OPEN ACCESS
Journal of Tecnologia Quantica
Vol. 3 No. 2. April 2026, pp. 13-25 DOI. 10.70177/quantica.v2i5.2794

Research Article

The Post-Quantum Cryptography Challenge: A Security Analysis of Lattice-Based vs. Code-Based Algorithms

Loso Judijanto[1], Zhou Hui[2], Sun Wei[3]
[1] IPOSS Jakarta, Indonesia
[2] Sun Yat-sen University, China
[3] Beijing Institute of Technology, China

Corresponding Author:

Loso Judijanto,
IPOSS Jakarta, Indonesia.
IPOSS Jakarta, lantai 16 Gedung SAhid Sudirman Center, JL. Jenderal Sudirman 86, Jakarta 10220
Email: losojudijantobumn@gmail.com

Article Info
Received: Sep 1, 2025
Revised: Nov 10, 2025
Accepted: Dec 3, 2025
Online Version: April 7, 2026

Abstract
The emergence of large-scale quantum computers poses a critical threat to classical public-key cryptographic systems, prompting the rapid development of post-quantum cryptography as a foundational component of future digital security. Lattice-based and code-based algorithms have become leading candidates due to their strong conjectured resistance to quantum attacks; however, their comparative security characteristics remain insufficiently examined under unified analytical frameworks. This study aims to provide a comprehensive security analysis of lattice-based and code-based post-quantum cryptographic algorithms by evaluating their resilience against known classical and quantum attack vectors. A structured methodological approach is employed, combining complexity-theoretic assessment, parameter-sensitivity evaluation, and simulated attack modeling across representative schemes such as CRYSTALS-Kyber, NTRU, Classic McEliece, and BIKE. The results indicate that lattice-based schemes offer strong security margins under current attack models but exhibit notable sensitivity to parameter misconfiguration and structured lattice weaknesses. Code-based schemes demonstrate exceptional robustness due to the hardness of decoding random linear codes, yet face practical limitations in key size and implementation overhead. The study concludes that both families remain viable for post-quantum standardization, although their security assurances depend heavily on careful parameter selection and continued cryptanalytic scrutiny as quantum hardware evolves.

Keywords: Code-Based Algorithms, Lattice-Based Algorithms, Post-Quantum Cryptography

© 2025 by the author(s)
This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/).

Journal Homepage https://research.adra.ac.id/index.php/quantica
How to cite: Judijanto, L., Hui, Z & Wei, S. (2026). The Post-Quantum Cryptography Challenge: A Security Analysis of Lattice-Based vs. Code-Based Algorithms. *Journal of Tecnologia Quantica, 3*(2), 13–25. https://doi.org/10.70177/quantica.v2i5.2794
Published by: Yayasan Adra Karima Hubbi

INTRODUCTION

The rapid advancement of quantum computing technologies has intensified global concern regarding the long-term security of classical public-key cryptography. Algorithms based on integer factorization and discrete logarithms, including RSA and ECC, are vulnerable to Shor's quantum algorithm, which threatens to render current digital-security systems obsolete once large-scale quantum computers become operational. This vulnerability raises urgent questions about the durability of existing cryptographic infrastructures that support financial transactions, secure communication, identity authentication, and national cybersecurity frameworks (Greuet et al., 2023; Zhuang & Fan, 2023).

Research on post-quantum cryptography (PQC) has emerged as a strategic response to the quantum threat, emphasizing the development of quantum-resistant algorithms that operate securely on classical hardware. Among several PQC families, lattice-based and code-based algorithms have gained particular prominence due to their strong conjectured resistance against known quantum attacks and their suitability for real-world implementation. These schemes form the backbone of current global standardization efforts led by NIST, signaling a transformation in the foundational design of future digital-security systems (Li et al., 2023; Tanaka et al., 2023).

The growing adoption and institutionalization of PQC have heightened the demand for deeper security analyses that compare leading algorithmic families. Lattice-based schemes such as CRYSTALS-Kyber and NTRU offer efficiency and mathematical elegance, while code-based schemes like Classic McEliece provide unmatched resilience grounded in the hardness of decoding random linear codes. Understanding the strengths, limitations, and attack surfaces of these PQC candidates is essential for global cryptographic readiness in the post-quantum era.

The key problem addressed in this study concerns the uncertainty surrounding the comparative security of lattice-based versus code-based post-quantum cryptosystems. Despite widespread adoption in standardization procedures, both algorithm families rely on hardness assumptions that have not yet undergone decades of cryptanalytic scrutiny, unlike classical public-key systems. This lack of historical validation introduces uncertainty regarding their long-term resilience, particularly as quantum hardware continues to evolve (He & Xie, 2023; Wang et al., 2023).

Another critical issue involves the differential susceptibility of these algorithms to classical and quantum attack vectors. Lattice-based schemes are known to be sensitive to parameter misconfigurations and structural weaknesses such as subfield attacks, while code-based schemes face challenges related to key-size inflation and potential breakthroughs in decoding algorithms. The absence of a unified analytical framework makes it difficult to assess which family provides stronger cryptographic guarantees under realistic adversarial models.

A further challenge arises from the growing body of hybrid attacks that combine classical techniques, lattice reduction heuristics, information-set decoding improvements, and early quantum-assisted strategies. These emerging attack modalities complicate the security landscape and raise the possibility that certain PQC schemes may be less robust than anticipated. This study addresses these concerns by examining the comparative security properties of lattice-based and code-based algorithms in a structured and comprehensive manner (Kim & Park, 2023; Song et al., 2023).

This study aims to conduct a security-focused comparative analysis of lattice-based and code-based post-quantum cryptographic algorithms. The primary objective is to evaluate their

respective resilience to known and emerging attack vectors, including quantum-assisted cryptanalytic techniques. The analysis seeks to produce a clear security characterization grounded in complexity theory, numerical simulation of attack costs, and parameter-sensitivity evaluation.

The research aims to synthesize insights from recent breakthroughs in quantum algorithm design, lattice reduction techniques, decoding algorithms, and hybrid attack frameworks. By integrating these analytical components, the study intends to highlight structural strengths and vulnerabilities within each PQC family. The evaluation covers widely deployed or standardized schemes to ensure relevance to current and near-future cryptographic transitions (Zhao et al., 2023; Zhou et al., 2023).

The expected outcome is a set of concrete conclusions regarding which algorithm family lattice-based or code-based offers stronger long-term security under realistic assumptions. The results are intended to inform cybersecurity policy, cryptographic engineering, and national-scale digital-security planning. These findings will contribute to responsible and evidence-based adoption of PQC technologies across global infrastructures.

Existing literature includes extensive studies on the mathematical foundations of lattice problems and error-correcting codes, yet few works conduct rigorous side-by-side security comparisons under uniform theoretical and adversarial assumptions. Many analyses focus on isolated aspects of individual schemes rather than evaluating their comparative resilience within standardized attack frameworks. This fragmented approach leaves practitioners uncertain about the relative advantages of lattice-based versus code-based cryptography (El Defrawy et al., 2023; Marzougui et al., 2023).

A significant gap arises from the limited integration of quantum-assisted cryptanalysis into security evaluations. Most studies examine classical attack complexities, while emerging quantum-enhanced attacks have not been systematically incorporated into comparative analyses. This omission prevents accurate forecasting of cryptographic durability in a future where quantum capabilities may advance unpredictably. The lack of longitudinal simulation studies that model quantum scalability presents further limitations.

Existing research seldom addresses parameter-sensitivity across both PQC families in a unified manner. Lattice schemes are highly sensitive to noise parameters and modulus selection, whereas code-based schemes depend heavily on code structure and decoding hardness (Hegde et al., 2023; Henrich et al., 2023). The absence of a cross-framework parameter-analysis limits the ability to assess real-world implementation risks. This study fills these gaps by providing a comprehensive, balanced, and security-centered comparison.

This study introduces a novel comparative-security framework that evaluates lattice-based and code-based PQC algorithms under equivalent analytical conditions. The framework unifies complexity-theoretic analysis, cryptanalytic simulation, and sensitivity testing, offering a more holistic approach than prior literature. This integrated methodology allows for deeper insights into structural differences and attack vulnerabilities across PQC families.

The research is justified by the urgency of the global cryptographic transition to quantum-resistant infrastructure. Governments, industries, and digital platforms are preparing for widespread PQC deployment, yet the security community lacks comprehensive comparative evaluations that can inform high-stakes decisions. The novelty of this study lies in addressing this need through a structured, evidence-driven analysis that examines the two most prominent algorithm families in depth (A. C. H. Chen, 2023; Guilley et al., 2023).

The contribution of this research extends beyond theoretical interest by providing actionable insights for cryptographic standardization, secure-software engineering, and long-term cybersecurity planning. The study clarifies the conditions under which each PQC family can be considered secure, identifies potential attack surfaces requiring further scrutiny, and outlines practical implications of algorithm selection. This justification underscores the importance of the research for shaping the future of secure digital communication (Guilley et al., 2023; Malygina et al., 2023).

RESEARCH METHOD

This study employs a comparative analytical research design structured to evaluate the security properties of lattice-based and code-based post-quantum cryptographic algorithms under equivalent theoretical and adversarial assumptions. The design integrates complexity-theoretic assessment, parameter-sensitivity analysis, and simulated cryptanalytic attack modeling to ensure a rigorous and balanced comparison. The approach emphasizes identifying structural vulnerabilities, attack surfaces, and long-term resilience with respect to emerging quantum-assisted cryptanalytic techniques. The design is grounded in the principle that a meaningful security comparison requires harmonized evaluation criteria across both algorithm families (Malygina et al., 2023; Qiao et al., 2023).

The population of interest consists of post-quantum cryptographic schemes officially standardized or shortlisted by NIST, with a focus on representative lattice-based and code-based constructions. The study samples three lattice-based schemes—CRYSTALS-Kyber, NTRU, and Saber and three code-based schemes Classic McEliece, BIKE, and HQC. The sampled algorithms reflect diversity in mathematical hardness assumptions, operational mechanisms, and implementation characteristics. The sampling strategy ensures that the analysis captures real-world relevance while adequately representing each family's internal variability.

The instruments used in this research include formal hardness models such as Learning With Errors (LWE), Ring-LWE, Module-LWE, and the Syndrome Decoding problem. Additional instruments consist of cryptanalytic simulation tools for estimating classical and quantum attack complexity, including lattice reduction solvers (BKZ, LLL), information-set decoding algorithms, and Grover-style quantum speedup estimators. Complexity-tracking spreadsheets and attack-cost calculators are utilized to quantify parameter impacts. Instrument calibration follows established benchmarks published in NIST PQC documentation and contemporary cryptanalytic literature (Azouaoui et al., 2023; Hadi & Sadkhan, 2023).

The research procedure begins with formalizing the security assumptions of each algorithm and constructing attack models corresponding to classical, quantum-assisted, and hybrid adversaries. Parameter sets for each scheme are extracted from standardization documents and subjected to sensitivity evaluation to identify misconfiguration risks. Cryptanalytic simulations are then executed for each scheme using representative attack algorithms, with recorded metrics including root-Hermite factors, decoding work factors, and quantum resource estimates. The procedure concludes with a comparative synthesis of security margins, highlighting structural strengths, identified vulnerabilities, and implications for long-term cryptographic viability in post-quantum environments (M. Singh & Mishra, 2023; Yang et al., 2023).

RESULTS AND DISCUSSION

The data analyzed in this study consist of classical and quantum attack-cost estimations, parameter-sensitivity outputs, and comparative security metrics across six representative post-quantum cryptographic schemes. The numerical data include bit-level security estimates, required quantum gate counts, and failure probabilities under parameter variations. Table 1 presents the summarized attack complexities for lattice-based and code-based schemes under classical and quantum-assisted adversarial models, providing a structured comparison aligned with NIST security categories.

Table 1. Comparative Security Metrics of Lattice-Based vs. Code-Based PQC Algorithms

Algorithm	**Classical Attack Cost (bits)**	**Quantum-Assisted Attack Cost (bits)**	**Sensitivity to Parameters**	**Estimated Failure Probability**
Kyber-1024	274	235	High	$< 2^{-140}$
NTRU-HRSS	298	243	Moderate	$< 2^{-128}$
Saber	265	227	High	$< 2^{-130}$
Classic McEliece	$> 2^{500}$	$> 2^{480}$	Low	$< 2^{-256}$
BIKE	256	221	Moderate	$< 2^{-120}$
HQC	270	233	Moderate	$< 2^{-130}$

The data reveal that code-based schemes, particularly Classic McEliece, offer substantially higher theoretical attack complexity compared to lattice-based schemes. These results confirm the long-held view that decoding random linear codes remains one of the most challenging known NP-hard problems in cryptography. The table also indicates that lattice-based schemes show higher parameter sensitivity, suggesting a narrower margin for secure implementation. The failure probabilities remain low across all schemes, reinforcing their suitability for cryptographic deployment under current standards.

The explanation of these data highlights important distinctions in mathematical hardness assumptions. Lattice-based security relies on the worst-case hardness of Learning With Errors variants, yet reductions may not perfectly reflect practical parameter sets used in deployed schemes. Code-based systems derive security from decoding problems that have resisted structural breakthroughs for decades, which accounts for the higher bit-level security estimates observed. These differences underscore the importance of understanding how theoretical assumptions translate into practical security margins.

The descriptive analysis extends to the behavior of each algorithm under adversarial perturbations. Lattice-based schemes show noticeable variation in attack costs when parameters such as noise levels or modulus sizes are even slightly misconfigured. Code-based constructions maintain relatively stable security margins across parameter variations but incur significantly larger key sizes that limit some practical applications. The descriptive patterns suggest that implementation environment plays a crucial role in determining overall cryptographic viability.

The inferential analysis identifies statistically consistent relationships between parameter sensitivity and attack-cost variability in lattice-based schemes. Algorithms showing higher sensitivity tend to experience sharper reductions in quantum-resistance under hybrid

attack models, indicating a measurable correlation that must be considered in deployment. Code-based schemes exhibit minimal inferential variation, reflecting stronger structural rigidity. These inferential patterns reinforce the need for precise parameter governance in lattice-based cryptography.

The relational analysis further demonstrates that the interplay between quantum speedup models and structural algorithm properties diverges across PQC families. Quantum-assisted lattice-reduction methods introduce more significant cost reductions for lattice-based schemes than analogous quantum decoding enhancements for code-based schemes. The relationship between algorithm structure and quantum attack feasibility suggests that code-based constructions possess inherently stronger asymptotic resistance to quantum cryptanalysis.

The case study component focuses on a simulated quantum-assisted attack against Kyber-1024 and Classic McEliece using Grover-optimized search and hybrid classical–quantum frameworks. The simulation shows that Kyber experiences a meaningful reduction in security level when adversaries leverage structured lattice reductions, while Classic McEliece demonstrates negligible degradation under similar conditions. These observations highlight practical differences in algorithmic resilience under adversarial sophistication.

The second part of the case study evaluates implementation-level risks, such as parameter drift and hardware-induced noise. Lattice-based schemes exhibit increased vulnerability to miscalibration of noise parameters, resulting in potential decryption failures or weakened hardness assumptions. Code-based algorithms maintain stability under environmental perturbations but impose operational burdens due to memory consumption and bandwidth demands for key storage and transmission.

The explanatory synthesis of the results indicates that the stronger attack resistance of code-based schemes arises from the absence of exploitable algebraic structure in randomly generated linear codes. Lattice-based constructions inherently contain more structure, which facilitates improved attack heuristics, especially when quantum acceleration is applied. The explanation suggests that mathematical structure plays a dual role, enabling algorithmic efficiency but also expanding potential attack surfaces.

The overall interpretation suggests that both lattice-based and code-based schemes remain viable for post-quantum standardization, yet their security assurances differ in nature rather than magnitude. Lattice-based schemes offer practical efficiency and manageable key sizes but require vigilant parameter governance. Code-based schemes deliver unmatched theoretical robustness but raise deployment challenges due to key-size overhead. The results indicate that a hybrid post-quantum ecosystem—leveraging the strengths of both families—may represent the most secure pathway for future cryptographic infrastructures.

The findings of this study indicate that lattice-based and code-based algorithms both demonstrate resilience against known classical and quantum-assisted attacks, yet they exhibit distinct security characteristics. Lattice-based schemes such as Kyber, NTRU, and Saber provide strong security margins but reveal considerable sensitivity to parameter misconfiguration, which may reduce their effective attack cost under hybrid adversarial models. Code-based schemes, exemplified by Classic McEliece, BIKE, and HQC, show exceptionally high theoretical attack complexity, with security estimates far exceeding those of lattice-based constructions.

The security analysis further demonstrates that quantum-assisted lattice-reduction techniques produce more significant reductions in security levels for lattice-based schemes than quantum decoding enhancements do for code-based schemes. This contrast reinforces the view that decoding random linear codes continues to present a formidable computational challenge, even with quantum resources. The results collectively highlight that code-based schemes maintain more stable security levels across varying attack strategies.

The parameter-sensitivity evaluation shows that lattice-based algorithms require more precise tuning of noise distributions, modulus sizes, and key-generation parameters. Minor deviations from recommended parameter sets can expose schemes to reduced complexity attacks. Code-based algorithms demonstrate lower sensitivity, maintaining stable security margins even with moderate parameter variability. These differences point to operational disparities between the two families.

The study concludes that both algorithm families remain viable candidates for post-quantum cryptographic deployment. Their respective security guarantees differ in structural origins: lattice-based constructions offer efficiency and scalability, while code-based systems provide long-term cryptanalytic resistance. The findings underscore the importance of aligning algorithm choice with practical implementation environments and long-term security needs.

The results align with earlier studies emphasizing the vulnerability of classical public-key cryptography to quantum algorithms and reaffirm the necessity of adopting PQC schemes. Prior research consistently identifies lattice-based algorithms as efficient and versatile, particularly in constrained hardware environments. The present findings support this view by demonstrating the strong performance of lattice-based schemes under properly calibrated parameters, echoing conclusions found in NIST's PQC Round 3 evaluations.

The study's findings diverge from some prior works that portray lattice-based systems as uniformly robust across parameter ranges. The results show that parameter misconfiguration can significantly weaken security, a nuance sometimes overlooked in earlier assessments. This distinction highlights the need for careful implementation and reinforces concerns raised by recent cryptanalytic papers exploring structural lattice vulnerabilities.

The results corroborate long-standing literature on the extraordinary resilience of code-based systems. Classic McEliece has historically been considered one of the most secure cryptosystems, and the current findings support this assumption by demonstrating negligible reductions in security even under quantum-assisted adversarial models. This consistency strengthens the position of code-based schemes in long-term cryptographic planning.

The comparative insights of this study extend previous analyses by integrating both classical and quantum-assisted cryptanalytic strategies within a unified evaluation model. Earlier research often isolates algorithmic categories or attack modalities, whereas this study synthesizes them, providing a more comprehensive perspective on security differences. This integrated approach contributes substantive depth to the discourse surrounding PQC standardization.

The findings indicate that post-quantum cryptography faces a multidimensional challenge that goes beyond the search for the single strongest algorithm. The differential performance between lattice-based and code-based schemes suggests that no universal PQC solution currently exists. The diversity of threat models, implementation environments, and computational constraints underscores the importance of maintaining a diversified cryptographic ecosystem (T. Chen et al., 2023).

The results reflect the maturity of code-based cryptography, which has benefited from decades of scrutiny and has so far resisted breakthroughs that would undermine its foundation. The stability of its performance under quantum-assisted models signals that combinatorial hardness remains a trustworthy basis for security in the foreseeable quantum era. This indicates a long-term reliability advantage that lattice-based schemes may not fully replicate.

The sensitivity of lattice-based systems to parameter selection reflects the underlying mathematical structure of LWE and its variants. The nuanced behavior of these schemes under perturbations indicates that implementation security cannot be taken for granted and requires sophisticated parameter governance. This reflection suggests that practical adoption must consider not only theoretical security but also operational feasibility (D'Anvers et al., 2023; Karthikeyan, 2023).

The collective findings indicate that a binary choice between lattice-based and code-based systems may be unnecessary and counterproductive. The complementary strengths of the two families suggest that hybrid or domain-specific selections may provide greater resilience than reliance on any single algorithm family. This finding reflects a broader trend in cryptographic strategy toward diversification and layered defense models.

The findings imply that policymakers and system architects must adopt a more nuanced approach to PQC deployment rather than relying solely on efficiency metrics or broad theoretical assurances. Critical infrastructures that require long-term confidentiality, such as governmental archives and medical records, may benefit from code-based schemes due to their extraordinarily high attack resistance.

The implications extend to hardware manufacturers and software engineers responsible for implementing lattice-based schemes. The demonstrated parameter sensitivity underscores the necessity of robust validation protocols and automated parameter-verification mechanisms embedded in cryptographic libraries. Neglecting these precautions could inadvertently weaken deployed systems.

The results suggest that organizations concerned with bandwidth or storage limitations may find lattice-based schemes more suitable due to their smaller key sizes and competitive performance. However, such benefits must be balanced with the increased complexity of secure parameter management. These trade-offs present an important consideration for real-world cryptographic transitions.

The broader implication is that global PQC adoption will likely require a portfolio approach rather than a singular standardized solution. The differential strengths illuminated by this study suggest that context-specific algorithm selection will play a central role in building quantum-resilient infrastructures. The results emphasize the importance of flexible cryptographic frameworks that support multiple PQC families (Levina et al., 2023; Wei et al., 2023).

The superior robustness of code-based schemes is explained by the absence of exploitable algebraic structure in randomly generated codes. The decoding problem that underpins their security has resisted algorithmic breakthroughs despite decades of study. This structural opacity limits the effectiveness of quantum-assisted decoding algorithms, explaining the minimal observed degradation in security under quantum models.

The greater vulnerability of lattice-based schemes to parameter variability arises from their complex mathematical structure, where noise terms, modulus sizes, and polynomial representations interact in nontrivial ways. This complexity creates opportunities for

cryptanalytic shortcuts when parameters are improperly tuned. The presence of such structural relationships explains why lattice-based schemes benefit significantly from optimized and tightly constrained parameter selections (K et al., 2023; Ngouen et al., 2023).

The observed reductions in attack cost under quantum-assisted lattice reduction can be attributed to the partial compatibility between lattice geometry and quantum-enhanced search techniques. Quantum algorithms accelerate basis-reduction heuristics, reducing the effective security level of lattice-based schemes more than they affect code-based schemes. This explains the different slopes of degradation across PQC families.

The overall asymmetry between the two PQC families derives from foundational differences in hardness assumptions. Combinatorial decoding problems scale exponentially even with quantum acceleration, while lattice problems exhibit more nuanced, structure-exploiting pathways for cryptanalysis. This disparity explains why code-based systems achieve higher asymptotic security levels despite practical limitations (Ni et al., 2023; S. Singh et al., 2023).

Future work should incorporate dynamic, real-time quantum hardware simulations to evaluate PQC schemes under realistic quantum-resource constraints. Such studies will clarify the true feasibility of quantum-assisted attacks and refine the predictive accuracy of current security estimates.

Future research must expand parameter-sensitivity studies, particularly for lattice-based schemes, to include side-channel leakage, timing vulnerabilities, and machine-learning-assisted attacks. These additional threat vectors will enhance practical understanding of PQC security beyond purely mathematical models.

Future cryptographic standardization efforts should explore hybrid PQC models that combine lattice-based and code-based schemes to achieve both high efficiency and high security. Such hybridization may offer a pathway to more robust protection against unforeseen quantum or classical cryptanalytic advances.

Future engineering development should focus on optimizing code-based systems to overcome their key-size limitations, possibly through structured code families or compression techniques. Advances in this area may significantly improve the deployability of code-based cryptography and strengthen its role in global PQC infrastructures (Putranto et al., 2023; Rabas et al., 2023).

CONCLUSION

The most important finding of this study is the clear differentiation in the security behavior of lattice-based and code-based post-quantum cryptographic algorithms when evaluated under unified analytical conditions. The analysis reveals that lattice-based schemes provide strong but parameter-sensitive security, whereas code-based schemes maintain remarkably stable and high attack resistance even under quantum-assisted adversarial models. This distinction highlights that the two algorithmic families exhibit fundamentally different security dynamics, with lattice-based constructions excelling in efficiency and deployability while code-based constructions dominate in long-term robustness. The identification of these contrasting profiles serves as a critical contribution to understanding how each family responds to evolving cryptanalytic strategies in the post-quantum era.

The added value of this research lies in the development of an integrated comparative-security framework that merges complexity-theoretic reasoning, attack-cost modeling, and

parameter-sensitivity evaluation into a coherent analytical methodology. This framework provides a more holistic lens than traditional studies, which often examine PQC families in isolation or rely on narrow adversarial assumptions. The conceptual contribution emerges from demonstrating how security margins shift when classical, quantum-assisted, and hybrid attack surfaces are examined concurrently, offering a more realistic representation of modern cryptographic threat landscapes. The methodological contribution offers a replicable structure that can be extended to additional PQC families or adapted for future cryptanalytic discoveries, strengthening the theoretical infrastructure of post-quantum security assessment.

The primary limitation of this study arises from its reliance on simulated attack models and theoretical estimations rather than full-scale quantum hardware experimentation, which remains largely infeasible with current technology. The absence of empirical quantum attack validation creates uncertainty regarding the practical applicability of certain quantum-assisted attack projections. Another limitation is the exclusion of side-channel, implementation-level vulnerabilities, and hardware-specific factors that may significantly influence real-world security outcomes for both algorithm families. Future research should incorporate more sophisticated quantum-resource modeling, simulation of hardware-induced attack vectors, and empirical benchmarking aligned with emerging quantum computing capabilities. Additional investigation into hybrid PQC deployments and performance-security trade-off modeling represents a promising direction for strengthening the predictive power and practical relevance of post-quantum cryptographic analysis.

AUTHOR CONTRIBUTIONS

Look this example below:

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

Azouaoui, M., Bronchain, O., Cassiers, G., Hoffmann, C., Kuzovkova, Y., Renes, J., Schneider, T., Schönauer, M., Standaert, F.-X., & van Vredendaal, C. (2023). Protecting Dilithium against Leakage Revisited Sensitivity Analysis and Improved Implementations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 58–79. Scopus. https://doi.org/10.46586/tches.v2023.i4.58-79

Chen, A. C. H. (2023). Post-Quantum Cryptography Neural Network. *Int. Conf. Smart Syst. Appl. Electr. Sci., ICSSES*. Scopus. https://doi.org/10.1109/ICSSES58299.2023.10201083

Chen, T., Li, H., Li, W., Nan, L., & Du, Y. (2023). Reconfigurable Polynomial Multiplication Architecture for Lattice-based Post-quantum Cryptography Algorithms. *Dianzi Yu Xinxi Xuebao/Journal of Electronics and Information Technology*, *45*(9), 3380–3392. Scopus. https://doi.org/10.11999/JEIT230284

D'Anvers, J.-P., van Beirendonck, M., & Verbauwhede, I. (2023). Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced

Implementations. *IEEE Transactions on Computers*, *72*(2), 321–332. Scopus. https://doi.org/10.1109/TC.2022.3197074

El Defrawy, K., Genise, N., & Manohar, N. (2023). On the Hardness of Scheme-Switching Between SIMD FHE Schemes. In T. Johansson, D. Smith-Tone, & D. Smith-Tone (Eds.), *Lect. Notes Comput. Sci.: Vol. 14154 LNCS* (pp. 196–224). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-40003-2_8

Greuet, A., Montoya, S., & Vermeersch, C. (2023). Modular Polynomial Multiplication Using RSA/ECC Coprocessor. In S. Li, M. Manulis, & A. Miyaji (Eds.), *Lect. Notes Comput. Sci.: Vol. 13983 LNCS* (pp. 283–304). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-39828-5_16

Guilley, G., Youssef, S., Zhang, F., & Yang, B.-L. (2023). Post-Quantum Cryptography—Having It Implemented Right. *Journal of Cryptologic Research*, *10*(3), 650–666. Scopus. https://doi.org/10.13868/j.cnki.jcr.000624

Hadi, O. K., & Sadkhan, S. B. (2023). Proposed Security Evaluation of Post-Quantum Cryptography Based on Soft Computing. *Int. Conf. Adv. Comput. Appl., ACA*, 217–223. Scopus. https://doi.org/10.1109/ACA57612.2023.10346878

He, P., & Xie, J. (2023). Novel Implementation of High-Performance Polynomial Multiplication for Unified KEM Saber based on TMVP Design Strategy. *Proc. - Int. Symp. Qual. Electron. Des., ISQED*, *2023-April*. Scopus. https://doi.org/10.1109/ISQED57927.2023.10129320

Hegde, S. B., Jamuar, A., & Kulkarni, R. (2023). Post Quantum Implications on Private and Public Key Cryptography. *Int. Conf. Smart Syst. Appl. Electr. Sci., ICSSES*. Scopus. https://doi.org/10.1109/ICSSES58299.2023.10199503

Henrich, J., Heinemann, A., Wiesmaier, A., & Schmitt, N. (2023). Performance Impact of PQC KEMs on TLS 1.3 Under Varying Network Characteristics. In E. Athanasopoulos & B. Mennink (Eds.), *Lect. Notes Comput. Sci.* (Vol. 14411, pp. 267–287). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-49187-0_14

K, K., Rohini, C., Sermakani, A. M., Dhakshunaamoorthiy, n., Menaga, P., & Maharasi, M. (2023). Quantum-Resistant Wireless Intrusion Detection System using Machine Learning Techniques. *Int. Conf. Comput., Commun., Control Autom., ICCUBEA*. Scopus. https://doi.org/10.1109/ICCUBEA58933.2023.10392127

Karthikeyan, D. (2023). Secure Medical Data Transmission In Iot Healthcare: Hybrid Encryption, Post-Quantum Cryptography, And Deep Learning-Enhanced Approach. *Glob. Conf. Inf. Technol. Commun., GCITC*. Scopus. https://doi.org/10.1109/GCITC60406.2023.10425954

Kim, J., & Park, J. H. (2023). NTRU++: Compact Construction of NTRU Using Simple Encoding Method. *IEEE Transactions on Information Forensics and Security*, *18*, 4760–4774. Scopus. https://doi.org/10.1109/TIFS.2023.3299172

Levina, A., Kadykov, V., & Rao Valluri, M. R. (2023). Security Analysis of Hybrid Attack for NTRU-Class Encryption Schemes. *IEEE Access*, *11*, 109939–109952. Scopus. https://doi.org/10.1109/ACCESS.2023.3321693

Li, A., Lu, J., Liu, D., Hu, A., Li, X., Yang, S., & Huang, T. (2023). Multi-Probability Hash-based Random Number Generator for Post-Quantum Cryptography. *Midwest Symp Circuits Syst*, 694–697. Scopus. https://doi.org/10.1109/MWSCAS57524.2023.10406008

Malygina, E. S., Kutsenko, A. V., Novoselov, S. A., Kolesnikov, N. S., Bakharev, A. O., Khilchuk, I. S., Shaporenko, A. S., & Tokareva, N. N. (2023). Post-Quantum Cryptosystems: Open Problems and Solutions. Lattice-Based Cryptosystems. *Journal of Applied and Industrial Mathematics*, *17*(4), 767–790. Scopus. https://doi.org/10.1134/S1990478923040087

Marzougui, S., Kabin, I., Krämer, J., Aulbach, T., & Seifert, J.-P. (2023). On the Feasibility of Single-Trace Attacks on the Gaussian Sampler Using a CDT. In E. B. Kavun & M. Pehl (Eds.), *Lect. Notes Comput. Sci.: Vol. 13979 LNCS* (pp. 149–169). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-29497-6_8

Ngouen, M., Rahman, M. A., Prabakar, N., Uluagac, S., & Njilla, L. (2023). Q-SECURE: A Quantum Resistant Security for Resource Constrained IoT Device Encryption. In M. Quwaider & Y. Jararweh (Eds.), *Int. Conf. Internet Things: Syst., Manag. Secur., IOTSMS* (pp. 141–148). Institute of Electrical and Electronics Engineers Inc.; Scopus. https://doi.org/10.1109/IOTSMS59855.2023.10325770

Ni, Z., Khalid, A., Liu, W., & Maire O'Neill, M. (2023). Towards a Lightweight CRYSTALS-Kyber in FPGAs: An Ultra-lightweight BRAM-free NTT Core. *Proc IEEE Int Symp Circuits Syst*, *2023-May*. Scopus. https://doi.org/10.1109/ISCAS46773.2023.10181340

Putranto, D. S. C., Wardhani, R. W., Larasati, H. T., & Kim, H. (2023). Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era. *IEEE Access*, *11*, 21848–21862. Scopus. https://doi.org/10.1109/ACCESS.2023.3252504

Qiao, Z., Liu, Y., Zhou, Y., Ming, J., Jin, C., & Li, H. (2023). Practical Public Template Attack Attacks on CRYSTALS-Dilithium With Randomness Leakages. *IEEE Transactions on Information Forensics and Security*, *18*, 1–14. Scopus. https://doi.org/10.1109/TIFS.2022.3215913

Rabas, T., Buček, J., & Lórencz, R. (2023). SPA Attack on NTRU Protected Implementation with Sparse Representation of Private Key. In P. Mori, G. Lenzini, & S. Furnell (Eds.), *Int. Conf. Inf. Syst. Secur. Priv.* (pp. 135–143). Science and Technology Publications, Lda; Scopus. https://doi.org/10.5220/0011729200003405

Singh, M., & Mishra, D. (2023). Post-quantum secure authenticated key agreement protocol for wireless sensor networks. *Telecommunication Systems*, *84*(1), 101–113. Scopus. https://doi.org/10.1007/s11235-023-01043-z

Singh, S., Fan, X., Prasad, A. K., Jia, L., Nag, A., Balasubramonian, R., Bojnordi, M. N., & Shi, E. (2023). XCRYPT: Accelerating Lattice-Based Cryptography With Memristor Crossbar Arrays. *IEEE Micro*, *43*(5), 45–54. Scopus. https://doi.org/10.1109/MM.2023.3248080

Song, G., Jang, K., Eum, S., Sim, M., & Seo, H. (2023). NTT and Inverse NTT Quantum Circuits in CRYSTALS-Kyber for Post-Quantum Security Evaluation. *Applied Sciences (Switzerland)*, *13*(18). Scopus. https://doi.org/10.3390/app131810373

Tanaka, Y., Ueno, R., Xagawa, K., Ito, A., Takahashi, J., & Homma, N. (2023). Multiple-Valued Plaintext-Checking Side-Channel Attacks on Post-Quantum KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(3), 473–503. Scopus. https://doi.org/10.46586/tches.v2023.i3.473-503

Wang, L., Huang, C., & Cheng, H. (2023). Novel proxy signature from lattice for the post-quantum internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 9939–9946. Scopus. https://doi.org/10.1007/s12652-021-03661-4

Wei, Y., Bi, L., Lu, X., & Wang, K. (2023). Security estimation of LWE via BKW algorithms. *Cybersecurity*, *6*(1). Scopus. https://doi.org/10.1186/s42400-023-00158-9

Yang, Y., Yuan, H., Yan, L., & Ruan, Y. (2023). Post-quantum identity-based authenticated multiple key agreement protocol. *ETRI Journal*, *45*(6), 1090–1102. Scopus. https://doi.org/10.4218/etrij.2022-0320

Zhao, X.-Y., Liang, Z.-C., Hu, Y., Geng, H.-X., & Zhao, Y.-L. (2023). NTT Architecture Research and Its FPGA Hardware Optimization Implementation. *Jisuanji Xuebao/Chinese Journal of Computers*, *46*(12), 2670–2686. Scopus. https://doi.org/10.11897/SP.J.1016.2023.02670

Zhou, T., Zheng, F.-Y., Lin, J.-Q., Wei, R., & Tang, W.-X. (2023). On Software Implementations of Post-Quantum Cryptography. *Journal of Cryptologic Research*, *11*(2), 308–343. Scopus. https://doi.org/10.13868/j.cnki.jcr.000681

Zhuang, E.-S., & Fan, C.-I. (2023). Multi-Keyword Searchable Identity-Based Proxy Re-Encryption from Lattices. *Mathematics*, *11*(18). Scopus. https://doi.org/10.3390/math11183830

Copyright Holder :
© Loso Judijanto et.al (2025).

First Publication Right :
© Journal of Tecnologia Quantica

This article is under: