Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 11, 2025

A COMPARATIVE ANALYSIS OF LWE BASED POST QUANTUM CRYPTOGRAPHIC SCHEMES: BALANCING CRYPTOGRAPHIC SECURITY, EFFICIENCY METRICS, AND IMPLEMENTATION FEASIBILITY IN THE POST QUANTUM TRANSITION ERA

Kainat Mubarik[*1], **Malik Aazaz Abbasi**[2]

[*1,2]*Shifa Tameer-e-Millat University Islamabad*

[*1]kainataizaz29@gmail.com, [2]aazazabbasi57571@gmail.com

DOI: https://doi.org/10.5281/zenodo.17777060

Keywords
Post-Quantum Cryptography (PQC), Lattice-Based Cryptography, Learning with Errors (LWE), NIST Standardization, Cryptographic Transition, Quantum Computing, Harvest Now, Decrypt Later (HNDL), CRYSTALS-Kyber, CRYSTALS-Dilithium, Key Encapsulation Mechanism (KEM), Digital Signature Algorithm (DSA).

Article History
Received: 08 October 2025
Accepted: 14 November 2025
Published: 29 November 2025

Corresponding Author: *
Kainat Mubarik

Abstract

The imminent threat posed by the realization of large-scale, fault-tolerant quantum computers (QCs), capable of leveraging Shor's algorithm to break foundational classical public-key cryptosystems like RSA and ECC, necessitates an immediate and comprehensive shift to Post-Quantum Cryptography (PQC). This urgency is intensified by the "Harvest Now, Decrypt Later" (HNDL) threat, which compromises long-term data confidentiality. The NIST PQC Standardization process has established Lattice-Based Cryptography as the leading family for new standards. This paper presents a comprehensive comparative analysis of major PQC schemes built upon the foundational mathematical problem, Learning with Errors (LWE). We systematically evaluate these LWE-based schemes (CRYSTALS-Kyber, CRYSTALS-Dilithium) by balancing three critical dimensions: cryptographic security (against classical and quantum attacks), efficiency metrics (key size, signature size, and operational speed), and implementation feasibility across diverse hardware environments. Our findings provide essential insights and a structured framework to guide engineers, policy-makers, and organizations in making informed decisions for the strategic and secure migration to quantum-resistant standards in the post-quantum transition era.

INTRODUCTION

The global technological landscape faces an unprecedented cryptographic crisis driven by the projected realization of large scale, fault tolerant quantum computing (Alghamdi et al., 2025) These machines, leveraging algorithms such as Shor's algorithm, possess the capability to efficiently solve the hard mathematical problems underlying current classical public key cryptosystems, including Rivest–Shamir Adleman (RSA) and elliptic curve cryptography (ECC) (Joseph et al., 2022). The resulting vulnerability necessitates a proactive and rapid transition to quantum resistant cryptography (PQC) (Chen et al., 2022). This urgency is compounded by the "Harvest Now, Decrypt Later" (HNDL) threat scenario (Choudhury et al., 2025). Under the HNDL paradigm, sophisticated adversaries may intercept and indefinitely store large volumes of encrypted communications and sensitive data today, anticipating the computational capability to decrypt them once quantum computers mature (Reddy et al., 2025) For critical sectors such as national defense, finance, and healthcare where long-term confidentiality spanning decades is nonnegotiable, the exposure of archived data presents irreversible national security and privacy implications (Turnip et al., 2025). Consequently, governments, standardization agencies, and industry stakeholders are actively working on transition strategies to safeguard mission critical infrastructure for the long term, making cryptographic migration an immediate requirement rather than a future option (Singh et al., 2025).

The U.S. National Institute of Standards and Technology (NIST) responded to this threat by launching a comprehensive post quantum cryptography standardization initiative in 2016 (Joseph et al., 2022). This rigorous process, which involved extensive public evaluation, peer review, and international collaboration, sought algorithms that demonstrated robust cryptanalytic resistance, verifiable efficiency, and maturity implementation (Bavdekar et al., 2023).

The culmination of this effort resulted in the formal approval and selection of lattice-based cryptography as the foundation for the majority of the first PQC standards (NIST, 2022). Specifically, the selection of schemes like CRYSTALS Kyber, CRYSTALS Dilithium, and Falcon highlights the strong confidence in the security guarantees derived from the underlying hard lattice problems, particularly those associated with the Learning with Errors (LWE) assumption (Mittal et al., 2025). Furthermore, these lattice-based schemes have demonstrated the requisite efficiency and suitability for implementation across diverse computing environments, ranging from high performance servers to resource constrained embedded systems (Turnip et al., 2025)

This review provides a rigorous comparative analysis focused on the essential trilemma facing PQC deployment: cryptographic security, quantitative efficiency, and practical implementation feasibility. The analysis begins by establishing the theoretical foundations of the LWE problem and the mechanisms that connect its average case hardness to worst case lattice problems (Mittal et al., 2025). It then details the NIST standardized schemes, contrasting their functional roles and inherent trade offs (Nguyen et al., 2025). The report proceeds to examine concrete cryptanalytic threats, focusing on lattice reduction and specialized statistical attacks. Finally, a comprehensive evaluation of performance benchmarks and critical implementation challenges particularly concerning physical side channel security is provided to inform optimal strategic deployment (Ghosh et al., 2025).

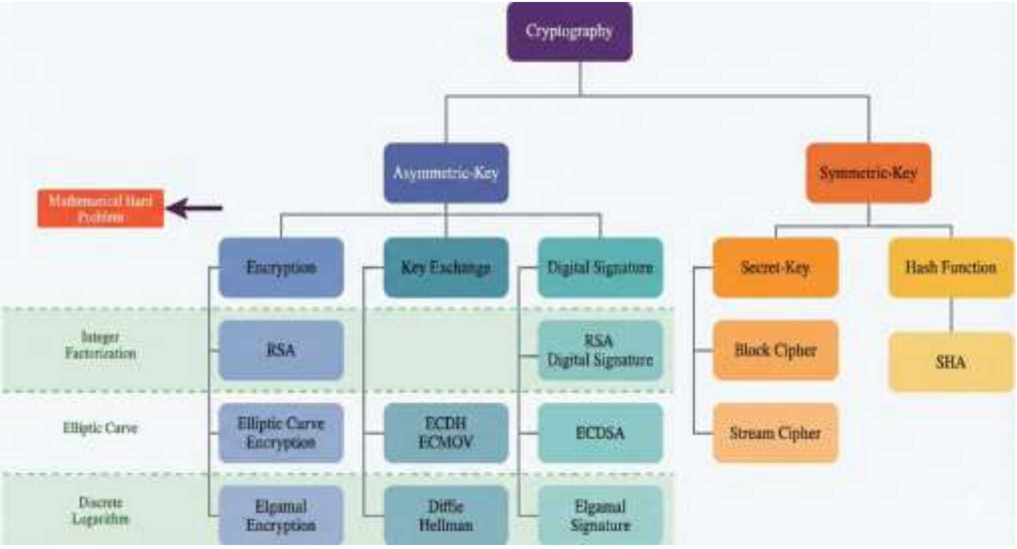
2. Theoretical Foundations and Hardness Assumptions

2.1. Learning With Errors (LWE) Problem: Definition and Parameterization

The Learning with Errors (LWE) problem serves as the foundational mathematical basis for the most prominent post quantum cryptographic schemes. Formally, an LWE instance is defined by finding a short secret vector **s** given access to an oracle that produces samples of the form (a, b), where a is a uniformly random vector, and b is the inner product of a and s, plus a small error term (e), all computed modulo q. The error term is sampled from a defined distribution, chi (Hayouni et al., 2025).

The security of LWE based cryptosystems is intrinsically linked to the careful parameterization of three crucial components: the dimension (n), which controls the size of the secret and the lattice; the modulus (q), which defines the arithmetic context; and the short error distribution (chi), typically Gaussian or binomial, which introduces the noise essential for cryptographic security (Mittal et al., 2025). The hardness of the LWE problem is not only fundamental to PQC but is also the essential ingredient for advanced cryptographic primitives such as Fully Homomorphic Encryption (FHE) schemes, highlighting its pervasive role in modern, quantum secure computation (Ghosh et al., 2025).

2.1 Overview of Cryptography: Asymmetric-Key vs. Symmetric-Key System



2.2. Security Guarantees: Worst Case to Average Case Hardness Reductions

The mathematical strength of LWE is derived from its established security reductions, which link the hardness of solving average LWE instances to the difficulty of solving the hardest instances of classic lattice problems (Turnip et al., 2025).

Regev's Breakthrough

A pivotal result in lattice-based cryptography is the work by Regev (2009), which provides a reduction proving that efficiently solving the average case LWE problem implies an efficient solution for the worst-case instances of problems such as the Gap Shortest Vector Problem (GapSVP) and the Shortest Independent Vector Problem (SIVP). This reduction is critical because it offers a quantifiable, worst case security guarantee against classical cryptanalysis. If an attacker could consistently break LWE instances (the average case), they could, in principle, solve the hardest known problems in lattice theory (the worst case) (Joseph et al., 2022).

First Order Observation: Quantum Necessity in Proof

A significant aspect of this foundational reduction is that Regev's original proof requires a quantum algorithm to perform the reduction (Regev, 2009). This means that assuming the worst-case hardness of GapSVP and SIVP, the LWE problem is proven hard even against classical attacks. The necessity of a quantum step in the reduction is important: it underscores that LWE is inherently a quantum aware primitive. An efficient solution to the LWE learning problem implies a quantum algorithm for GapSVP and SIVP (NIST, 2022). While this demonstrates a strong theoretical foundation, the long standing open question remains whether this reduction can be proven purely classically (non quantum) (Chen et al., 2016).

2.3. Structured Lattices: Transition from RLWE to MLWE

Generic LWE schemes suffer from substantial performance and size overheads. Early LWE based cryptosystems required public keys whose size scaled polynomially in the dimension (n), up to the fourth power, and similarly large ciphertexts (Joseph et al., 2022). This size complexity made them impractical for widespread deployment. The transition to structured lattices was motivated by the need to compress key materials and accelerate computations (Hayouni, H et al., 2025).

Structured Optimization

Schemes based on Ring LWE (RLWE) and its generalization, Module LWE (MLWE), introduce algebraic structure by defining the problem over polynomial rings, often cyclotomic rings. This structure allows key sizes and operations to scale much more favorably, achieving practical efficiency necessary for widespread integration (NIST, 2022). For example, the use of shared random bit strings under specific assumptions can reduce public key size to scale approximately linearly in the dimension (n) (Regev, 2009).

MLWE Advantages

The standardized schemes CRYSTALS Kyber (ML KEM) and CRYSTALS Dilithium (ML DSA) utilize the Module LWE setting. MLWE maintains most of the efficiency benefits derived from structure while simultaneously mitigating certain specialized algebraic attacks that have been shown to be particularly effective against pure RLWE schemesm (Choudhury et al., 2025). This strategic choice provides a superior balance, ensuring that the necessary performance gains do not introduce undue algebraic weaknesses, thereby cementing MLWE's suitability as the primary assumption for NIST selected PQC standards (Ghosh et al., 2025).

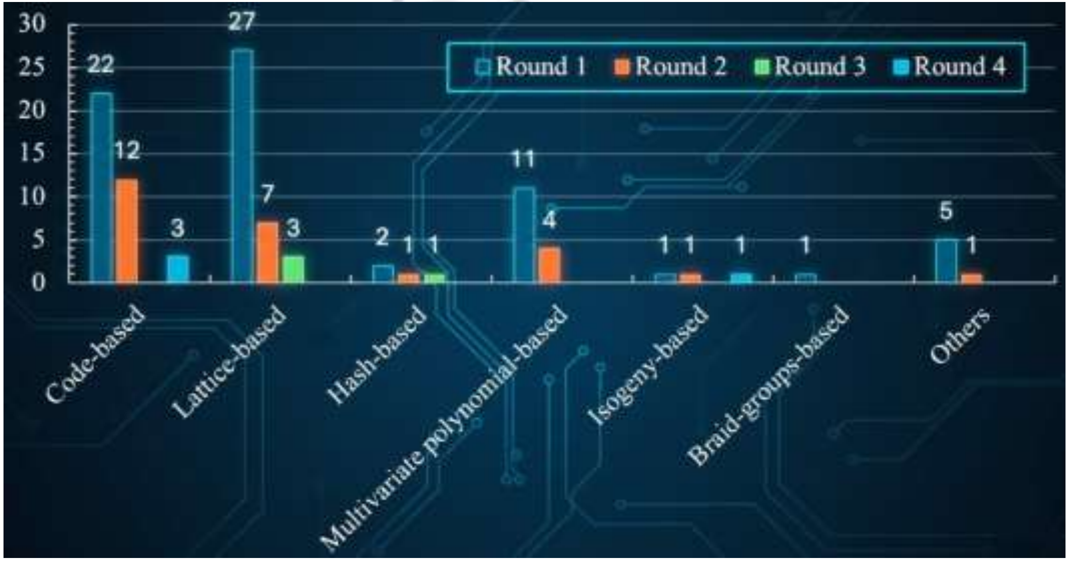
3. The NIST Selection: Standardized LWE Based Schemes

3.1. Overview of the NIST PQC Standardization and Scheme Formalization

The NIST standardization process, an extensive collaborative effort initiated in 2016, culminated in the formal approval of the first set of quantum resistant algorithms (Joseph et al., 2022). Following the selection announcement, NIST began drafting standards for the designated algorithms. By August 2023, draft standards for the core lattice-based schemes—Kyber, Dilithium, and Falcon—were released (FIPS 203, 204, and 205, respectively), with formal finalization occurring by August 2024 (Turnip et al., 2025).

With standardization, the algorithms received generic, function specific names: CRYSTALS Kyber is standardized as ML KEM (Module Lattice Key Encapsulation Mechanism), and CRYSTALS Dilithium is standardized as ML DSA (Module Lattice Digital Signature Algorithm) (NIST, 2024).

Figure 3.1 Dominance of Lattice-Based Schemes in NIST Standardization Rounds



3.2. Module Lattice KEM (ML KEM / CRYSTALS Kyber)

Kyber is the standardized Key Encapsulation Mechanism (KEM) (NIST, 2022). Its core function is the secure establishment of a shared secret key between two parties over an insecure channel. Kyber is widely recommended due to its excellent overall performance, characterized by high speed for all cryptographic operations and relatively small key sizes (Choudhury et al., 2025). Empirical testing, particularly within protocol integration contexts like TLS 1.3, has demonstrated that the Kyber 768 parameter set achieves superior key exchange efficiency compared to alternatives (Bavdekar et al., 2023).

3.3. Module Lattice DSA (ML DSA / CRYSTALS Dilithium)

Dilithium is the designated default standard for digital signatures (DSA) (NIST, 2022. Its primary application is authentication and guaranteeing data integrity (WQS Events, n.d.). Dilithium is recognized for its high performance, offering robust security coupled with fast operational speeds across a variety of operations. Along with Kyber, Dilithium provides a high level of confidence in both its cryptanalytic resistance and implementation maturity (Hayouni, H et al., 2025).

3.4. Falcon: Optimized Compactness DSA

Falcon is the second lattice based digital signature scheme to be standardized. Unlike Dilithium, which prioritizes speed and implementation simplicity, Falcon is optimized specifically for generating the smallest signature and public key sizes (Joseph et al., 2022)

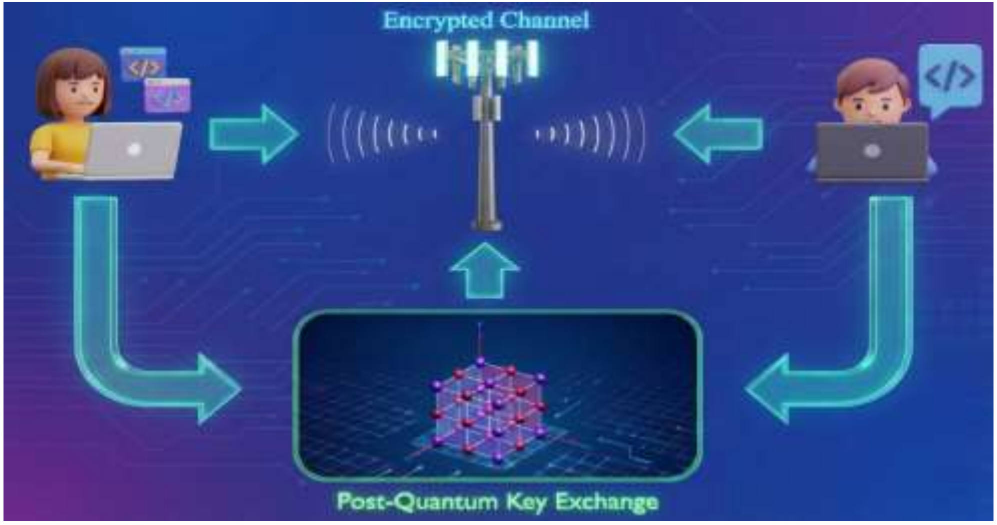
Strategic Deployment of Falcon

NIST's strategy is to recommend Dilithium (ML DSA) as the default signature scheme, reserving Falcon (FN DSA) for specific niche applications where minimizing communication bandwidth or storage is critical (NIST, 2024). These include environments such as resource constrained IoT devices or smart cards that require post quantum signatures but cannot handle Dilithium's larger signature size (e.g., a 2KB ML DSA signature) (NIST, 2024). Another crucial role is within Public Key Infrastructure (PKI), where root Certificate Authorities could use FN DSA to sign certificates, resulting in smaller signatures within certificate chains and thereby lightening client TLS handshakes (Mittal et al., 2025).

Implementation Complexity Considerations

The decision to designate Dilithium as the default signature scheme (Singh et al., 2025), despite Falcon's substantial size advantage, reveals an underlying assessment of implementation feasibility. Falcon's high efficiency relies on complex operations, notably the Gaussian sampling required during signingm (Mpofu et al., 2025) This complexity presents a significant hurdle in terms of implementation maturity, rigorous side channel protection, and overall algorithmic simplicity compared to Dilithium. This suggests that the NIST process valued the perceived ease of developing robust physical security countermeasures and the simplicity of implementation as critical factors when selecting the standard default for widespread adoption (Choudhury et al., 2025).

Figure 3.2 Concept of Post-Quantum Key Exchange over Encrypted Channels



4. Concrete Security and Cryptanalysis

4.1. Lattice Reduction Attacks (LRA) and BKZ Benchmarks

Lattice reduction algorithms form the baseline threat model against LWE based schemes, defining the necessary parameter sizes for achieving NIST security levels (1, 3, and 5). The primary tool for estimating the complexity of LRA is the Block Korkin Zolotarev (BKZ) algorithm, particularly its modern variants (BKZ 2.0) (Hayouni, H et al., 2025).

Theoretical estimates of attack performance, relying heavily on BKZ complexity, are essential for parameter selection. However, the concrete security landscape is dynamic. Ongoing debates regarding security loss, such as those that have occurred for specific parameter sets like Kyber 512, underscore the challenge of accurately modeling practical BKZ attack costs versus purely theoretical estimates (Perlner, 2020). The discussion surrounding comparisons of attack costs to "Earth resources" for high security instances further encourages the consideration of larger scale attacks in the evaluation of cryptographic security (Joseph et al., 2022).

4.2. Dual and Hybrid Attacks: Decision LWE Efficacy

Recent cryptanalytic efforts have focused on concrete benchmarking of alternative attack types against the standardized parameter choices, which often use specialized small secret or small error distributions not fully covered by traditional theoretical BKZ estimates (Mittal et al., 2025).

Specialized Attacks

The security evaluation includes specific LWE attacks such as the Search LWE attacks uSVP, SALSA, and Cool&Cruel, alongside Decision LWE attacks like the Dual Hybrid Meet in the Middle (MitM). For certain parameters, standard Search LWE methods (like uSVP) are practically infeasible, running for over 1100 hours without recovering secrets for Kyber parameters. In contrast, specialized attacks targeting specific mathematical properties of the implementation can be highly effective. For example, researchers have demonstrated that the Dual Hybrid MitM attack can solve Decision LWE instances for Kyber parameters using secrets with Hamming weights up to 4 in less than one hour (Mittal et al., 2025).

This benchmarking effort reveals a crucial causal relationship: while standard lattice attacks may provide a high theoretical floor for security, implementation specific characteristics (such as the choice of secret distribution) create vulnerability pathways. Optimization choices that reduce key size or computational burden by selecting small or sparse secrets inadvertently introduce a severe cryptanalytic advantage for the attacker, enabling rapid recovery via statistical or hybrid techniques (Singh et al., 2025.

4.3. Attacks on Sparse and Low Weight Secrets

The use of sparse binary secrets is an optimization technique considered for schemes related to LWE, particularly in Fully Homomorphic Encryption applications, as it can reduce computation complexity. However, this choice introduces a measurable security risk (Ghosh et al., 2025).

The statistical attack known as "The Cool and the Cruel" targets LWE instances with sparse binary secrets (Nolte et al., 2024). The methodology relies on an initial lattice reduction step. The key observation is that applying lattice reduction to the LWE matrix concentrates the high variance entries (the "hard parts") in the early columns of the extracted matrix. This allows the attacker to separate the secret into two sub problems: first, solving the "cruel" (hard) bits in the early columns, and second, finding the remaining "cool" (easy) bits in linear time using statistical techniques. The attack is demonstrably effective against LWE instances up to dimension n=768 (Choudhury et al., 2025).

Furthermore, the study confirms a critical differential vulnerability: Ring LWE instances are significantly more susceptible to "The Cool and the Cruel" attack than generic LWE instances. This demonstrates that parameter optimizations aimed at minimizing key size or computation time by using sparse or small secrets inadvertently create severe cryptanalytic pathways, which compel cryptographers to use larger parameters to restore the required security margin. This effectively negates the initial efficiency gains sought through the sparse secret structure (Choudhury et al., 2025).

5. Comparative Efficiency and Performance Metrics

The practical viability of LWE based schemes hinges on their efficiency metrics—specifically, communication overhead (key and ciphertext/signature size) and computational latency—across varied hardware environments (Mittal et al., 2025).

5.1. Communication Overhead Analysis: Key and Size Metrics

Communication size is a first order metric, directly impacting network overhead (especially in TLS handshakes) and memory requirements for storage. The relative sizes of the standardized schemes at NIST Security Levels 1 and 3 illustrate the efficiency trade offs (Research Team, 2025).

Table 1: Key and Ciphertext/Signature Sizes (in bytes) for Standardized PQC Schemes

Algorithm	NIST Level	Public Key (bytes)	Secret Key (bytes)	Ciphertext/Signature (bytes)	Function
CRYSTALS Kyber (ML KEM)	1	800	1632	768	KEM
CRYSTALS Dilithium (ML DSA)	1	1184	2800	2044 (Sig)	DSA
Falcon	1	897	1281	666 (Sig)	DSA
CRYSTALS Kyber (ML KEM)	3	1184	2400	1088	KEM
CRYSTALS Dilithium (ML DSA)	3	1472	3504	2701 (Sig)	DSA
Falcon	3	1441	2305	1007 (Sig)	DSA

The data confirms that Falcon maintains a substantial advantage in signature size, requiring 666 bytes at Level 1 compared to Dilithium's 2044 bytes, reinforcing its position as the size optimized choice (Chen et al., 2016).

5.2. Computational Latency Benchmarking across Heterogeneous Environments

Computational latency, measured through operation times, determines the overhead incurred during real time use. Comprehensive benchmarking across diverse platforms is crucial for informed deployment planning, distinguishing performance between high performance cloud infrastructure and severely resource constrained devices (Ghosh et al., 2025).

Table 2 provides raw operation times for NIST Security Level 1 across a server architecture (E1) and an embedded device (E3).

Table 2: Performance Latency (Raw Operation Times in ms) at NIST Security Level 1

Algorithm	Operation	Server Architecture (E1, ms)	Embedded Device (E3, ms)	Deployment Insight
CRYSTALS Kyber	KeyGen	0.08	1.25 \pm 0.04	Optimal for rapid, dynamic key establishment.
CRYSTALS Kyber	Encrypt	0.09	1.60 \pm 0.06	Excellent for high volume network encryption.
CRYSTALS Dilithium	KeyGen	0.12	1.75 \pm 0.06	Strong baseline key generation performance.

CRYSTALS Dilithium	Sign	0.15	1.95 \pm 0.07	Strong performance for high throughput signing applications.
Falcon	KeyGen	0.22	3.40 \pm 0.11	Highest key generation latency due to complex Gaussian sampling.
Falcon	Sign	0.28	3.85 \pm 0.12	Highest signing latency, complexity traded for size.
Falcon	Verify	0.04	0.70 \pm 0.03	Fastest verification operation, optimized for public trust validation.

Performance Scaling Implications

Analysis of these benchmarks reveals a fundamental disparity based on the computing environment. High performance server architectures, such as those used in cloud services, can implement the standardized algorithms with negligible performance impact, often increasing latency by less than 5% compared to classical schemes (Ghosh et al., 2025). This makes immediate adoption feasible for large scale infrastructure.

However, the situation is drastically different for resource constrained embedded systems. These devices experience significant overhead, with computational demands varying by up to 12 times between algorithms at equivalent security levels (Research Team, 2025). For instance, Kyber's operations are generally the fastest, making it the preferred choice for key exchange on the edge (Bavdekar et al., 2023).

Signature Scheme Trade off

The efficiency analysis confirms a crucial trade off for signature schemes. Falcon achieves the superior size profile, but this compactness is achieved at the expense of computational speed. Falcon's latency for KeyGen (3.40 ms) and Sign (3.85 ms) on embedded systems is significantly higher than Dilithium's (1.75 ms and 1.95 ms, respectively) (Research Team, 2025). Conversely, Falcon boasts the fastest verification operation (0.70 ms), optimizing for the most frequent public operation. This dictates a strategic selection: if minimizing storage or transmission bandwidth is the primary constraint, Falcon is selected. If system throughput requires fast, frequent signing, Dilithium remains the mandatory default (Turnip et al., 2025).

5.3. Protocol Integration Costs (TLS 1.3)

Integrating PQC into established communication protocols, such as Transport Layer Security (TLS) 1.3, requires structural adjustments to handle the larger key and ciphertext sizes inherent to lattice cryptography (NIST, 2022) This process involves the client specifying supported PQC schemes (Kyber, Dilithium, Falcon, SPHINCS+) in the ClientHello message and the server responding by confirming the chosen cipher suite (Ghosh et al., 2025).

Performance assessments of PQC integrated into TLS 1.3 confirm that Kyber 768 and Dilithium3 achieve superior computational efficiency for key exchange and signing, respectively. While these algorithms offer high speeds, naive implementation of PQC in TLS 1.3 can increase the handshake size significantly. Nonetheless, Falcon, despite its higher signing latency, is consistently noted for yielding the smallest overall TLS handshake size, validating its specialized role in minimizing protocol overhead where communication efficiency is the critical metric (Hayouni, H et al., 2025).

6. Implementation Feasibility and Physical Security Challenges

6.1. The Vulnerability Shift to Side Channel Attacks (SCAs)

The successful standardization of LWE based schemes addresses the vulnerability posed by quantum computing. However, this migration only shifts the focus of practical threats back to classical attacks, particularly Side Channel Attacks

(SCAs). PQC schemes remain inherently vulnerable to SCAs, which exploit physical implementation leaks through quantifiable channels such as timing variations, power consumption profiles, or electromagnetic radiation (MDPI, 2025). These non invasive techniques target intermediate states generated by the cryptographic process to recover the secret key. Therefore, robust implementation feasibility requires evaluating not just algorithmic speed, but also resilience against physical compromise (Chen et al., 2016).

6.2. Targeted Attacks on Structured Operations (NTT and SIS)

The core efficiency driven optimizations within lattice cryptography introduce predictable structural weaknesses that adversaries exploit (Joseph et al., 2022).

NTT Leakage and the SIS Connection

The Number Theoretic Transform (NTT) is employed extensively in highly optimized schemes like Kyber and Dilithium to achieve fast polynomial multiplication. While fast, the NTT operation is a major source of side channel information leakage. Recent cryptanalysis has demonstrated that information leaked during NTT computations can be re cast into an instance of the Short Integer Solution (SIS) problem. This connection allows attackers to solve the derived SIS instance efficiently, leveraging even incomplete leakage data to significantly accelerate the time to key recovery (Turnip et al., 2025).

Vulnerabilities in Matrix Polynomial Multiplication

Older LWE/RLWE schemes, such as Frodo and NewHope, are prime examples of this vulnerability. Noninvasive SCAs (power and timing analysis) targeting the intermediate states of matrix polynomial multiplication related to the subkeys can recover the full secret key with a 99% success rate. Furthermore, the application of advanced techniques like deep learning to analyze side channel traces has shown outcomes that significantly exceed the efficacy of traditional approaches like horizontal differential power analysis (Hayouni, H et al., 2025).

This situation highlights a fundamental conflict: the operations optimized for speed (such as NTT based arithmetic and structured polynomial multiplication) inherently introduce structural regularity that maximizes side channel leakage, creating a direct antagonism between computational performance and physical security robustness (Mittal et al., 2025).

6.3. Countermeasure Engineering and Overhead Assessment

To ensure practical security, strong countermeasures must be deployed, particularly in high risk environments like IoT. These measures, however, introduce unavoidable performance and resource overheads (Turnip et al., 2025).

Principles of Constant Time Implementation

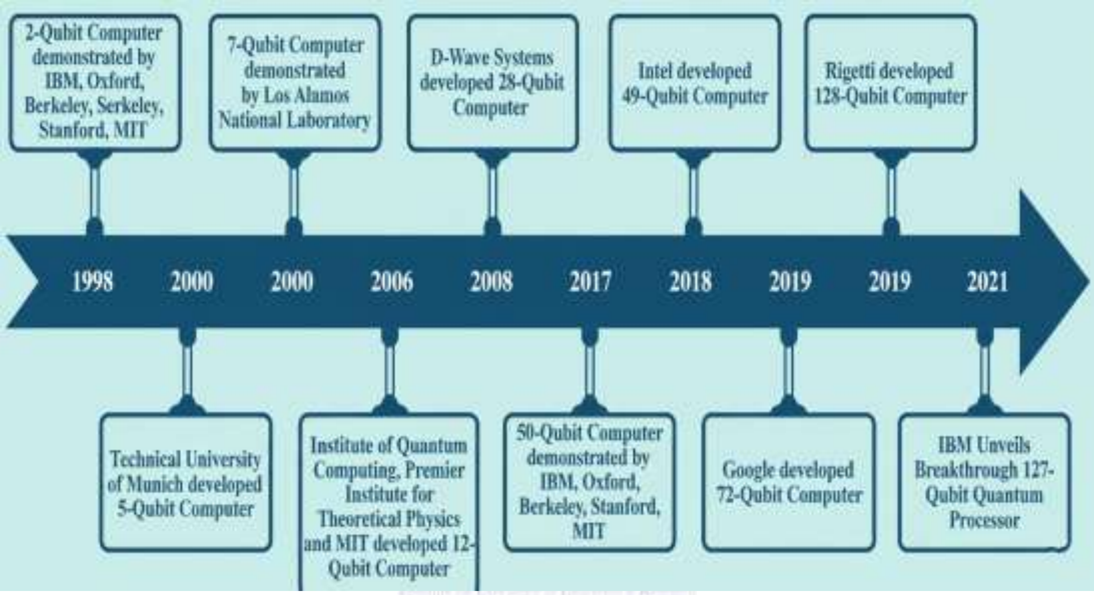
A baseline defense involves strict adherence to constant time coding principles, ensuring that execution time and memory access patterns are independent of secret data. Specific implementations require the adoption of robust techniques, including full masking or blinding, the use of table free butterfly operations within the NTT, constant time reducers, and disciplined management of Direct Memory Access (DMA) and cache usage to prevent timing side channel leakage (Keysight, 2025).

Advanced Masking and Cost

More robust protection requires advanced obfuscation techniques. Necessary measures include the implementation of robust masking techniques, such as shuffling and random delay insertion (MDPI, 2025). Specific research on CRYSTALS Kyber has led to the suggestion of both additive and multiplicative masking to mitigate vulnerabilities in polynomial multiplication. The multiplicative masking technique was introduced as a novel countermeasure specifically for Kyber. Despite their necessity, even proposed countermeasures are not entirely effective against sophisticated SCAs, emphasizing the necessity for continuous evaluation and improvement (Choudhury et al., 2025).

The integration of these protective measures dramatically alters the efficiency profile. The latency and resource figures presented in Section 5 represent raw, unprotected performance. The cost of securing the implementation, evidenced by the necessary overhead associated with a masked implementation of Kyber (NIST, 2022), significantly revises these estimates downward. Consequently, the implementation feasibility of LWE based PQC in constrained systems is often defined by the cost incurred in securing the implementation, rather than the raw speed of the unprotected algorithm (Bavdekar et al., 2023).

Figure 6.1 Evolution of Quantum Computing: A Timeline of Qubit Advancemen


2-Qubit Computer demonstrated by IBM, Oxford, Berkeley, Serkeley, Stanford, MIT
7-Qubit Computer demonstrated by Los Alamos National Laboratory
D-Wave Systems developed 28-Qubit Computer
Intel developed 49-Qubit Computer
Rigetti developed 128-Qubit Computer
1998
2000
2000
2006
2008
2017
2018
2019
2019
2021
Technical University of Munich developed 5-Qubit Computer
Institute of Quantum Computing, Premier Institute for Theoretical Physics and MIT developed 12-Qubit Computer
50-Qubit Computer demonstrated by IBM, Oxford, Berkeley, Stanford, MIT
Google developed 72-Qubit Computer
IBM Unveils Breakthrough 127-Qubit Quantum Processor

7. Conclusion and Strategic Recommendations

7.1. Synthesis of Findings and Optimal Deployment Scenarios

The comparative analysis of LWE based post quantum cryptographic schemes confirms their necessary role in mitigating the quantum threat and highlights the acute trade offs between mathematical security, operational efficiency, and physical implementation feasibility.

The standardized schemes—Kyber, Dilithium, and Falcon—each occupy a specific optimal deployment niche determined by their strengths and weaknesses in this trilemma. Kyber (ML KEM) is the superior choice for high-volume, general-purpose key establishment due to its low latency across all operations. Dilithium (ML DSA) is the robust default for digital authentication, offering high throughput signing speed, despite the penalty of larger signature sizes. Falcon is strategically reserved for highly constrained environments or applications demanding minimal communication overhead (e.g., PKI trust roots), compensating for its smaller size with significantly increased operational latency for key generation and signing (Hayouni, H et al., 2025)..

Table 3: Comparative PQC Trade offs and Deployment Suitability

Algorithm	Function	Primary Advantage	Primary Disadvantage	Ideal Deployment Scenario
CRYSTALS Kyber (ML KEM)	KEM	Highest operational speed and key exchange efficiency; balanced size.	Vulnerable to SCA via NTT leakage; specialized attacks on sparse secrets.	Cloud services, High volume TLS traffic,

				General purpose key exchange.
CRYSTALS Dilithium (ML DSA)	DSA	Recommended default; fast signing speed; high implementation confidence.	Largest signature size; significant communication overhead.	High throughput transaction systems, General enterprise infrastructure.
Falcon	DSA	Smallest signature and public key sizes (best communication efficiency).	Highest latency for KeyGen and Sign; complex implementation (Gaussian sampling).	PKI root CAs, bandwidth constrained IoT devices, Smart cards.

7.2. Challenges in Standardization and the Path to Ubiquitous PQC Adoption

The post standardization challenge centers on bridging the persistent gap between theoretical high performance, achieved through algebraic optimization (e.g., NTT), and the requirement for robust physical security. The use of highly efficient operations like the NTT creates a structural weakness that adversaries exploit through SCAs (by reduction to SIS instances) (Keysight, 2025).

For ubiquitous PQC adoption, particularly in resource constrained IoT environments where overhead costs are magnified, standardization efforts must evolve. The focus must shift toward establishing common, secure implementation practices and frameworks that reliably generalize robust SCA countermeasures such as multi-layer masking and constant time execution—across diverse, heterogeneous hardware platforms. The lack of adequate security countermeasures tailored to IoT constraints presents a major roadblock to securing PQC on the edge (Hayouni, H et al., 2025).

7.3. Open Research Questions in Lattice Cryptography

Further research must address several critical open questions to secure the PQC transition:

1. **Concrete Security Modeling:** There is an ongoing need to accurately model and incorporate the concrete costs of specialized cryptanalytic attacks (such as hybrid Meet in the Middle and "The Cool and the Cruel" (Nolte et al., 2024)) into the security parameter selection process. This is crucial to ensure that implementation specific optimizations, such as the use of sparse or small secrets, do not fatally compromise the security margin required for long term confidentiality (Bavdekar et al., 2023).
2. **Low Overhead Countermeasures:** The development of low overhead, multi-layer masking and blinding techniques specifically designed for the Number Theoretic Transform (NTT) remains a critical objective. These techniques must minimize the performance penalty on highly constrained devices while providing provable security against differential power analysis and timing attacks (Joseph et al., 2022).
3. **Classical Reduction Proof:** The theoretical community continues to seek purely classical (non-quantum) proof of Regev's LWE reduction, which would eliminate the reliance on quantum complexity theory to establish the average case hardness of the LWE problem (Regev, 2009).

Acknowledgment

We would like to express my deepest gratitude to my parents for their unconditional love, constant encouragement, and unwavering support throughout my academic journey. Their guidance and prayers have always been a source of strength and motivation for me. We are also sincerely thankful to my teachers, whose dedication, knowledge, and mentorship have shaped my learning and inspired me to strive for excellence. Their continuous support and valuable guidance played an essential role in the completion of this work.

References

Alghamdi, A. (2025). Post-quantum cryptography implementation challenges: Security implications for critical infrastructure.

Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: a review of techniques, challenges and standardizations. In 2023 International Conference on Information Networking (ICOIN) (pp. 146 151). IEEE.

Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith Tone, D. (2016). Report on post quantum cryptography (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

Choudhury, B., Hota, A., Karmakar, M., Saha, S., Nag, A., & Nandi, S. (2025). A comprehensive survey on pre vs post Quantum security schemes for 5G enabled IoT Applications. IEEE Access.

Choudhury, B., Hota, A., Karmakar, M., Saha, S., Nag, A., & Nandi, S. (2025). A comprehensive survey on pre vs post Quantum security schemes for 5G-enabled IoT Applications. IEEE Access.

Consortium for Homomorphic Encryption. (2018). Standardization of the LWE Hardness Assumption for Fully Homomorphic Encryption.

Ghosh, T., & Nath, I. (2025). Secure Satellite Communication in the Post Quantum Era: A Lattice Based Cryptographic Approach.

Hayouni, H. (2025). Adaptive post quantum security framework for wireless sensor networks using lightweight cryptography and context aware key management. The Journal of Supercomputing, 81(15), 1 58.

Joseph, A., (2022). The urgency of Post Quantum Cryptography migration: The Harvest Now, Decrypt Later (HNDL) threat.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post quantum cryptography. Nature, 605(7909), 237 243.

Keysight Technologies. (2025). PQC Implementations Still Leak: SCA and FI Risks in Dilithium and Kyber.

MDPI. (2025). Side channel attacks and countermeasures for post quantum cryptography: A review. Journal of Cyber Security and Data Protection, 8(2), 15.

Mittal, H., & Jain, B. (2025, May). Post Quantum Cryptography: A Comprehensive Review of Past Technologies and Current Advances. In Proceedings of First Global Conference on AI Research and Emerging Developments (G CARED) (pp. 360 366).

National Institute of Standards and Technology. (2022). Selection of the first set of Post Quantum Cryptographic Schemes (Kyber, Dilithium, Falcon)

National Institute of Standards and Technology. (2024). NIST Releases First Three Finalized Post Quantum Encryption Standards (FIPS 203, 204, 205).

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. IEEE Access.

Nolte, N., (2024). The cool and the cruel: Separating hard parts of LWE secrets. AFRICACRYPT.

Perlner, C. (2020, August 17). PQC Forum discussion on Kyber 512 security loss and complexity comparison. [

Reddy, A. (2025). Evaluating Post-Quantum Cryptography in the Era of Quantum Supremacy: Quantum Shadows. Famous Journal of computer science and Technology, 2(7), 41-59.

Regev, O. (2009). On lattices, learning with errors, and cryptosystems. Journal of the ACM, 56(6), Article 34.

Singh, M., Sood, S. K., & Bhatia, M. (2025). Post quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. Archives of Computational Methods in Engineering, 1 42.

Singh, M., Sood, S. K., & Bhatia, M. (2025). Post quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. Archives of Computational Methods in Engineering, 1 42.

Turnip, T. N., Andersen, B., & Vargas Rosales, C. (2025). Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. IEEE Communications Surveys & Tutorials.

Mpofu, K. T., & Mthunzi-Kufa, P. (2025). Post-Quantum Cryptography: Number Theoretic Foundations and Future-Proof Protocols.

Mittal, H., & Jain, B. (2025, May). Post-Quantum Cryptography: A Comprehensive Review of Past Technologies and Current Advances. In Proceedings of First Global Conference on AI Research and Emerging Developments (G-CARED) (pp. 360-366).