engineering proceedings

MDPI

Proceeding Paper

Lightweight Post-Quantum Cryptography: Applications and Countermeasures in Internet of Things, Blockchain, and E-Learning †

Chin-Ling Chen [1,2], Kuang-Wei Zeng [3], Wei-Ying Li [4], Chin-Feng Lee [3], Ling-Chun Liu [5,*] and Yong-Yuan Deng [2,*]

[1] School of Information Engineering, Changchun Sci-Tech University, Changchun 130022, China; clc@mail.cyut.edu.tw
[2] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan
[3] Department of Information Management, Chaoyang University of Technology, Taichung 41349, Taiwan; s11314903@gm.cyut.edu.tw (K.-W.Z.); lcf@cyut.edu.tw (C.-F.L.)
[4] Administration Department YingShun Technology Co., Ltd., Taichung 412018, Taiwan; totoro@y-shun.com.tw
[5] Department of Computer Information and Network Engineering & Master Program, Lunghwa University of Science and Technology, Taoyuan City 33326, Taiwan
* Correspondence: 0287yell@gmail.com (L.-C.L.); allendeng@cyut.edu.tw (Y.-Y.D.)
† Presented at the 8th Eurasian Conference on Educational Innovation 2025, Bali, Indonesia, 7–9 February 2025.

Abstract

With the rapid advancement of quantum computing technology, traditional encryption methods are encountering unprecedented challenges in the Internet of Things (IoT), blockchain systems, and digital learning (e-learning) platforms. Therefore, we systematically reviewed the applications and countermeasures of lightweight post-quantum cryptographic techniques, focusing on the requirements of resource-constrained IoT devices and decentralized systems. We compared the encryption methods based on ring learning with errors (Ring-LWE), Binary Ring-LWE, ring-ExpLWE, the collaborative critical generation framework Q-SECURE, and hardware accelerators for the CRYSTALS-dilithium digital signature scheme. According to the high security and efficiency demands for data transmission and user interaction in e-learning platforms, we developed lightweight encryption schemes. By reviewing existing research achievements, we analyzed the application challenges in IoT, blockchain, and e-learning scenarios and explored strategies for optimizing post-quantum encryption schemes for effective deployment.

Keywords: lightweight post-quantum cryptography; e-learning; internet of things (IoT); blockchain; ring learning with errors (Ring-LWE)

check for updates

Academic Editors: Teen-Hang Meen, Chun-Yen Chang and Cheng-Fu Yang

Published: 12 August 2025

Citation: Chen, C.-L.; Zeng, K.-W.; Li, W.-Y.; Lee, C.-F.; Liu, L.-C.; Deng, Y.-Y. Lightweight Post-Quantum Cryptography: Applications and Countermeasures in Internet of Things, Blockchain, and E-Learning. *Eng. Proc.* **2025**, *103*, 14. https://doi.org/10.3390/engproc2025103014

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The advancement of quantum computing technology poses unprecedented challenges to cryptographic systems. Through powerful parallel processing capabilities [1], quantum computers have the potential to rapidly compromise traditional public-key encryption methods such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), which are currently widely deployed in network communications and data protection [2]. Quantum computing utilizing Shor's algorithm might breach conventional public-key systems in hours [3], placing quantum-resistant encryption on a critical focus in contemporary cryptography.

Post-quantum cryptography (PQC) has emerged as a promising solution to address quantum computing threats. Lattice-based encryption methods, particularly ring learning with errors (Ring-LWE) and its variant Ring-ExpLWE [4,5], have garnered significant attention due to their security properties and computational efficiency. The Post-Quantum Cryptography Standardization Program of the National Institute of Standards and Technology has progressed to its final phase, identifying several promising algorithmic candidates, including CRYSTALS-Kyber proposed by Avanzi et al. [6] and CRYSTALS-Dilithium proposed by Bai et al. [7]. These algorithms demonstrate theoretical security guarantees and practical performance advantages.

With the proliferation of e-learning platforms in education, securing learners' data has become increasingly crucial [8]. E-learning systems rely on real-time data transmission and user interaction to deliver personalized learning experiences, which require secure and efficient encryption technologies [8]. Vulnerable to quantum threats, traditional encryption schemes can compromise future data protection requirements for e-learning platforms. Blockchain technology, dependent on cryptographic methods for transaction security and data integrity, requires encryption to maintain low latency while providing high resistance to attacks due to its public ledger characteristics [9]. Vulnerable to quantum threats, traditional encryption needs to meet future data protection requirements for e-learning platforms [10], making traditional encryption schemes like RSA or ECC implementations impractical [11]. At the same time, diverse contemporary cryptography has been proposed for computationally efficient algorithms [12]; quantum computing further threatens the security of these devices by potentially nullifying existing encryption methods.

We investigated the impact of quantum computing technology on existing encryption systems, focusing on threats to IoT devices reliant on public critical systems in this study. Quantum computational capabilities render current network communication protocols obsolete, further jeopardizing personal data privacy and corporate confidentiality. Thus, understanding quantum computing's potential implications for network security and developing quantum-resistant encryption is paramount. Given the hardware resource constraints of IoT devices, implementing effective post-quantum encryption schemes on these devices emerges as an important research topic. In this study, we evaluated various post-quantum encryption algorithms applicable to resource-constrained systems, specifically examining lattice-based encryption methods such as Ring-ExpLWE, Binary Ring-LWE, and Lightweight Ring-LWE [4,5,13,14].

2. Current Research

2.1. Lattice-Based Encryption

Lattice-based cryptography represents one of the most promising PQCs. These methods rely on computationally intractable lattice problems, with learning with errors (LWE) being a notable variant. Ring-LWE, an extension of LWE, incorporates minor random errors into linear equations to enhance the complexity of the problem. Ring-LWE extends LWE by applying polynomial rings with minor random errors and rendering them resistant to efficient quantum computer attacks. Notably, Binary Ring-LWE (BRLWE) and ring learning with exponential errors (Ring-ExpLWE) demonstrate their potential in IoT applications. Lightweight encryption schemes based on BRLWE have been proposed to optimize the complexity of polynomial computation for devices with limited resources [11,14]. Ma et al. [11] emphasized resilience against side-channel attacks, which is crucial for medical and industrial IoT deployments. Ring-ExpLWE, a Ring-LWE variant, employs an exponential distribution for error vector generation, superseding the binary distribution in Ring-BinLWE. This method has significantly improved encryption/decryption performance through optimization for resource-limited platforms such as Cortex-M3 [5].

2.2. Collaborative Computing and Distributed Cryptography

Network-based collaborative computing architectures have been proposed to address computational bottlenecks in post-quantum key generation on single devices. These approaches enable resource-constrained IoT devices to leverage network-wide computational capabilities for key generation. Yavuz et al. [15] introduced a scalable collaborative computing framework that facilitates efficient post-quantum key generation for IoT devices. This method accelerates generation by distributing computational load, although its effectiveness significantly depends on network stability and device availability. Q-SECURE further advances collaborative computing concepts. Ngouen [16] proposed a "Client-Helpers" architecture, enabling dynamic allocation of network computational resources for IoT devices. This innovation allows low-power devices to participate in post-quantum cryptographic operations, enhancing overall cryptographic security.

2.3. Post-Quantum Digital Signature Technology

Digital signatures are important for ensuring data integrity and authentication in IoT devices. Quantum-resistant digital signature schemes must maintain high security while minimizing resource consumption. Gupta [17] proposed a hardware accelerator for the CRYSTALS-Dilithium digital signature scheme. This accelerator significantly improves signature generation and verification speeds on field-programmable gate array (FPGA) and application-specific integrated circuit (ASIC) platforms through optimized polynomial operations and efficient integration of hardware modules, emerging as a strong candidate for IoT applications.

3. Applications and Challenges

3.1. Applications in IoT

The IoT technology has been widely applied in smart homes, medical devices, and industrial automation. The proliferation of these devices has increased the demand for data security and privacy, further exacerbated by the emerging threat of quantum computing [3]. Lightweight post-quantum cryptographic techniques, such Binary Ring-LWE and Ring-ExpLWE, are appropriate for resource-constrained IoT devices due to their ability to provide high security under limited computational and energy conditions [4,5].

Despite the theoretical quantum resistance of lattice-based cryptography, implementing such technologies in IoT environments presents significant challenges. IoT devices operate under constraints of low power consumption, limited computational capacity, and restricted storage resources, making it challenging to deploy encryption schemes with high computational demands [11]. Despite the theoretical quantum resistance of lattice-based cryptography, implementing such technologies in IoT environments presents significant challenges. IoT devices typically operate under constraints of low power consumption, limited computational capacity, and restricted storage resources, making it challenging to deploy encryption schemes with high computational demands [14]. This issue is particularly pronounced in medical and industrial applications, where devices face stricter requirements for power efficiency and response times [16].

Solutions to address these challenges have been established, including hardware acceleration techniques such as FPGA and ASIC accelerators to enhance computation speed and reduce power consumption [17]. Additionally, collaborative key generation architectures, such as Q-SECURE [16], allow IoT devices to share computational resources within a network, alleviating the computational burden on individual devices. This collaborative approach improves efficiency and security during the critical generation process. Table 1 summarizes techniques and challenges encountered in the PQC era for IoT devices.

Table 1. PQC in IoT.

Year	Author	Technologies	Solution	Challenges in PQC
2024	Koblitz et al. [4]	Binary Ring Learning With Errors (Binary Ring-LWE)	Offers a lightweight scheme for resource-constrained IoT	Balancing minimal resource use with robust quantum resistance
2022	Xu et al. [5]	Ring exponential learning with errors (Ring-ExpLWE)	Enhances encryption/decryption efficiency on limited devices	Managing increased key sizes and computational overhead
2024	Ma et al. [11]	Lightweight post-quantum cryptosystem based on Binary Ring-LWE	Improves security and side-channel resilience on IoT devices	Integrating advanced security within strict resource limits
2024	Ahmadunnisa & Mathe [14]	Lightweight Binary Ring-LWE architecture (CNC)	Reduces computational demand in IoT encryption schemes	Overcoming performance constraints on low-resource hardware
2023	Ngouen et al. [16]	Q-SECURE collaborative key generation architecture	Distributes key generation load among IoT devices	Ensuring secure and efficient coordination in distributed systems
2023	Gupta et al. [17]	Hardware accelerators (FPGA/ASIC) for CRYSTALS-Dilithium	Speeds up digital signature operations while lowering power use	Addressing increased computational costs and signature sizes

3.2. Applications in Blockchain

Blockchain technology relies on cryptographic mechanisms to ensure the security of its transactions and the integrity of its ledger. Due to its public ledger, blockchain systems demand encryption that exhibits strong resistance to attacks and maintains low latency to preserve performance [10]. With advances in quantum computing, traditional encryption methods such as RSA and ECC face the potential risk of being compromised, posing a significant threat to blockchain security [3].

To implement post-quantum cryptographic techniques on the blockchain, the associated computational and resource demands must be accounted for. PQC signature schemes such as CRYSTALS-Dilithium provide high security but introduce significant computational overhead, resulting in transaction verification delays and system performance degradation [7,17]. Furthermore, blockchain consensus mechanisms and smart contract operations require seamless integration of post-quantum encryption to ensure both efficiency and security [16].

Researchers developed lightweight post-quantum digital signature schemes, such as SPHINCS+, utilizing hash-based designs to reduce resource consumption [17]. Distributed computation and hierarchical signature structures improve signature verification speeds, reduce transaction delays, and improve blockchain efficiency [15]. These optimization strategies enhance the usability of blockchains in quantum environments without compromising security. To elucidate the various techniques and challenges encountered in the PQC era for blockchain, we list related issues in Table 2.

Table 2. PQC techniques and their challenges.

Year	Author	Technologies	Solution	Challenges in PQC
2021	Bai et al. [7]	CRYSTALS-Dilithium digital signature scheme	Enhances blockchain security; however, high computational overhead may delay transaction verification	High computational complexity and latency; implementation challenges in resource-constrained settings
2023	Gupta et al. [17]	SPHINCS+ lightweight digital signature scheme	Reduces resource consumption via a hash-based design	Requires further validation of maturity and stability; balance between security and efficiency remains a challenge
2023	Ngouen et al. [16]	Integration of PQC in blockchain consensus and smart contracts	Balances security with system efficiency	Compatibility issues with existing architectures; technical challenges in development and deployment
2023	Yavuz et al. [15]	Distributed computing and hierarchical signature architecture	Improves signature verification speed and reduces transaction delays	Dependence on stable network conditions; potential issues with network latency and resource coordination

3.3. Application in E-Learning

With the widespread adoption of e-learning platforms, data security has become a key requirement to protect the privacy of learners and the integrity of educational content [18]. These platforms rely on real-time data transmission and interactive functionalities that must address potential quantum computing threats. Traditional RSA and ECC are insufficient in providing adequate protection in a quantum environment [3].

E-learning platforms must balance high security with real-time interaction capabilities between students and educators while maintaining low latency and high efficiency. These platforms involve frequent data exchanges and user authentication processes [19]. The computational demands of post-quantum cryptographic techniques pose resource challenges in such environments, potentially impairing the effectiveness of real-time interactions. To meet the requirements of e-learning platforms, researchers have proposed lightweight post-quantum cryptographic solutions, such as optimized Ring-LWE and CRYSTALS-Dilithium digital signature schemes [5,15]. Collaborative computation architectures and cloud-based encryption technologies can distribute computational loads, reduce pressure on endpoint devices, and balance security and performance.

In addition, post-quantum digital signature schemes such as CRYSTALS-Dilithium and SPHINCS+ provide secure and verifiable communication for critical e-learning scenarios, including online assessments, certificate issuance, and authenticated submissions, where data integrity and non-repudiation are essential [7,17,18]. Learning analytics, involved in the collection and analysis of behavioral and performance data, can also benefit from PQC-secured channels and privacy-preserving encryption, ensuring student data confidentiality under quantum threat models [19]. These post-quantum mechanisms allow e-learning platforms to have long-term resilience against quantum-enabled attacks while maintaining trust, efficiency, and compliance in future digital learning environments.

4. Conclusions

We examined multiple PQC technologies applicable to IoT devices and explored novel solutions to address the potential threats posed by quantum computing. High-security and resource-optimized application scenarios are applied to IoT, blockchain, and e-learning. The significant potential of PQC technologies was verified to resist quantum attacks while also underscoring the challenges associated with computational resource consumption, implementation costs, and technical standardization. E-learning platforms demand real-time data transmission and interactive user engagement while ensuring data integrity and privacy. It requires encryption to prioritize both efficiency and security. The application of PQC in such platforms safeguards user data against quantum computing threats and enhances the overall reliability and transparency of the system.

Utilizing a decentralized ledger technology, blockchain's high demands for security and privacy position itself as an essential tool for PQC applications. It is necessary to develop more lightweight and efficient post-quantum cryptographic schemes to meet the needs of resource-constrained devices within distributed networks, such as e-learning, IoT, and blockchain systems. Technological innovation and interdisciplinary collaboration enable the widespread adoption of post-quantum cryptographic technologies across various industries as a robust security tool.

Author Contributions: Conceptualization, C.-L.C. and K.-W.Z.; Methodology, K.-W.Z.; Software, K.-W.Z.; Validation, C.-L.C., K.-W.Z. and W.-Y.L.; Formal analysis, K.-W.Z.; Investigation, K.-W.Z.; Resources, C.-L.C.; Data curation, K.-W.Z.; Writing—original draft preparation, K.-W.Z.; Writing—review and editing, C.-L.C.; Visualization, C.-L.C.; Supervision, C.-F.L., L.-C.L. and Y.-Y.D.; Project administration, C.-F.L.; Funding acquisition, W.-Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the YingShun Technology Co., Ltd., Taiwan, under the Grant number of Chaoyang University of Technology: 15454. This work was supported by the National Science and Technology Council (NSTC), Taiwan, under NSTC Grant numbers: 112-2410-H-324 -001 -MY2.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare that this study received funding from Administration Department YingShun Technology Co., Ltd. The funder was not involved in the study design, collection, analysis, interpretation of data, the writing of this article or the decision to submit it for publication. The authors declare no conflicts of interest.

References

1. Kumar, M.; Mondal, B. Study on Implementation of Shor's Factorization Algorithm on Quantum Computer. *SN Comput. Sci.* **2024**, *5*, 413. [CrossRef]
2. Mustafa, I.; Khan, I.U.; Aslam, S.; Sajid, A.; Mohsin, S.M.; Awais, M.; Qureshi, M.B. A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications. *IEEE Access* **2020**, *8*, 99273–99285.
3. Biswas, S.; Das, P. Analysis of Quantum Cryptology and the RSA Algorithms Defense Against Attacks Using Shor's Algorithm in a Post Quantum Environment. In *Proceedings of the 5th International Conference, CICBA 2023, Kalyani, India, 27–28 January 2023*; Communications in Computer and Information Science (CCIS); Springer: Cham, Switzerland, 2024; Volume 1956.
4. Koblitz, N.; Samajder, S.; Sarkar, P.; Singha, S. Concrete Analysis of Approximate Ideal-Sivp to Decision Ring-Lwe Reduction. *Adv. Math. Commun.* **2024**, *18*, 1216–1258. [CrossRef]
5. Xu, D.; Wang, X.; Hao, Y.; Zhang, Z.; Hao, Q.; Jia, H.; Dong, H.; Zhang, L. Ring-ExpLWE: A High-Performance and Lightweight Post-Quantum Encryption Scheme for Resource-Constrained IoT Devices. *IEEE Internet Things J.* **2022**, *9*, 24122–24134. [CrossRef]

6. Avanzi, R.; Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation (version 3.01). 2021. Available online: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf (accessed on 31 January 2025).
7. Bai, S.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (version 3.1). 2021. Available online: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (accessed on 31 January 2025).
8. Akacha, S.A.-L.; Awad, A.I. Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability* **2023**, *15*, 14132. [CrossRef]
9. Lamriji, Y.; Makkaoui, K.E.; Beni-Hssane, A. Towards fast ECC signing algorithms for Blockchain. In Proceedings of the 5th International Conference on Networking, Information Systems, and Security: Envisage Intelligent Systems in 5G/6G-Based Interconnected Digital Worlds (NISS 2022), Bandung, Indonesia, 30–31 March 2022.
10. Mishra, S.; Mondal, B.; Jha, R.K. Lightweight Authentication Scheme Based on ECC for IoT. *SN Comput. Sci.* **2024**, *5*, 949. [CrossRef]
11. Ma, C.; Shankar, A.; Kumari, S.; Chen, C.M. A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security. *Internet Things* **2024**, *28*, 101391. [CrossRef]
12. Al-Neami, I.A.; Hameed, Z.S.; Al-Zubaydi, Z.A. Adaptive FPGA-Based Intrusion Detection System for Real-Time Internet of Things Security. *J. Intell. Syst. Internet Things* **2025**, *14*, 278–292.
13. Bao, T.; He, P.; Bai, S.; Xie, J. TINA: TMVP-Initiated Novel Accelerator for Lightweight Ring-LWE-Based PQC. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2024**, *32*, 870–882. [CrossRef]
14. Ahmadunnisa, S.; Mathe, S.E. CNC: A lightweight architecture for Binary Ring-LWE based PQC. *Microprocess. Microsyst.* **2024**, *106*, 105044. [CrossRef]
15. Yavuz, A.A.; Darzi, S.; Nouma, S.E. Lightweight and Scalable Post-Quantum Authentication for Medical Internet of Things. *arXiv* **2023**, arXiv:2311.18674.
16. Ngouen, M.; Rahman, M.A.; Prabakar, N.; Uluagac, S.; Njilla, L. Q-SECURE: A Quantum Resistant Security for Resource Constrained IoT Device Encryption. In Proceedings of the 2023 10th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2023, San Antonio, TX, USA, 23–25 October 2023; pp. 141–148.
17. Gupta, N.; Jati, A.; Chattopadhyay, A.; Jha, G. Lightweight Hardware Accelerator for Post-Quantum Digital Signature CRYSTALS-Dilithium. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2023**, *70*, 3234–3243. [CrossRef]
18. Almufairej, A.; Binghaith, L.; Alshareef, D.; Jamail, N.S.M. Cyber Security Risk Management: E-Learning System. In Proceedings of the 2022 5th International Conference of Women in Data Science at Prince Sultan University, WiDS-PSU 2022, Riyadh, Saudi Arabia, 28–29 March 2022; pp. 146–149.
19. Wu, D. Design and Construction of Digital Network Learning Platform for Artificial Intelligence. In Proceedings of the 2023 IEEE International Conference on Paradigm Shift in Information Technologies with Innovative Applications in Global Scenario (ICPSITIAGS), Indore, India, 28–29 December 2023; pp. 106–110.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.