional narratives, governance concerns and technological debates across different types of qualitative evidence. The analytical framework draws on interdisciplinary perspectives from cybersecurity governance theory, sociotechnical systems theory, digital ethics and technological adaptation scholarship. Together, these frameworks support the investigation of the relationship between technological systems and institutional power, policy and human-centered decisions.

The sampling strategy is based on the principles of purposive and criterion-based qualitative sampling. The data sources were intentionally chosen for their relevance to quantum computing, cybersecurity governance, cryptographic transition, and institutional readiness. The study does not seek statistical representativeness, but informational richness, analytical relevance and thematic depth. The chosen materials include cybersecurity policy frameworks, institutional white papers, government cybersecurity strategies, technology reports, international standardization documents, academic journal articles and expert commentaries from organizations that are actively involved in the development of quantum and post-quantum security.

The analysis particularly focuses on institutional sources related to international cybersecurity and technology governance, including international standardization organizations, governmental cybersecurity agencies, quantum research institutions, technology companies and academic cybersecurity centers. This selection strategy allows an analysis of the way different institutional actors frame the risks, opportunities, and governance implications related to quantum technological disruption. In addition, case-based examples of national cybersecurity strategies, cryptographic standardization efforts, and technological preparedness frameworks were provided to offer contextual depth and comparative interpretive insight.

Data collection was conducted through several qualitative methods that sought to enhance the analytical triangulation and the interpretive credibility. The main method was a thorough review of policy documents on cyber security transition frameworks, quantum readiness plans, cryptography standardization reports and institutional risk assessments. These documents were examined for dominant governance narratives, institutional concerns, strategic priorities, and emerging policy directions around post-quantum transformation.

The study examined the policies and also used expert-oriented secondary qualitative materials, including published interviews, institutional statements, cybersecurity conference discussions, technology white papers, and expert views from academic literature. These materials were analysed to examine the understanding of the institutional preparedness and technological uncertainty of new digital security contexts by practitioners and policymakers in cybersecurity and quantum research. Historical developments in the field of cybersecurity and the evolution of cryptography were also reviewed to place contemporary debates into a broader context of technological trajectories.

The study also qualitatively analyzed documents of academic literature on quantum computing, post-quantum cryptography, digital governance, technology ethics, and cybersecurity adaptation. This allowed the integration of interdisciplinary academic perspectives and the identification of conceptual themes shared by technical, political and institutional dimensions. Multiple sources of qualitative data were used to deepen the themes and improve the capacity for critical synthesis of technological and governance-oriented perspectives in the study.

Data was analysed thematically. The analysis was conducted in a series of linked stages. All collected materials were systematically reviewed to familiarise with the data and immerse concepts. Recurring themes of cybersecurity risk, cryptographic vulnerability, institutional readiness, ethical governance, technological uncertainty and digital resilience were identified at this stage. Open coding procedures were then used to sort key concepts, institutional narratives, and interpretive themes that emerged across the qualitative materials.

After coding, related concepts were grouped into larger thematic categories that represented major dimensions of the study. Quantum Threats to Public-Key Cryptography, Institutional Challenges, Governance Uncertainty, Quantum Surveillance Ethical Implications, Geopolitical Competition, Technological Readiness and Opportunities for Secure Digital Transformation were key themes. The themes were then critically interpreted using sociotechnical and governance-oriented theoretical frameworks to explore the interaction between technological innovation, institutional structures and political realities.

Reflexivity was an important part of the methodological process. The study acknowledged that qualitative interpretation is always a product of researcher perspective and whether the research is conducted in a critical way, ongoing critical reflection of analytical assumptions, theoretical alignment, and interpretive framing are engaged. Special attention was paid to avoid technological determinism and to provide balanced interpretation of optimistic and critical views on quantum transformation. Reflexive engagement further enabled analytic transparency and methodological integrity throughout the interpretive process.

The study also demonstrated trustworthiness and credibility through methodological triangulation, analytical consistency, and interpretive rigor . Using multiple sources of qualitative data provided cross-validation of emerging themes and reduced reliance on any single institution's perspective. Transferability and conceptual depth were enhanced by thick description and contextual interpretation. Systematic coding procedures and transparent analytical progression increased dependability, and reflexive documentation and evidence-based thematic interpretation increased confirmability.

Ethical issues were carefully considered throughout the research process. With a primary reliance on publicly available policy documents, academic literature, institutional reports and secondary expert materials, risks associated with participant confidentiality and direct human subject vulnerability were minimal. But the ethical responsibility was still there in terms of accurately representing institutional perspectives, responsibly interpreting technological debates, and avoiding selective analytical bias. Where cited were expert points of view and institutional pronouncements, interpretive fairness and contextual integrity were preserved.

The study provides some analytical insights but has some methodological limitations. This is a qualitative inquiry and does not seek statistical generalizability, nor predictive modeling of quantum technological timelines, or cryptographic implementation outcomes. Because quantum computing is a rapidly evolving field, institutional strategies and technological capabilities may also change significantly over time. Furthermore, the use of secondary qualitative materials may restrict direct access to classified institutional decisionmaking processes and upcoming classified cybersecurity strategies.

Nevertheless, qualitative inquiry is very appropriate in this domain as quantum cybersecurity transformation goes well beyond pure technical computation to larger issues of governance, ethics, institutional trust, strategic readiness, and sociotechnical adaptation. The subtleties of these dimensions cannot be fully captured by algorithmic performance analysis or quantitative modeling alone. This approach offers a more comprehensive analysis of how institutions and communities of experts are responding to the challenges, opportunities and uncertainties of the nascent quantum era, with its focus on interpretive understanding and critical thematic investigation.

Results and Discussion

Introduction to the Results

The results of this qualitative study suggest that quantum computing is increasingly viewed not only as an emergent computational innovation, but also as a disruptive force that can fundamentally reshape global cybersecurity architectures, institutional trust systems, and digital governance regimes. The increasing gap between the rapid pace of quantum technologies and the relatively slow pace of institutional migration to quantum-safe infrastructure is one of the most frequently cited challenges in the academic world, institutional reports, cybersecurity policy discussions, and expert commentary.

Thematic analysis revealed several related themes: rising exposure of classical encryption systems, institutional unpreparedness for quantum disruption, geopolitical rivalry for quantum supremacy, ethical concerns over surveillance and digital power

asymmetries, and the strategic necessity of post-quantum cryptographic migration. At the same time, the findings also uncovered opportunities for cybersecurity innovation, collaboration in international technology, and the building of resilient digital infrastructures that can support secure communication systems in the future.

The results demonstrate that the transition to post-quantum security is not merely a technical issue but a multi-dimensional governance challenge that entails political decision-making, institutional adaptation, economic investment, ethical regulation, and long-term digital resilience planning.

Theme Findings

Theme 1: Lack of Strength in Classical Encryption Systems

One of the most salient themes that emerge from this analysis is the increasing fragility of classical cryptographic infrastructures in the face of quantum computational progress. The existing digital infrastructure such as banking networks, military communications, health care databases, cloud infrastructure, e-governance, international financial transactions etc. still relies heavily on classical public-key cryptography, e.g., RSA and elliptic curve cryptography.

Table 1

Theme	Technological Challenge	Institutional Response	Qualitative Interpretation
Vulnerability of Classical Encryption	Quantum algorithms threaten RSA and ECC systems	Early-stage cryptographic transition planning	Institutions acknowledge risks but remain operationally dependent on vulnerable infrastructures
Data Longevity Risks	Sensitive data may be decrypted retrospectively	Limited archival protection strategies	Long-term confidentiality is increasingly uncertain
Critical Infrastructure Exposure	Financial and governmental systems rely on outdated encryption	Gradual modernization initiatives	Cybersecurity modernization remains reactive rather than preventive

The findings reveal an important contradiction in the current cybersecurity governance. Although awareness of quantum threats has increased significantly, the real-world application of post-quantum security is still sporadic and uneven. This result is consistent with prior research, arguing that the unwillingness of cybersecurity institutions to react proactively to disruptive technologies (e.g., blockchain-based currencies) is often a consequence of bureaucratic inertia, financial limitations, and technological uncertainty.

Qualitatively, the continued use of vulnerable encryption infrastructures is emblematic of a wider institutional disposition to favor short-term operational continuity at the expense of long-term strategic resilience. Therefore, the quantum threat in the future is not only technological but also institutional and governance related.

Theme 2: Institutional Unpreparedness for Quantum Disruption

Another major theme relates to institutional unpreparedness and uneven readiness among governments, corporations, and cybersecurity organizations. The results indicate that while many institutions are conceptually aware of quantum threats, they lack comprehensive migration frameworks, technical expertise, workforce preparedness, and strategic coordination mechanisms.

Evidence suggests that preparedness gaps are especially noticeable between technologically advanced states and developing digital economies. As well-funded nations increase investment in quantum research, cryptographic standardization, and cybersecurity modernization, resource-constrained agencies tend to remain dependent on legacy infrastructures with limited adaptive capacity.

Table 2

Institutional Sector	Observed Preparedness Level	Key Challenge	Qualitative Insight
Government Agencies	Moderate but fragmented	Policy coordination	Strategic awareness exceeds implementation capability
Financial Institutions	Relatively advanced	Migration cost and operational disruption	Economic dependency accelerates adaptation pressure

Healthcare Systems	Limited	Resource and infrastructure limitations	Sensitive data remain highly vulnerable
Small and Medium Enterprises	Low	Lack of expertise and funding	Quantum preparedness remains inaccessible for many organizations

The results also indicate that uncertainty about the timing of practical quantum disruption is often a factor influencing institutional responses. Some organizations delay action due to skepticism about near-term quantum capabilities while others promote immediate migration strategies to reduce future systemic risk.
This tension reflects a more general dilemma of governance, noted in the literature, that institutions have to spend significant resources on threats that are still technologically emergent but potentially catastrophic. The study thus emphasizes the paradox of quantum cybersecurity governance: decision-makers need to prepare extensively for a technological future that is uncertain, but potentially irreversible.

Theme 3: Strategic Significance of Post-Quantum Cryptography

The analysis clearly identifies post-quantum cryptography (PQC) as a major strategic response to future cybersecurity disruption. Experts, policymakers, and institutional actors increasingly see PQC not only as a technical upgrade but as a fundamental requirement to preserve digital trust, national security, and economic stability.

Results show that the role of PQC is beyond encryption replacement. Instead, PQC is more and more seen as a component of a larger change toward quantum-resilient digital ecosystems.

Table 3

Cryptographic System	Quantum Threat	Post-Quantum Alternative	Future Security Implication
RSA	Vulnerable to Shor's algorithm	Lattice-based cryptography	Enhanced long-term resistance
ECC	Quantum factorization risks	Hash-based signatures	Improved authentication security
Classical Key Exchange	Quantum computational exposure	Code-based cryptography	Greater resilience for secure communications

However, the findings also highlight substantial uncertainty about the long-term reliability and scalability of certain PQC algorithms. Some experts caution that the race to standardization may create unforeseen vulnerabilities, particularly if advances in quantum algorithms or computing techniques eventually undermine newly adopted systems.

This is a reflection of a deeper contradiction in cybersecurity modernization: institutions urgently need quantum-safe systems, but the accelerated adoption of immature standards may generate new security risks. The study thus bolsters academic calls for adaptive and flexible cryptographic governance instead of rigid technological standardisation.

Theme 4: Ethics, Surveillance and Digital Power

The results reveal that quantum technologies are more and more associated with ethical issues related to surveillance, privacy erosion and concentration of digital power. Within the broader academic and institutional debate there was often concern among participants that the quantum computational advantage may exacerbate the asymmetry of surveillance powers between technologically advanced states and companies.

The analysis brings up issues that quantum-enabled decryption capabilities could threaten:

- Rights of personal privacy,
- Confidential communications;
- First Amendment protections,
- Diplomatic confidentiality,
- And civil rights.

Such concerns are particularly salient in the context of authoritarian rule, where sophisticated surveillance infrastructures are already in place.

The study also raises new ethical concerns about the uneven distribution of technology. Currently, the development of quantum computing is focused on technologically advanced states and large private-sector corporations, contributing to concerns over digital inequality and technological dependency.

The results qualitatively suggest that quantum cybersecurity cannot be understood only in the technical security frameworks. Rather, it must be read through ethical and political lenses involving:

- Distribution of power,
- Independence of technology,
- Digital rights,
- And responsibility for governance.

This is congruent with contemporary critical cybersecurity scholarship that emphasizes the reproduction of larger social and geopolitical inequalities by technological systems.

Theme 5: Technology and Cyber Geopolitics: Global Competition

Another major theme is the intensifying geopolitical competition around quantum innovation. The findings show that quantum computing has been strategically associated with national security, cyber security, economic competitiveness, and technological sovereignty.

The qualitative evidence suggests that the major global powers are increasingly seeing quantum leadership as a determinant of future geopolitical influence. Governments are therefore throwing a lot of money into:

- Quantum research laboratory,
- National cyber security programmes;
- Cryptographic modernization,
- And quantum communication infrastructure.

The study concluded that this race for technology drives innovation, while at the same time increasing global cyber instability. On the one side, competition drives scientific progress and investments in cybersecurity. On the other hand, it promotes secrecy, technological fragmentation, cyber militarization and less international cooperation.

This finding echoes larger geopolitical tensions of the digital age, where cybersecurity technologies are becoming more and more tools of strategic power instead of just defensive infrastructure.

Theme 6: Challenges of transitioning to quantum-safe systems

The shift towards quantum-safe systems became one of the most operationally challenging issues surfaced in the analysis. Institutions are faced with major challenges in terms of:

- Infrastructure interoperability,
- Implementation cost
- Complexity of technical,
- Shortages of labour,
- And the uncertainty of regulations.

Many organizations continue to operate highly interdependent legacy systems that do not easily permit the integration of new cryptographic standards without disrupting critical functions. Migration environments are especially challenging for financial institutions, healthcare infrastructures, transportation systems and government databases.

The results indicate that migration challenges are not only technical. The implementation efforts are considerably hindered by organizational resistance to change, lack of understanding of the executive and competing financial priorities.

Importantly, the research identifies the risk of a "security transition gap" in which incomplete or uneven adoption of PQC could unintentionally create hybrid vulnerabilities in digital infrastructures.

This finding supports existing scholarship that argues that cybersecurity transformation requires not only technological upgrades but also institutional culture change, strategic planning and sustained governance coordination.

Theme 7: Cybersecurity Innovation and Resilience Opportunities

Nevertheless, they also demonstrate important opportunities associated with the quantum transition, despite the risks they identify. The rise of PQC has stimulated:

- Cryptographic innovation;
- Investment in research into cyber security;
- International standardization activities,
- And cross-disciplinary collaborations.

The analysis suggests that quantum disruption could eventually enhance long-term cybersecurity resilience by compelling institutions to upgrade outdated infrastructures that would otherwise remain untouched for decades.

The move to quantum-safe systems is therefore both defensive and transformative. Proactive adaptation can result in institutions having stronger digital resilience, better trust systems and more secure communication architectures.
The results also indicate that interdisciplinary cooperation between:

- Governments;
- Colleges,
- Cybersecurity sectors;
- Future quantum security transitions will increasingly depend on international organizations for effective management.

Discussion Integrated

The results of this study provide strong support for the arguments in the scholarly literature that quantum computing is one of the most consequential disruptions to cybersecurity in the twenty-first century. The study, however, also contributes to the current scholarship by demonstrating that the quantum transition is not just a cryptographic problem, but a governance, institutional, ethical and geopolitical one.

The research points to an important contradiction at the heart of today's cybersecurity systems. As modern societies become more dependent on digital infrastructures, the cryptographic foundations upon which these infrastructure are secured are facing potential obsolescence. This paradox highlights the institutional fragility and shortcomings of global cybersecurity governance models.

The study also shows that preparedness is uneven and largely determined by economic strength, technological capacity and geopolitical location. As a consequence, the emerging quantum divide may mirror today's global digital divides, with technologically advanced countries enjoying strategic supremacy and less advanced systems becoming more vulnerable to cyber dependency and infrastructural insecurity.

The findings also challenge the purely technological conceptions of cybersecurity resilience. To adapt effectively to quantum disruption, you need:

- Institutional foresight,
- Regulation flexibility,
- Ethical responsibility,
- International collaboration,
- And long-term strategic investment.

Importantly, the study concludes that the success of future governance of cybersecurity will likely depend on the capacity of institutions to transition from reactive security cultures to anticipatory resilience models. “Those organizations that wait for quantum disruption to be fully operational before taking protective measures may find that they have been exposed to irreversible security.

The results ultimately indicate that post-quantum cryptography should not be regarded as a mere replacement technology, but as part of a wider transformation of the way in which societies conceptualise trust, privacy, sovereignty and security in ever more complex digital ecosystems.

Conclusion

This qualitative study explored the emerging relationship between quantum computing and post-quantum cryptography from technological, institutional, ethical and geopolitical perspectives. The results demonstrate that quantum computing is both a serious threat to cybersecurity and a revolutionary force that could change the future architecture of secure digital systems.

The analysis shows that existing cryptographic infrastructures are increasingly at risk from future quantum capabilities especially in sectors with long-term data confidentiality and secure communications systems. Although practical large-scale quantum attacks have yet to materialise fully, the prospect of future quantum decryption is already influencing cybersecurity governance, institutional planning and cryptographic modernisation strategies across the globe.

A key finding from the research is that institutional preparedness continues to be patchy and fragmented. While some governments and technology leading firms have begun strategic shifts to post-quantum security architectures, many organizations are still running vulnerable legacy infrastructures with limited migration capabilities. This imbalance signals deeper systemic inequalities in the global digital governance system, and suggests that future quantum disruption could exacerbate existing cybersecurity inequalities between technologically advanced and resource-constrained systems.

The study also concludes that post-quantum cryptography has evolved from a narrow technical solution into a strategic pillar of digital resilience, national security and technological sovereignty. Therefore, moving to quantum-safe infrastructure requires not only cryptographic innovation, but also coordinated governance mechanisms, workforce development, regulatory adaptation and international collaboration.

Crucially, the findings reveal that the coming quantum landscape raises important ethical and political issues. Quantum enabled computational power could greatly expand state and corporate surveillance capabilities and challenge existing frameworks for privacy protection, civil liberties and digital rights. The concentration of quantum expertise and infrastructure in a handful of technologically dominant states and corporations may also exacerbate geopolitical asymmetries and heighten competition in cyber power.

The study underscores the critical importance of proactive, rather than reactive, cybersecurity strategies from a governance perspective. Those institutions that hesitate in migrating to quantum-safe systems due to uncertainty about the technology or financial considerations could be facing long-term security exposure that is harder and harder to unwind. Hence, anticipatory resilience planning becomes a key principle of future cybersecurity governance.

The study also states that successful adaptation to quantum disruption needs inter-disciplinary cooperation between:

- Policy-makers,
- Cybersecurity agencies,
- Technology industry,

- Educational institutions;
- And regulatory bodies at the international level.

Fragmented approaches to migration without collaborative governance frameworks may lead to inconsistent security standards and create new systemic vulnerabilities in interconnected digital ecosystems.
The findings suggest a number of practical recommendations. Governments should: fast-track national quantum readiness strategies; boost funding for post-quantum research; improve cybersecurity workforce development; and develop long-term migration roadmaps for critical infrastructure systems. To reduce operational disruption during transition processes, organizations need to focus on building inventory assessments of cryptographic technology, hybrid security architectures, and phased implementation planning.

There is a need for more collaboration globally to develop harmonized standards, responsible quantum governance and address the risks of technological fragmentation and cyber militarization. Ethical frameworks on privacy protection, digital rights, algorithmic accountability and surveillance governance must also keep up with technological advancement.

The study acknowledges that quantum technologies are still in a fast-evolving state with many unknowns remaining in terms of timelines, scalability and future cryptographic resilience. However, the qualitative evidence is very compelling that the shift to quantum-safe digital infrastructures is no longer a matter of speculation but an emerging strategic imperative.

Future work should therefore investigate:

- Sector-specific migration challenges;
- Comparative national preparedness models,
- Ethical governance frameworks of quantum technologies,
- Quantum inequality socio-economic implications,
- And the long-term link between quantum innovation and global cybersecurity stability.

In summary, quantum computing and post-quantum cryptography together represent a defining technological shift of the contemporary digital age. The future security of digital societies will depend not only on technological innovation but also on the ability of institutions, governments and international systems to anticipate disruption, govern responsibly and build resilient cybersecurity ecosystems that can sustain trust in an increasingly uncertain quantum future.

References

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2021). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(2), 56–78. https://doi.org/10.3390/healthcare7020056

Ahmad, F., & Um-e-Farwa, A. (2026). Faculty Readiness and Pedagogical Transformation in AI-Enabled Personalized Learning: A Phenomenological Study. *Journal of Social & Organizational Matters*, *5*(1), 19-30.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y. K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309

Ali, M., Shahzad, M. N., Amra, S., & Mahmood, M. (2022). Early career researchers' experiences of being school teachers and PhD students concurrently. *International Journal of Early Childhood Special Education*, *14*(7).

Alkhatib, O. J. ., Raja, S. ., & Asadullah. (2025). Modeling the Influence of Generative AI Writing Tools on Academic Integrity and Writing Proficiency in Higher Education: A Structural Equation Modeling Approach. *Research Journal for Social Affairs*, *3*(6), 1653-1660. https://doi.org/10.71317/RJSA.003.06.0655

Alkhatib, O. J., Asif, S., & Ullah, A. (2026). Next-Generation Smart Engineering Classrooms Using Generative Artificial Intelligence Technologies: https://doi. org/10.5281/zenodo. 20999171. *Journal for Current Sign*, *4*(2), 1377-1411.

Alkhatib, O. J., Rahman, F., Hussain, A. K., Siddique, M. E., & Farooq, H. O. (2026). Impact of Generative Artificial Intelligence on Student Learning Outcomes: The Mediating Role of Student Engagement and AI Literacy in Higher Education. *The Critical Review of Social Sciences Studies*, *4*(1), 6400-6424.

Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—A new hope. In *25th USENIX Security Symposium Proceedings* (pp. 327–343). USENIX Association.

Aman, F., Ullah, A., Shahzad, S., Ejaz, A., & Yasin, G. (2026). Integrating Artificial Intelligence in Educational Technology: Assessing Its Impact on Student Learning Outcomes and Engagement in Pakistani Schools. *Social Science Review Archives*, *4*(1), 4692-4707.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J., Barends, R., Biswas, R., Boixo, S., Brandao, F., Buell, D., Burkett, B., Chen, Y., & Google AI Quantum Team. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Asadullah, Dr. Khatiba bibi, & Muhammad Mukhtyar. (2024). RELATIONSHIP BETWEEN STUDENTS READING INTERESTS AND SELF-REGULATED LEARNING AT GRADUATION LEVEL: A COMPARISON OF SCIENCE AND ARTS STUDENTS. *International Journal of Contemporary Issues in Social Sciences*, *3*(3), 2630–2641. Retrieved from https://ijciss.org/index.php/ijciss/article/view/1444

Asadullah, Sinha, D., Kumar, S., Kumari, R., Kaur, A., & Kaur, J. (2026). Artificial Intelligence in Personalised Learning System. *International Journal on Research and Development - A Management Review*, *15*(1), 112–120. https://doi.org/10.65521/ijrdmr.v15i1.1727

Asadullah., Farooqi, M. T. K., & Saleem, K. (2024). Unpacking the Students' Experiences in Pakistan: Analyzing the Pursuit of Excellence in Teaching Practices at Higher Education Level. *Global Regional Review, IX(III)*, 1-10. https://doi.org/10.31703/grr.2024(IX-III).01

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer. https://doi.org/10.1007/978-3-540-88702-7

Biden, J. R. (2022). *National security memorandum on promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems*. The White House.

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., Stebila, D., & Wear, A. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. *IACR Cryptology ePrint Archive*.

Buchmann, J., Dahmen, E., & Schneider, M. (2021). Merkle tree traversal revisited. *Post-Quantum Cryptography*, 63–78. Springer.

Campagna, M., Chen, L., Dagdelen, O., Ding, J., Fernick, J., Gisin, N., Hayford, D., Jao, D., Kashefi, E., Mosca, M., & Sevinc, S. (2015). *Quantum safe cryptography and security: An introduction, benefits, enablers and challenges*. European Telecommunications Standards Institute.

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2020). Blockchain versus database: A critical analysis. *Journal of Software: Evolution and Process, 31*(12), e2188. https://doi.org/10.1002/smr.2188

CISA. (2022). *Post-quantum cryptography roadmap*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy* (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032

ENISA. (2021). *Post-quantum cryptography: Current state and quantum mitigation*. European Union Agency for Cybersecurity.

Essa, R., Shabih, T., Ullah, A., Siddique, M. E., Arif, S. N., & Shabih, A. (2026). IMPACT OF DIGITAL LEARNING TECHNOLOGIES ON STUDENT ACHIEVEMENT, TEACHING EFFECTIVENESS, AND EDUCATIONAL POLICY DEVELOPMENT IN HIGHER EDUCATION SYSTEMS. *Spectrum of Engineering Sciences*, *4*(6), 3316-3347.

Farwa, U., & Riaz, M. (2026). Developing Critical Thinking Skills Through Active Learning: Strategies for Higher Secondary and Undergraduate Education. *Social Science Review Archives*, *4*(1), 3485-3494.

Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Goldwasser, S., & Bellare, M. (2008). *Lecture notes on cryptography*. Massachusetts Institute of Technology.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 212–219). ACM. https://doi.org/10.1145/237814.237866

Hasselbach, C., & Krier, J. (2022). Quantum computing and cybersecurity: Emerging governance challenges. *Cybersecurity Policy Review, 4*(1), 33–49.

IBM Security. (2023). *The quantum-safe journey: Migration strategies for enterprises*. IBM Corporation.

ITU. (2022). *Quantum information technology for networks*. International Telecommunication Union.

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2020). Quantum-secured blockchain. *Quantum Science and Technology, 3*(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b

Kumar, R., Marchang, N., & Tripathi, R. (2021). Distributed denial of service attacks and defense mechanisms in cloud computing: A survey. *Journal of Network and Computer Applications, 162*, 102631. https://doi.org/10.1016/j.jnca.2020.102631

Lyubashevsky, V. (2012). Lattice signatures without trapdoors. In *Advances in Cryptology – EUROCRYPT 2012* (pp. 738–755). Springer. https://doi.org/10.1007/978-3-642-29011-4_43

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

National Security Agency. (2022). *Quantum computing and post-quantum cryptography frequently asked questions*. NSA Cybersecurity Directorate.

NIST. (2022). *Post-quantum cryptography standardization*. National Institute of Standards and Technology. https://www.nist.gov/pqcrypto

NIST. (2024). *Selected algorithms for post-quantum cryptography standardization*. National Institute of Standards and Technology.

NSA. (2021). *Commercial national security algorithm suite and quantum computing FAQ*. National Security Agency.

Nweke, H. F., Teh, Y. W., Mujtaba, G., & Al-Garadi, M. A. (2020). Data fusion and multiple classifier systems for human activity detection and health monitoring: Review and open research directions. *Information Fusion, 46*, 147–170. https://doi.org/10.1016/j.inffus.2018.06.002

OECD. (2021). *Quantum technologies and policy implications*. Organisation for Economic Co-operation and Development.

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science, 10*(4), 283–424. https://doi.org/10.1561/0400000074

Perlner, R., Cooper, D., Chang, A., Bassham, L., & Turan, M. S. (2020). *Status report on the third round of the NIST post-quantum cryptography standardization process*. National Institute of Standards and Technology.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., & Razavi, M. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236. https://doi.org/10.1364/AOP.361502

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

Sarker, I. H. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 8*(1), 1–29. https://doi.org/10.1186/s40537-021-00444-1

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton & Company.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Sovacool, B. K., Hook, A., Martiskainen, M., Brock, A., & Turnheim, B. (2020). The decarbonisation divide: Contextualizing landscapes of low-carbon exploitation and toxicity in Africa. *Global Environmental Change, 60*, 102028.

Stallings, W. (2022). *Cryptography and network security: Principles and practice* (9th ed.). Pearson.

ULLAH, A. (2020). Students' experiences of failure to get admission in desired medical degree programs and their choices of alternative degrees.

Ullah, A., & Farooqi, M. T. K. (2025). Dimensions of Quality Teaching in Higher Education: A Comparative Analysis of Faculty Perceptions Across Demographic Variables. *ProScholar Insights*, *4*(4), 217-227.

Ullah, A., & Saeed, S. (2026). EFFECT OF PARENTING STYLE ON SELF-ESTEEM AND ACADEMIC PERFORMANCE OF SCHOOL CHILDREN. *Spectrum of Engineering Sciences*, *4*(6), 3745-3762.

Ullah, A., Khan, A., & Baig, M. (2026). THE PERCEIVED IMPACT OF GAMIFICATION ON STUDENTS'MOTIVATION AND ACADEMIC PERFORMANCE: A QUALITATIVE ANALYSIS OF STUDENTS'EXPERIENCES. *Policy Journal of Social Science Review*, *4*(6), 921-948.

Ullah, N., Ishaq, M., Rahman, F., Aslam, M. U., & Adil, F. (2026). An Advanced AI-Driven Risk Assessment Framework for US Banking Institutions: Integrating Predictive Financial Analytics, Regulatory-Aware Governance and Cybersecurity Risk Intelligence. *Journal of Management Science Research Review*, *5*(2), 3176-3204.

United Nations Institute for Disarmament Research. (2021). *The cybersecurity implications of quantum technologies*. UNIDIR.

Verma, G. K., & Singh, B. B. (2021). Cloud computing security issues and challenges: A survey. *International Journal of Computer Applications, 174*(12), 1–6.

Wang, W., Xu, H., He, X., & Ashikhmin, A. (2022). Quantum-resistant blockchain and distributed ledger technologies: A systematic review. *Future Generation Computer Systems, 129*, 1–18. https://doi.org/10.1016/j.future.2021.11.019

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science, 362*(6412), eaam9288. https://doi.org/10.1126/science.aam9288

World Bank. (2022). *Digital development and cybersecurity resilience in emerging economies*. World Bank Publications.

World Economic Forum. (2022). *Transitioning to a quantum-secure economy*. World Economic Forum.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Yousafzai, S., Asif, A., Urfi, F., Ahmad, L., & Ullah, A. (2026). Investigating Social Communication Difficulties among Children with Autism Spectrum Disorder in Educational Settings. *Research Consortium Archive*, *4*(2), 2825-2841.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647

Zhou, L., Su, C., Chiu, W., Yeh, K., & Yeo, Y. (2023). Post-quantum cryptography adoption challenges in critical infrastructures. *Journal of Information Security and Applications, 72*, 103418. https://doi.org/10.1016/j.jisa.2022.103418

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27