# Cryptographic defense against quantum computer attacks: A scoping review

Vullnet Gërvalla[1,†] and Eliot Bytyçi[1,*, †]

[1] University of Prishtina, Avenue Mother Teresa, No-5, 10000, Prishtinë, Republic of Kosova

**Abstract**

With the advancement of quantum computing, traditional cryptography algorithms are becoming more vulnerable to attacks. As a result, researchers and industries are exploring new methods to withstand those possible attacks in the future. Thus, we conducted a scoping review on one of cybersecurity's most pressing challenges: keeping our data safe from quantum computing attacks. The survey focuses more on the studies with realistic implementation chances that are tested or proven to work, published between 2020 and 2024, identified through online databases: IEEE Xplore, Springer Link, ACM Digital Library, and ScienceDirect. From our perspective, based on the survey, there are two main paths to addressing the issue: quantum key distribution and post-quantum algorithms. Moreover, selected studies agree that implementing these new solutions isn't cheap, but complete security failure is far more expensive. Of course, the solutions have limitations, most notably, that these solutions can't be fully tested against real quantum computers yet since they're still being developed. But that doesn't mean that we need to wait for quantum computing to be the norm, before we start thinking of ways to defend against them. Furthermore, there are several tested solutions that believe that they are ready for implementation now, especially in critical areas like finance and healthcare.

**Keywords**

quantum cryptography, quantum computer, post-quantum, quantum key distribution

## 1. Introduction

The emergence of practical quantum computing threatens to undermine the foundational pillars of cryptographic security. Classical public-key encryption schemes, such as Rivest-Shamir-Adleman (RSA) and elliptic-curve cryptography (ECC), that rely on mathematical problems, prime factorization and discrete logarithms, respectively, are believed to be unbreakable for classical computers. However, with the development of large-scale quantum computers, algorithms like Shor's [1] promise the efficient factorization of large integers, rendering classical keys vulnerable and compromising a multitude of secure communication protocols. As a result, the cryptographic community has accelerated the pursuit of quantum-resistant, or post-quantum [2], cryptographic schemes that can withstand the capabilities of a quantum adversary.

In parallel to post-quantum cryptography (PQC), quantum key distribution (QKD) systems offer another complementary approach for secure communication in a quantum world. QKD leverages fundamental quantum mechanical properties, such as quantum entanglement, to enable secure distribution of symmetric keys with theoretically unbreakable security guarantees [3]. However, despite its promise, QKD faces challenges in terms of infrastructure, cost, and integration with existing systems. Meanwhile, PQC solutions, ranging from lattice-based, hash-based, and code-based cryptographic algorithms, are rapidly advancing toward standardization and practical deployment. Organizations like the U.S. National Institute of Standards and Technology (NIST) are leading the efforts to finalize post-quantum encryption and signature standards [4].

[1] 6th International Conference Recent Trends and Applications in Computer Science and Information Technology RTA-CSIT, May 22-24, 2025, Tirana, Albania

* Corresponding author.

† These authors contributed equally.

vullnet.gervalla@student.uni-pr.edu (V. Gërvalla); eliot.bytyci@uni-pr.edu (E. Bytyçi)

0009-0003-6134-5280 (V. Gërvalla); 0000-0001-7273-9929 (E. Bytyçi)

This scoping review examines the development, testing and real-world implementation of both QKD and PQC solutions. While the theoretical security properties of many proposed algorithms are well-documented, their practical readiness - particularly in terms of cost implications and the challenges of migrating existing infrastructures, remains underexplored. Indeed, the shift to quantum-resistant security is not merely a matter of selecting a new algorithm, it involves assessment of performance overhead, compatibility with legacy systems, and cost-effectiveness. For organizations managing sensitive data that must remain secure for decades, the urgency of this transition cannot be overstated.

While a growing body of literature explores the theoretical foundation of post-quantum cryptography and quantum key distribution, not all studies equally address the feasibility of near-term deployment. Many solutions have been conceptually validated, but their practicality in large-scale, latency-sensitive networks remains underexamined. Additionally, understanding the cost of integrating quantum resistant measures is critical, as the financial overhead can pose significant barriers to adoption. Recent years have seen several research prototypes, and the development of hybrid solutions, combining classical and quantum-resistant methods [5]. By examining these works systematically, we aim to bridge the gap between theory and practice and identify which solutions are ready for implementation, what their associated costs might be, and how prepared various industries are to integrate them.

Having said that, this review is structured around these primary objectives:

1. **Identify and characterize recent quantum-resistant cryptographic solutions:** We focus on solutions published from 2022 onwards, including QKD implementations and various classes of PQC algorithms. Although the range of PQC schemes is broad, particular emphasis is placed on lattice-based cryptography, as this category is well-represented in current research and is considered a leading candidate for standardization.
2. **Assess cost and real-world readiness:** Beyond pure cryptographic strength, this review evaluates the economic and engineering challenges associated with these quantum-resilient measures. We examine studies that address increased resource consumption, latency or bandwidth overhead, necessary hardware modifications, and cost estimates. This includes investigations that quantify the added expense of integrating quantum-safe solutions into critical infrastructures.
3. **Analyze current implementation challenges and potential solutions:** This review highlights the technical hurdles, design complexities, migration roadmaps, and regulatory or policy considerations that influence the feasibility of adopting quantum-safe measures. Special attention is given to studies that present frameworks, guidelines, or case studies illustrating how organizations can transition their security infrastructures efficiently.

In undertaking this analysis, we offer a more grounded perspective, countering overly theoretical optimism or undue pessimism, and instead providing a balanced, evidence-based overview of where we stand today in our preparedness for the quantum era.

## 2. Methodology

For this scoping review we followed the Arksey & O'Malley five-stage scoping review process: identifying the research questions, identifying relevant studies, study selection, charting the data, and finally collating, summarizing and reporting results. Having laid out the research questions and aims of this review above, the following sections outline the information sources, screening and selection procedures, charting the data and risk of bias.

### 2.1. Identifying Relevant Studies

We included studies meeting the following criteria:

- **Population and Context:** Studies focusing on cryptographic schemes designed to be secure against quantum attacks, including both quantum key distribution (QKD) and post-quantum cryptographic (PQC) algorithms. These studies addressed the threat posed by quantum computers to classical cryptographic infrastructures.
- **Intervention and Phenomenon of Interest:** We targeted research presenting or evaluating cryptographic solutions, frameworks, protocols, or proofs-of-concept related to quantum-safe security. This encompassed:
    - Post-quantum algorithms under consideration for standardization (e.g., lattice-based cryptography).
    - Quantum key distribution (QKD) systems or protocols demonstrating real-world or testbed implementations.
    - Hybrid solutions combining classical and quantum-safe techniques.
- **Outcomes of Interest:** Primary outcomes included considerations of security against quantum attacks, algorithmic complexity, and resistance to quantum-based cryptanalysis. Secondary outcomes included implementation cost estimates, performance overhead (e.g., increases in latency, bandwidth consumption, or computational resources), and readiness for large-scale deployment. We focused on indicators that reflect how close the described solutions are to practical implementation, rather than purely theoretical security claims.
- **Timeframe and Language:** The search was limited to studies published between 2022 and the time of the review, end of 2024, ensuring the inclusion of the most recent advancements and practical demonstrations. Only open-access studies in English were considered to maintain consistency and ensure access to complete texts.
- **Exclusion Criteria:** We excluded studies that:
    - Addressed quantum cryptographic topics unrelated to secure key exchange or digital signature schemes (e.g. non-cryptographic quantum computation research).
    - Focused solely on quantum hardware aspects without direct cryptographic relevance.
    - Fell outside of the thematic scope of quantum-safe cryptography defence, such as studies focusing only on classical cryptographic methods.

### 2.2. Information sources and search strategy

We conducted the literature search across four major scholarly databases well-regarded in the fields of computing and cryptography: IEEE Xplore, ACM Digital Library, Springer Link, and Science Direct. These databases were selected for their broad coverage of cryptographic research, established peer-review standards, and wide inclusion of reputable conference proceedings and journal articles.

- **Search Queries and Filters:** We limited the search to English-language, open-access articles published from 2022 to the end of 2024. The search terms used in all databases included “cryptography” and “quantum” in the title field. By requiring these terms in the title, we aimed to retrieve studies that placed quantum-safe cryptography or quantum-related cryptographic defenses as a primary focus. Each database’s filtering tools were utilized to restrict by publication year (2022–2024) and open-access availability where possible.

### 2.3. Study selection process

The study followed a multi-stage selection process:

1. **Initial Retrieval:** More than one hundred papers were retrieved by combining the results from the four selected databases.

2. **Title-Based Screening:** From the initial set of about one hundred papers, we examined the titles for relevance. We included only those titles that explicitly suggested a focus on quantum-related cryptography (e.g., mention of "post-quantum," "quantum key distribution," "quantum-safe," or "quantum cryptanalysis") and the defense mechanisms or migrations associated with them. Titles that were too broad, unclear, or related to quantum computing but not cryptography were excluded. This step narrowed the pool down to approximately 30 studies.
3. **Abstract Review:** Next, the abstracts of these 30 studies were thoroughly read. Abstracts needed to demonstrate a clear emphasis on practical or semi-practical implementation aspects of post-quantum or quantum-safe cryptographic solutions. Abstracts that mentioned cost analysis, performance overhead, or other readiness indicators were favored. Those that focused solely on theoretical aspects without any connection to practical deployment scenarios were excluded. After this screening, 20 studies were deemed suitable for full inclusion.

## 2.4. Charting the Data

Data extraction for each included paper was guided by a structured approach, where the following were gathered:

- **Bibliographic Information:** Title, authors, year of publication, and publication venue (journal or conference proceedings).
- **Type of Solution:** Whether the study focused on QKD, lattice-based PQC algorithms, code-based algorithms, hybrid approaches, or general frameworks for migrating to quantum-safe cryptography.
- **Implementation Context:** Any mention of testbeds, pilot deployments, or real-world networks. If implementation was purely theoretical or simulated, we noted this distinction.
- **Cost and Overhead:** Information regarding additional computational, hardware, or financial costs introduced by quantum-safe solutions. Studies that provided numerical or qualitative assessments of cost, energy consumption, required infrastructure changes, and staffing or training needs were highlighted.
- **Performance Metrics:** Details on cryptographic performance such as key generation and exchange times, encryption/decryption speed, bandwidth consumption, memory overhead, and latency factors.
- **Readiness and Feasibility:** Qualitative descriptors of how close these solutions are to practical deployment. Particular attention was paid to studies that discussed timelines, migration strategies, interoperability with existing systems, and industry or policy guidance.

## 2.5. Risk of bias and quality assessment

Due to the relatively recent and highly technical nature of the field, we did not apply a traditional risk of bias tool often used in other sciences scoping reviews. Instead, we considered indicators of reliability and practical significance as a proxy for quality assessment. For example, we gave greater weight to studies that included some form of empirical testing, performance benchmarks, or cost analysis rather than those offering purely speculative or theoretical results. Studies that presented reproducible experiments, open-source code, or alignment with recognized standardization bodies (e.g., referencing the NIST Post-Quantum Cryptography process) were considered more robust.

While this is not a standard bias assessment tool, it aligns with the pragmatic aims of this review. The logic here is that a "proven to work" or "tested" claim suggests at least some level of verification against real or simulated conditions, reducing the likelihood that conclusions are based solely on speculation. Thus, studies presenting empirical or semi-empirical data and referencing ongoing

standardization efforts were deemed to be at lower risk of bias in terms of overstating their practical readiness.

## 3. Results

The search and selection process identified 20 studies, from which [1] describes one of the earliest quantum algorithms for breaking classical cryptography and [2] contributed to defining the quantum cryptography terminology used in this review. The remaining 18 studies each contributed to different aspects of quantum-safe cryptography.

The studies examined various approaches to creating secure systems in the face of quantum computing threats. For example, authors in [6] combined QKD and PQC to create a hybrid framework tested under simulated conditions. While other [5] developed a three-key hybrid system combining classical and quantum-safe algorithms, implemented on Field-programmable Gate Array (FPGA) platforms. In the IoT context, study [7] integrated blockchain technology with lightweight cryptographic protocols and QKD to secure resource-constrained devices. These studies addressed different aspects of quantum-safe cryptography, from theoretical innovations to practical deployment challenges.

The studies varied in their level of empirical testing and practical application. For instance, authors in [4] provided real-world validation of its hybrid system for securing 5G networks, reducing its bias risk. On the other hand, study [8] offered mostly theoretical analysis without practical validation, making it more prone to bias. Studies that included real-world testing or detailed implementation strategies generally provided stronger and more reliable evidence.

### 3.1. Result analysis

Individual studies explored a variety of themes and methodologies. For instance, authors in [9] highlighted advancements in photon-source technologies to improve QKD scalability, while others optimized hardware for lattice-based PQC, demonstrating improved efficiency for constrained devices [10]. Additionally, in a case the potential role of AI in enhancing QKD systems, offering innovative but untested proposals for dynamic optimizations, was examined [3].

The synthesis of the studies identified three primary application contexts:

- critical infrastructures and networks,
- IoT systems, and
- algorithm/hardware optimization.

Each application context was further grouped based on the cryptographic approach (into hybrid systems, QKD, and PQC). Studies that did not fit into these categories are also discussed to ensure comprehensive coverage.

#### 3.1.1. Critical infrastructures and networks

Several studies focused on using hybrid cryptographic systems to protect critical infrastructures. For example, [12] proposed a TLS protocol that combines QKD with lattice-based PQC algorithms like CRYSTALS-Kyber, ensuring strong security while maintaining compatibility with existing infrastructure. Others [5] developed a flexible three-key system that integrates pre-quantum, post-quantum, and quantum cryptography. This study stood out for its implementation on FPGA platforms, showing real-world feasibility while maintaining security against quantum threats.

Advancements in QKD were highlighted in [9], which explored the use of quantum dot photon sources to improve scalability and reduce vulnerabilities in large-scale networks. Similarly, [4] validated the use of QKD in critical infrastructure, focusing on secure key exchange in large communication networks through hierarchical key management, enhancing security with reduced latency.

This study [8] explored the resilience of lattice-based cryptosystems against quantum attacks. Although primarily theoretical, it emphasized the importance of lattice-based methods, like CRYSTALS-Kyber, which are increasingly recognized for their potential in critical infrastructure. Similarly, authors in [11] evaluated PQC algorithms for operational technology systems, highlighting the need for low-latency solutions in legacy environments.

### 3.1.2. IoT and Resource-Constrained Environments

A solution proposed by [7] integrated blockchain, lightweight cryptography, and QKD to secure multimedia data in IoT devices. This study emphasized energy efficiency and scalability for resource-constrained environments. Authors in [13] combined QKD with lattice-based PQC, optimizing security for IoT systems with limited computational power.

This study [14] discussed how QKD protocols, like BB84, could secure IoT applications, focusing on vulnerabilities in sensing and networking layers. It also emphasized the challenges of adapting QKD to short-range and low-power devices.

Interestingly, the authors in [10] provided a hardware-specific approach to optimize PQC for IoT, achieving lower energy consumption. Similarly, [15] offered practical insights into integrating lattice-based PQC algorithms into cryptographic libraries, enhancing usability for constrained systems.

### 3.1.3. Algorithms and hardware optimization

The authors in [6] explored how TLS protocols could integrate QKD and PQC, validated under ETSI standards. This study emphasized scalability and cost-efficiency, making it relevant for real-world applications.

Alternatively, [9] provided significant advancements in QKD scalability, focusing on photon-source technology to address long-distance communication challenges.

Notably, [16] applied quantum annealing to optimize PQC algorithms, showing potential for improving efficiency in cryptographic tasks. Whereas [17] focused on planning systematic transitions to PQC, highlighting dependency analysis and cost considerations.

### 3.1.4. Studies outside the above-mentioned groupings

Some studies did not fit into specific application contexts but provided broader insights, for instance [18] explored the institutional and policy challenges of adopting quantum-safe cryptography, focusing on organizational readiness and regulatory gaps. Whereas [19] introduced Quantum Secure Direct Communication (QSDC) as an alternative to QKD, emphasizing its potential for direct, secure communication. Notably, [3] explored AI's role in enhancing QKD performance, presenting innovative but untested ideas.

## 3.2. Reporting biases

Some studies emphasized benefits while underreporting challenges. For instance, [3] highlighted potential optimizations through AI but did not address the practical hurdles of implementing such systems. Similarly, [20] discussed hybrid cryptographic systems but offered limited details on real-world scalability.

## 3.3. Certainty of evidence

Studies involving real-world testing, such as [4] and [5], provided the highest certainty of evidence. Theoretical studies, like [8], contributed valuable insights but lacked empirical testing, limiting their practical applicability. Overall, the evidence showed significant progress in quantum-safe cryptography while highlighting areas that need further development.

## 4. Discussion

This scoping review provides a comprehensive mapping of the current landscape of quantum-resistant cryptographic solutions, highlighting both the diversity of approaches and the varying levels of implementation readiness. By exploring the breadth of research rather than assessing the strength of evidence, we have identified key themes, research gaps, and future directions that can inform both research and practice in this rapidly evolving field.

The findings of this scoping review emphasize the critical need for both theoretical innovation and practical implementation in quantum-safe cryptography. Hybrid cryptographic systems, combining QKD and PQC, emerged as a leading solution for ensuring resilience against quantum threats. For instance, [12] demonstrated the robust integration of QKD and lattice-based PQC into TLS protocols, addressing quantum-era security challenges while maintaining compatibility with existing infrastructures. Similarly, [5] provided a compelling example of a three-key system achieving security flexibility and resilience against quantum attacks.

While practical applications in IoT and 5G networks highlighted the feasibility of transitioning to quantum-safe measures, challenges in scalability, latency, and cost persist. For instance, [7] illustrated the integration of blockchain and lightweight cryptography with QKD for resource-constrained environments, but the study also emphasized the infrastructure demands of QKD. Likewise, [4] showcased QKD's potential in securing critical infrastructures but acknowledged the difficulty of large-scale deployment.

Post-quantum cryptography has shown promise as a scalable alternative or complement to QKD. Studies like [10] optimized lattice-based algorithms for constrained devices, while [15] underscored the importance of usability through open-source integrations. However, theoretical studies like [8] underscored the field's reliance on lattice-based algorithms, which, while promising, remain subject to scrutiny and future potential quantum attacks.

### 4.1. Limitations

This review identified several limitations in the current body of research. While empirical studies provided valuable insights, many studies, such as [3] and [19], relied heavily on theoretical models without practical validation. This reliance on untested proposals limits the immediate applicability of their findings.

Another limitation was the lack of cost and scalability analyses in many studies. For instance, [9] provided advancements in QKD technologies but did not address the financial and infrastructural challenges of implementing these systems in real-world networks. Similarly, [18] discussed organizational and policy barriers but offered limited quantitative data on cost or resource requirements.

Standardization and interoperability challenges were another recurring theme. While studies like [17] presented structured approaches for transitioning to PQC, the absence of finalized standards complicates large-scale adoption. This uncertainty is particularly significant in critical infrastructure environments where backward compatibility with legacy systems is critical.

### 4.2. Future work

Based on this review, several roads for future research and development are clear. Initially, theoretical studies, such as [8] and [3], need empirical testing to validate their assumptions and proposed solutions. More experimental implementations and testbeds, like those in [4], should be prioritized.

Addressing scalability challenges in QKD and PQC is critical. Studies like [9] should extend their focus to include cost and performance benchmarks for real-world deployments. Similarly, the infrastructure requirements highlighted in [7] need to be addressed to make quantum-safe cryptography viable for large-scale adoption.

Hybrid systems combining QKD and PQC showed significant promise but require further optimization for resource efficiency and ease of integration. This study [5] offers a valuable starting point for exploring lightweight and flexible implementations.

Studies like [18] emphasized the need for clear guidelines and frameworks to support the transition to quantum-safe measures. Collaborative efforts between researchers, industry stakeholders, and policymakers are essential for defining interoperability standards and incentivizing adoption.

Future research should focus on energy-efficient PQC implementations, particularly for IoT and constrained environments. [10] demonstrated the potential for hardware-specific optimizations, which should be further developed and scaled.

### 4.3. Conclusion

This scoping review highlights the growing importance of quantum-safe cryptography in preparing for the challenges posed by quantum computing. Hybrid systems that combine QKD and PQC have emerged as a powerful approach, offering both resilience and flexibility against quantum threats. Studies such as [5] and [12] demonstrate practical solutions that integrate quantum-safe methods into existing infrastructures. Similarly, advancements in PQC, as shown in [10], highlight the potential for scalable and efficient cryptographic systems.

However, challenges remain. While QKD provides unmatched security, its cost and scalability limit its widespread adoption. PQC, on the other hand, offers a more accessible alternative but requires further optimization for resource-constrained environments like IoT systems. The lack of finalized standards and the need for practical validation also pose barriers to the adoption of quantum-safe solutions.

To fully realize the potential of quantum-safe cryptography, future efforts should focus on bridging the gap between theory and practice. This includes testing proposed systems in real-world settings, addressing scalability and cost issues, and developing clear policies and standards to guide implementation.

## Declaration on Generative AI

During the preparation of this work, the authors used GPT-4o and Grammarly to improve the grammar and to spell check.

## References


[1] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26, 5 (Oct. 1997), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Gasser, L. (2023). Post-quantum Cryptography. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_10

[3] Radanliev, P. Artificial intelligence and quantum cryptography. J Anal Sci Technol 15, 4 (2024). https://doi.org/10.1186/s40543-024-00416-6

[4] Asier Atutxa, Ane Sanz, Jorge Sasiain, Jasone Astorga, Eduardo Jacob, "Towards a quantum-safe 5G: Quantum Key Distribution in core networks", Computer Communications, Volume 224, 2024, Pages 145-158, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2024.06.005

[5] S. Ricci, P. Dobias, L. Malina, J. Hajny and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 12, pp. 23206-23219, 2024, doi: 10.1109/ACCESS.2024.3364520.

[6] K. -S. Shim, B. Kim and W. Lee, "Research on Quantum Key, Distribution Key and Post-Quantum Cryptography Key Applied Protocols for Data Science and Web Security," in Journal of Web Engineering, vol. 23, no. 6, pp. 813-830, September 2024, doi: 10.13052/jwe1540-9589.2365.

[7] Shalini Dhar, Ashish Khare, Ashutosh Dhar Dwivedi, Rajani Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography", Internet of Things, Volume 25, 2024, 101019, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.101019.

[8] Bruce Schneier. 2024. Lattice-Based Cryptosystems and Quantum Cryptanalysis. Commun. ACM Online First (June 2024). https://doi.org/10.1145/3665224

[9] Bozzio, M., Vyvlecka, M., Cosacchi, M. et al. Enhancing quantum cryptography with quantum dot single-photon sources. npj Quantum Inf 8, 104 (2022). https://doi.org/10.1038/s41534-022-00626-z

[10] Akçay, L., Yalçın, B.Ö. Lightweight ASIP Design for Lattice-Based Post-quantum Cryptography Algorithms. Arab J Sci Eng (2024). https://doi.org/10.1007/s13369-024-08976-w

[11] J. Oliva del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo and J. Etxezarreta Martinez, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," in IEEE Internet of Things Journal, vol. 11, no. 18, pp. 30217-30244, 15 Sept.15, 2024, doi: 10.1109/JIOT.2024.3410702.

[12] Carlos Rubio García, Simon Rommel, Sofiane Takarabt, Juan Jose Vegas Olmos, Sylvain Guilley, Philippe Nguyen, Idelfonso Tafur Monroy, "Quantum-resistant Transport Layer Security", Computer Communications, Volume 213, 2024, Pages 345-358, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2023.11.010

[13] Hosam Alhakami, "Enhancing IoT Security: Quantum-Level Resilience against Threats", Computers, Materials and Continua, Volume 78, Issue 1, 2024, Pages 329-356, ISSN 1546-2218, https://doi.org/10.32604/cmc.2023.043439

[14] Diksha Chawla, Pawan Singh Mehra, "A Survey on Quantum Computing for Internet of Things Security", Procedia Computer Science, Volume 218, 2023, Pages 2191-2200, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.01.195

[15] Hekkala, J., Muurman, M., Halunen, K. et al. Implementing Post-quantum Cryptography for Developers. SN COMPUT. SCI. 4, 365 (2023). https://doi.org/10.1007/s42979-023-01724-1

[16] X. Ji, B. Wang, F. Hu, C. Wang and H. Zhang, "New advanced computing architecture for cryptography design and analysis by D-Wave quantum annealer," in Tsinghua Science and Technology, vol. 27, no. 4, pp. 751-759, Aug. 2022, doi: 10.26599/TST.2021.9010022.

[17] K. F. Hasan et al., "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," in IEEE Access, vol. 12, pp. 23427-23450, 2024, doi: 10.1109/ACCESS.2024.3360412.

[18] Ini Kong, Marijn Janssen, Nitesh Bharosa, "Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions", Government Information Quarterly, Volume 41, Issue 1, 2024, 101884, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2023.101884

[19] D. Pan et al., "The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 26, no. 3, pp. 1898-1949, thirdquarter 2024, doi: 10.1109/COMST.2024.3367535.

[20] Sanzida Hoque, Abdullah Aydeger, and Engin Zeydan. 2024. Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. In Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (PECS '24). Association for Computing Machinery, New York, NY, USA, 9–16. https://doi.org/10.1145/3659997.3660033