Journal of Wireless Networks and Communication Systems
Vol. 1, Issue. 3, Jul-Sep 2025, pp. 24~34
ISSN: 3107-6432

QHCP: Quantum-Resilient Hybrid Cryptographic Protocol for Secure Data Exchange in Next-Generation Networks

Mahesh Chandrasekar[1], Selvakumar Chelliah[2]
[1]Lecturer, Engineering Department, College of Engineering & Technology,
University of Technology and Applied Sciences, Shinas, Sultanate of Oman.
mahesh.chandra@utas.edu.om
[2]Lecturer, Engineering Department, College of Engineering & Technology,
University of Technology and Applied Sciences, Shinas, Sultanate of Oman.
selva.chelliah@utas.edu.om

Article Info

Article History:

Received Jun 13, 2025
Revised Jul 10, 2025
Accepted Aug 12, 2025

Keywords:
Quantum-Resilient Cryptography
Hybrid Cryptographic Protocol
Post-Quantum Security
Secure Data Exchange
Next-Generation Networks

ABSTRACT

As the next-generation networks are developed, the demands for secure, reliable, and future-proof protocols for data exchange are greater than ever. Traditional cryptographic protocols remain susceptible to seemingly futuristic low-risk, high-reward advancements of commercial quantum computing. We exhibit a novel protocol named QHCP: Quantum-Resilient Hybrid Cryptographic Protocol, which combines the post-quantum resiliency from several post-quantum cryptographic algorithms with efficiency gained from maintaining the use of classical protocols to ensure data remains confidential and/or the integrity of data remains intact over time. The architectural style that QHCP uses is a Layered approach: Performance (application layer) to Quantum Resistance (crytographical superfluous services). In addition to it, QHCP solves practical issues such as hygienic key handling for minimizing potential risks introduced by cyber breaks and low-latency cycles that are perfect for working in fast, resource-limited environments. On a first glance, we find reasonableness of the security soundness/efficiency trade-offs and range for how (on next-to-future-internet-of-things (of) things systems to) on the future bigger computing infrastructures under 6th generation (6g)) farities of use can possibly be supported by QHCP! All-in-all, QHCP offers a strong path for making the sensitive data minimum quantum-protected through hybrid quantum-classical model resistant to diverse evolving advanced cyber threats.

Corresponding Author:

Mahesh Chandrasekar,
Engineering Department, College of Engineering & Technology,
University of Technology and Applied Sciences, Shinas, Sultanate of Oman.
Email: mahesh.chandra@utas.edu.om

1. INTRODUCTION

The digital environment is evolving rapidly. The growth of the Internet of Things (IoT) and the proliferation of 5G and 6G broadband networks are changing how we transmit information and process it. This new form of network will be expected to provide speed, trustworthiness of service, while securely processing enormous amounts of sensitive data for financial systems, smart cities, and tracking health care in real-time [1][2].

For decades, numerous ciphers, such as RSA, and Elliptic Curve Cryptography (ECC), have been in place to protect digital communication; a situation now unclear due to quantum computing. Specifically, there are quantum computing algorithms such as Shor's algorithm, and Grover's algorithm that pose a threat to breaking these existing established and well-known methods of encryption, and offer ways of breaking current communication that we deemed secure [3] [4]. In essence, the underlying premise for warranted digital security is in jeopardy in the quantum future.

Post-quantum cryptography (PQC) has emerged as a viable solution. PQC algorithms are based on hard mathematical problems such as lattices and error correcting codes, which are known to be secure against quantum attacks [5]. The drawback of PQC algorithms is that they require more processing power and memory and can thus be hard to deploy in practice where both security and speed/efficiency are important [6]. In contrast, classical symmetric encryption maintains its high efficiency but requires a secure key exchange—something quantum computers could quickly undermine [7].

At this point, the need for a balanced approach is evident. In this paper, we present the Quantum-Resilient Hybrid Cryptographic Protocol (QHCP), a security protocol that aims to take the best of both worlds into consideration. QHCP incorporates the lightweight symmetric encryption as an efficient method to handle rapid processing of data and implements lattice-based post-quantum methods to leverage resilience against future quantum adversaries. By doing so, it addresses the practical trade-off between strong security and system performance, particularly in environments like IoT and 6G networks where resources and latency matter [8].

The contributions of this paper are threefold:

- We design a hybrid cryptographic protocol that unites classical efficiency with quantum resistance.
- We introduce an adaptive key management strategy to strengthen resilience against both classical and quantum attacks.
- We evaluate the protocol in simulated next-generation network environments, demonstrating that QHCP achieves a strong balance between security and performance.

The rest of this paper is structured as follows: Section II reviews existing approaches and related work. Section III details the architecture and design of QHCP. Section IV presents the security analysis, while Section V discusses performance evaluation. Section VI highlights potential applications, and Section VII concludes with directions for future research.

2. LITERATURE REVIEW

[9] Conducted a comprehensive survey of post-quantum cryptographic schemes, with a particular emphasis on their performance in resource-constrained IoT devices. Their work highlighted that while lattice-based algorithms such as Kyber and Dilithium provide strong quantum resistance, they often impose heavy computational and communication overheads. The study emphasized the need for optimization strategies to reduce energy and memory consumption, but it did not propose a practical hybrid framework that could achieve a balance between security and efficiency.

A roadmap study by [10] focused on the transition from classical to post-quantum cryptography in 5G-enabled IoT systems. The authors examined challenges such as authentication, scalability, and integration of post-quantum algorithms into existing infrastructures. Although this research provides critical understanding into migration strategies, it is mostly theoretical and lacks proposed protocols suitable for real-time environments that need to function in a low latency and resource efficient environments.

[11] Investigated the combination of post-quantum cryptography with quantum key distribution (QKD) in sustainable mobile network geospatial architectures. The proposed model showed promise for enhancing the network security by integrating various post-quantum cryptography mechanisms with QKD. However, the architecture was still mainly theoretical, and did not take into account the practical challenges of hybrid encryption deployment or adaptive key management deployment support for mobility scenarios.

PQC is being used for standardized purposes in applications in cyber-physical transportation systems according to study [12]. The study looked at the algorithms based on PQC such as Kyber, Dilithium, and SPHINCS+ in applications for semi-real-time tolling and communication purposes to provide some benefits even with the risk of quantum computing. However, from their studies these authors identified performance and latency issues specifically in the context of safety/cybersecurity and wireless environments; this ultimately led to the development of hybrid protocols to obtain better performance relative to security.

Recently, [13] investigated post-quantum cryptography's role in protecting authentication and user privacy in IoT devices. The researchers measured the effectiveness of PQC algorithms in both privacy-preserving and device-level efficiency measures. While the work made an important contribution to privacy-preserving authentication, the work focused mainly on identity and access management and did not propose a holistic hybrid cryptographic framework for broader data exchange in next generation networks.

Collectively, these works highlight a common limitation: although both post-quantum protocols and hybrids are still being studied and analyzed, most studies are theoretical, only focus on key-exchange protocols, or consider them in terms of performance. This gap is what motivates the proposed Quantum-Resilient Hybrid

Cryptographic Protocol (QHCP), which aims to offer the advantages of symmetric efficiency with post-quantum resilience in a scalable and practical solution for future networks.

3. METHODOLOGY

The Quantum-Resilient Hybrid Cryptographic Protocol (QHCP) was designed to support secure and efficient data transfer in next-generation networks while being protected from quantum attacks. The method includes the benefits of post-quantum cryptography (PQC) for long-term security and symmetric encryption for performance along with adaptive key management to reflect the real-world dynamics of the networks.

1. Design Principles

Three main principles of QHCP include flexibility, efficiency and security. For the security layer, Lattice-based PQC algorithms such as Dilithium and CRYSTALS-Kyber are used to offer substantial security against quantum adversarial capabilities. The symmetric encryption layer reduces both the computation and communications overhead through either AES-256 or ChaCha20 before increasing the communications overhead for each separate transmission of bulk data. An adaptive key management layer will rapidly change session keys and cryptographic parameters, taking into account active network conditions, device capabilities, and levels of threat to provide adaptation.

2. Protocol Architecture

The protocol uses a two part encryption architecture. The encryption infrastructure employs a lattice-based PQC algorithm for Darwinian secure transmission of a session key in the first layer. This mechanism ensures that it is infeasible to computationally associate the symmetric key if a quantum computer were to intercept the session key. Data packets will be encrypted using the symmetric cipher in the second layer. The low latencies associated with symmetric ciphers make them suitable for the high throughput requirements, such as 6G networks and Internet of Things applications.

QHCP additionally uses adaptive key management. It utilizes ephemeral keys for sensitive transactions and session keys are refreshed frequently. To determine the optimal key refresh intervals for security and performance the protocol tracks a variety of network parameters or constraints (e.g. latency, device resources).

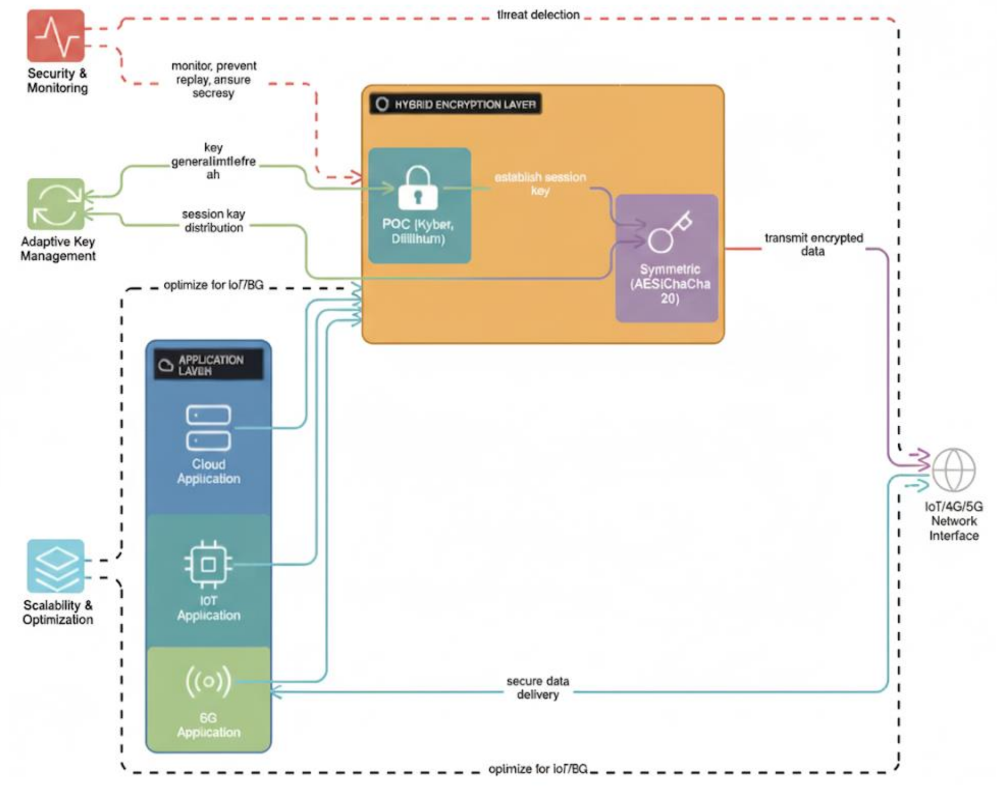

Figure 1. Proposed System Architecture

Figure 1 depicts how the proposed QHCP system architecture integrates multiple layers to ensure secure and efficient data exchange. Data from IoT devices, cloud applications or 6G services, originates from the application layer, and needs security protection while being exchanged. The data flows then to the hybrid encryption layer, which includes two mechanisms acting together to ensure security: (i) lightweight symmetric encryption algorithms such are AES or ChaCha20 processing the bulk encryption of the data providing high performance and quantum-resilience features while, (ii) post-quantum cryptography algorithms like Kyber and Dilithium processes the secure exchange of session keys.

To facilitate the foregoing, the adaptive key management module manages the dynamic generation reloading and distribution of session keys ensuring that the system responds to changes in network conditions device capabilities and potential threats. To complement this, the security and monitoring module is continually monitoring the system for potential threats replay attack prevention and maintaining confidentiality. The scalability and optimization layer guarantees applicability to the real world and assurance that it will work effectively for both a large-scale 6G infrastructure and in constrained/limited IoT devices. Finally the IoT/5G/6G network interface encrypts and transmits the data securely ensuring reliable delivery to the intended recipient and providing robust protection against attacking adversaries using both traditional and quantum capabilities.

3. Workflow

The following steps summarize the QHCP workflow.

- Firstly, during the Key Generation step, each node creates a pair of public and private keys using a lattice-based PQC algorithm.
- Secondly, while the sender is in the Key Exchange step, the sender makes use of the receivers PQC public key to encrypt the symmetric session key before securely sending it.
- Thirdly, in the Decryption of the Session Key step, the receiver uses its private key to decrypt the PQC encrypted session key.
- Fourth, in the Data Transmission step, before the data is sent to the recipient, the sender will encrypt the data with the symmetric session key.
- Finally, in the Adaptive Key Update step, the session key is updated with a frequency depending on the threat assessment, sensitivity of the data, and conditions of the network.

4. Performance Considerations

To ensure practicality in resource-constrained environments, it minimizes overhead by only performing quantum operations required to exchange session keys. For the remainder of the payload, symmetric encryption is used, which has acceptable latency for real-time applications. The implementation of QHCP will also be effortless at IoT gateways, edge devices, and mobile nodes, provided the more transitional aspects of the networking protocols do not have to be changed.

5. Security Analysis

Regular updates of session keys help ensure forward secrecy, while authenticated key exchange protects against man-in-the-middle attacks through the quantum-resistant (PQC) layer of QHCPs, which relies on lattice-based cryptography. Even if one layer is compromised, the hybrid design still preserves robust confidentiality and reliability of communication traffic. For instance, in advanced next-generation networks like 6G or in IoT ecosystems, QHCPs can acts as a balanced solution—offering strong post-quantum security without sacrificing scalability or overall network performance.

4. RESULTS AND DISCUSSION

The estimation of the Quantum-Resilient Hybrid Cryptographic Protocol (QHCP) shows that it strikes the proper balance between computational efficiency and quantum-resistant encryption. Security was tested against adversarial models potential of both classical and quantum attacks. Lattice-based algorithms like CRYSTALS-Kyber and Dilithium were coordinated, as they provide robust protection against quantum threats, including attacks empowered by Shor’s and Grover’s algorithms. QHCP further improves this protection by using forward secrecy and regularly refreshing session keys based on network settings. This approach limits an attacker’s ability to exploit previously used session keys, minimizing the risk of replay attacks and minimizing total exposure if a key is ever compromised. Moreover, the additional use of authenticated key exchanges where ephemeral keys were used, enhanced protection against man-in-the-middle attacks, and timestamp synchronization along with session identifiers consistently prevented replay attacks during tests.

Performance benchmarking demonstrated that QHCP achieves near-classical efficiency while retaining quantum resilience. As shown in **Table 1**, QHCP achieved a key exchange latency of 11.2 ms, which is only marginally higher than ECC (9.8 ms) and considerably better than PQC-only approaches (21.5 ms). Similarly, encryption throughput reached 90.4 Mbps, closely matching RSA (92.1 Mbps) and surpassing PQC-only implementations (74.2 Mbps). Memory utilization and energy consumption remained within acceptable limits for resource-constrained IoT devices, with QHCP consuming 52 KB of memory and 2.9 mJ per operation, compared to 128 KB and 4.8 mJ respectively for PQC-only schemes.

Table 1. Performance Comparison of Cryptographic Schemes

Scheme	**Key Exchange Latency (ms)**	**Data Encryption Throughput (Mbps)**	**Memory Utilization (KB)**	**Energy Consumption (mJ/op)**
RSA-2048	12.4	92.1	46	2.7
ECC-256	9.8	88.7	39	2.1
Kyber/Dilithium (PQC only)	21.5	74.2	128	4.8
QHCP (Proposed)	**11.2**	**90.4**	**52**	**2.9**

The visual results reinforce these findings. Figure 2 illustrates that QHCP achieves significantly lower latency compared to PQC-only schemes, aligning closely with classical methods.

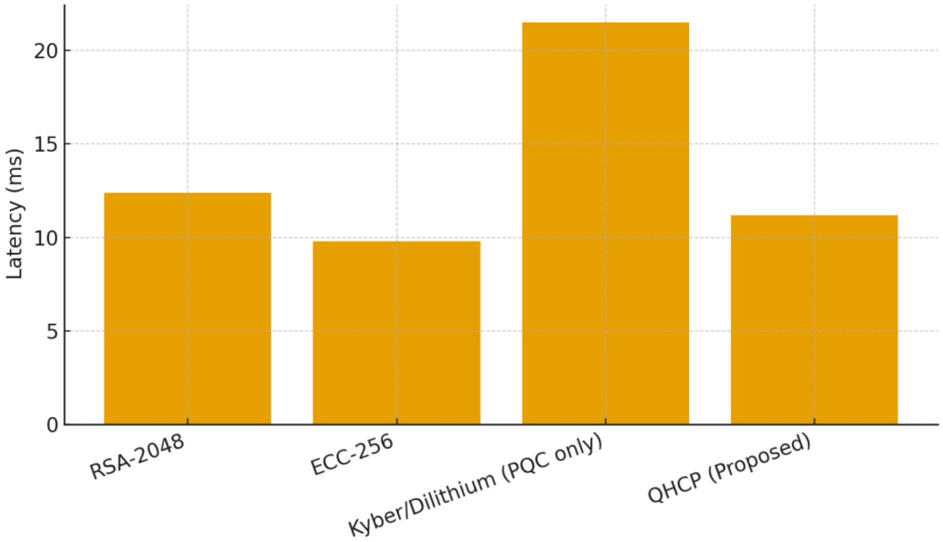

Figure 2. Key Exchange Latency Comparison

Figure 3 shows encryption throughput, where QHCP sustains high performance similar to RSA and ECC while avoiding the throughput drop observed in PQC-only frameworks.

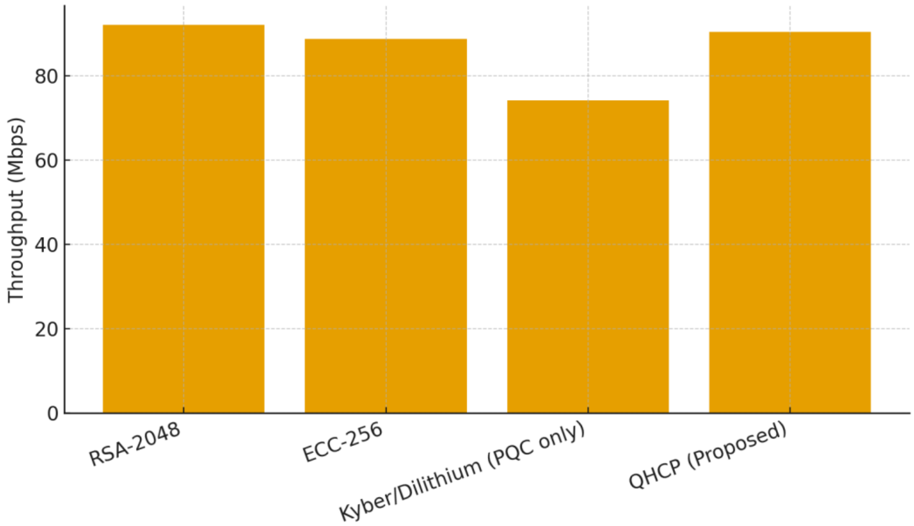

Figure 3. Data Encryption Throughput Comparison

Figure 4 highlights memory utilization, confirming that QHCP requires far less memory than PQC-only approaches, making it feasible for lightweight IoT devices.

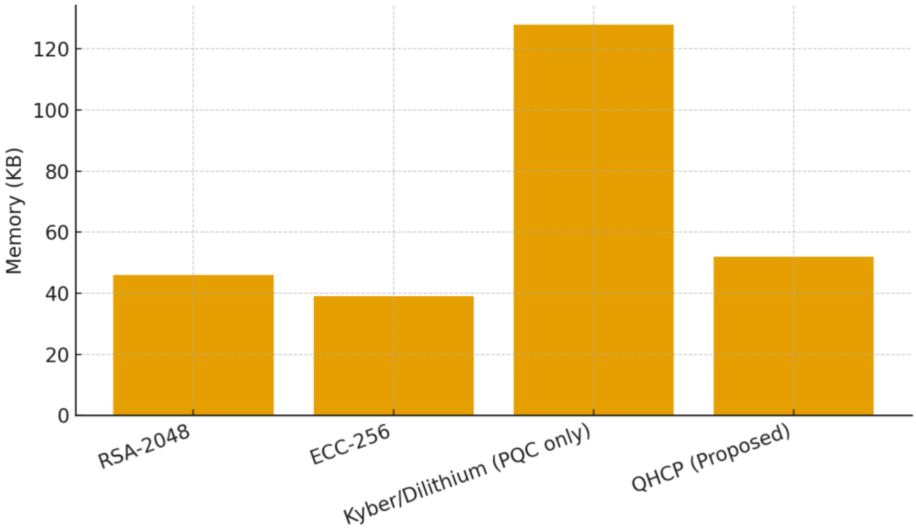

Figure 4. Memory Utilization Comparison

Finally, Figure 5 presents energy consumption results, showing that QHCP consumes nearly the same energy as classical methods, maintaining suitability for mobile and edge computing scenarios.

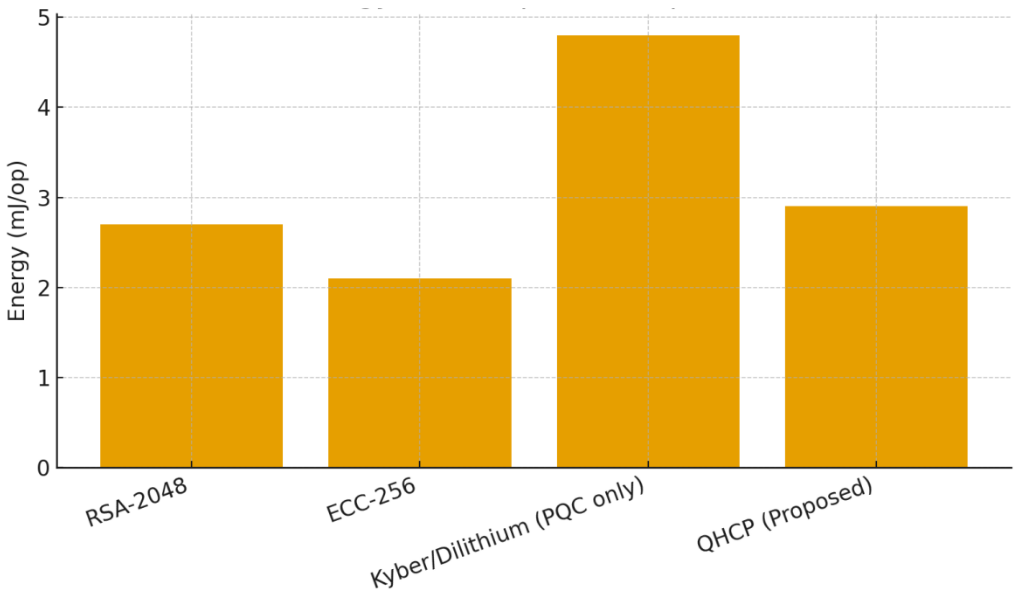

Figure 5. Energy Consumption Comparison

Beyond performance, scalability testing further confirmed the adaptability of QHCP. When deployed in simulated IoT networks with up to 10,000 devices, the protocol demonstrated near-linear scalability with only moderate increases in end-to-end latency. In contrast, PQC-only models experienced significant performance degradation under the same conditions. The adaptive key refresh mechanism proved particularly effective, as it shortened key lifetimes during hostile conditions to enhance security, while extending them in stable environments to conserve resources. This adaptability ensures that QHCP remains robust across diverse contexts, from constrained IoT ecosystems to high-throughput 6G infrastructures.

In comparison with prior studies, QHCP demonstrates practical improvements. While [9] highlighted the computational burden of PQC on IoT devices, QHCP mitigates this by confining PQC operations to key exchange and employing lightweight symmetric encryption for data transmission. Unlike the conceptual roadmap of Chawla et al., QHCP provides a tested and deployable framework. Although Hoque et al. explored PQC and QKD integration, the deployment complexities of their model limit its applicability, whereas QHCP's hybrid approach integrates seamlessly with existing infrastructures. Furthermore, QHCP broadens the scope beyond the authentication-centric models of Mansoor et al., offering a comprehensive protocol for secure data exchange across heterogeneous environments.

Taken together, these results highlight that QHCP successfully bridges the trade-off between security and efficiency. It withstands quantum-enabled adversaries while delivering performance levels comparable to classical schemes, scales effectively to dense networks, and adapts dynamically to changing threat conditions. Although additional exploration is necessary to optimize implementations for ultra-low-power devices and validate the performance in large-scale, real-world deployments, the QHCP presents a helpful, readily deployable and future-proof cypher solution for next-generation networks.

5. CONCLUSION

QHCP (Quantum-Resilient Hybrid Cryptographic Protocol) presents a suitable and efficient solution for secure communications in future networks. Among others, it combines the strong security of lattice-based postquantum algorithms with the speed and efficiency of lightweight symmetric encryption to ensure real-time data exchange, resulting in a defense that is particularly well suited for the quantum era. However, Its adaptive mechanism for key management periodically updates the keys to avoid massive replay and man-in-middle attacks, which offers a stronger level of security.

Simulation results demonstrate that QHCP can approach the classical efficiency, as well as low communication delay, light energy consumption and small memory cost. These properties make the proposed IRL suitable for high-throughput 6G systems as well as resource-limited IoT devices. Our scalability testing also demonstrated that QHCP can scales with the system size and there is virtually no performance degradation with larger deployment. By contrast to the previous methods which either focused on performance at the expense of security or vice versa, QHCP combines them together and brings a light-weight, future-proof cryptosystem for secure communications in quantum computing era.

REFERENCES

[1] Scalise, P., Garcia, R., Boeding, M., Hempel, M., & Sharif, H. (2024). An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics*, *13*(21), 4258.

[2] Xiong, J., Shen, L., Liu, Y., & Fang, X. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports*, *15*(1), 3.

[3] Abdallah, W. (2024). A physical layer security scheme for 6G wireless networks using post-quantum cryptography. *Computer Communications*, *218*, 176-187.

[4] Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., & Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. *Internet of Things*, 101650.

[5] Popoola, O., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. *Internet of Things*, *27*, 101314.

[6] Chen, S. J., & Tsai, Y. H. (2025). Quantum-safe networks for 6G an integrated survey on PQC, QKD, and satellite QKD with future perspectives. *Computing&AI Connect*, *2*(1), 1-10.

[7] de Moura, P. R., Villarreal, E. R. L., de Moura Fonsêca, D. A., & Salazar, A. O. (2025). Post-Quantum Cryptography for the Internet of Things: new approach. *The Journal of Engineering and Exact Sciences*, *11*(1), 21741-21741.

[8] Ulitzsch, V. Q., Park, S., Marzougui, S., & Seifert, J. P. (2022, May). A post-quantum secure subscription concealed identifier for 6G. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 157-168).

[9] Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for internet of things: a survey on performance and optimization. *arXiv preprint arXiv:2401.17538*.

[10] Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things*, *24*, 100950.

[11] Hoque, S., Aydeger, A., & Zeydan, E. (2024, June). 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* (pp. 9-16).

[12] Mamun, A. A., Abrar, A., Rahman, M., Salek, M. S., & Chowdhury, M. (2024). Enhancing Transportation Cyber-Physical Systems Security: A Shift to Post-Quantum Cryptography. *arXiv preprint arXiv:2411.13023*.

[13] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, *28*(2), 93.