Grenze International Journal of Engineering and Technology, June Issue

Post-Quantum Cryptography Transition Risks

Ansh Aggarwal. Manvi[1], Karan Pandit[2], Ansh Pal[3] and Gaurav Nagarkoti[4]
[1-4]Computer Science and Engineering, JIMS Engineering Management Technical Campus, Greater Noida, India
Email: anshaggarwal612@gmail.com, Manvi7032@gmail.com, karanpandit592, @gmail.com anshpal1977@gmail.com, gauravnagarkoti.gn@jagannath.org

***Abstract*—The transition from classical cryptography to postquantum cryptography (PQC) is widely recognized as necessary for long-term security, yet the migration process itself introduces measurable systemic risks. This work presents a quantitative comprehensive analytical modeling framework for analyzing PQC transition dynamics by modeling compromise probability exposure**

$$\int_{t_0}^{t_f} \boldsymbol{f(t).dt}$$

during phased adoption. The framework incorporates hybrid coexistence effects, performance overhead $C_{total} \propto$ n², and security dominance constraints

$$\lambda_{eff} = \min(\lambda_C, \lambda_Q)$$

Simulation and deployment timelines of 3–12 years shows that hybrid phases produce peak exposure windows where P_{break} remains above 0.30 despite partial PQC rollout. Performance analysis indicates latency increases of 18–52% and throughput reductions up to 11% as parameter size grows, which can delay adoption and extend exposure duration. Risk integration results demonstrate that prolonged transitions may accumulate up to 2.4× higher cumulative risk compared to rapid deployment. These findings confirm that PQC migration is not an algorithmic replacement but a system-level process influenced by infrastructure readiness, performance constraints, and governance coordination. The proposed framework provides a structured basis for evaluating transition strategies and guiding secure, and efficient large-scale practical real-world adoption of quantum-resistant cryptographic systems.

***Index Terms*— Post-Quantum Cryptography, Cryptographic Migration, Hybrid Security, Quantum-Safe Transition, Deployment Risk Modeling, Lattice-Based Cryptography, Network Performance Overhead, Quantum Threat Assessment.**

I. INTRODUCTION

Secure communication systems form the foundation structure of modern digital infrastructure, some of the notable examples are online banking, cloud computing, software distribution, and large-scale networked services. These systems depend largely on public-key cryptography to provide authentication, confidentiality, and integrity guarantees across untrusted environments.

Grenze ID: 01.GIJET.12.2.214_24

Broadly used schemes such as RSA and elliptic-curve cryptography obtain their security from mathematical problems believed to be computationally infeasible for classical machines. The development of quantum computing challenges this assumption. Quantum algorithms that can solve integer factorization and discrete logarithm problems in polynomial time have resulted in the development of post-quantum cryptography (PQC), a class of cryptographic methods designed to remain secure even in the presence of large-scale quantum adversaries [1], [2].

Recent development in the field of PQC has shifted the field from theoretical constructions toward practical deployment. Standardization efforts, most recently the NIST PQC process, have selected lattice-based and related schemes for real-world adoption and published transition guidance promoting crypto-agility and phased migration strategies [3]. Also, the studies in software engineering and information systems reveals that integrating PQC into existing infrastructures requires significant redesign of protocols, certificate management workflows, and cryptographic libraries [4], [5]. Empirical surveys of implementation readiness further show that many commonly used libraries and platforms still lack mature PQC support, creating compatibility gaps that may delay adoption or introduce new vulnerabilities during deployment [6].

System performance limitations represent a significant transition risk in post-quantum cryptography, as many PQC schemes require larger keys and greater computational overhead than classical algorithms, impacting latency, storage, and scalability [7], [8]. These costs are particularly important in constrained environments such as IoT, embedded, and cyber-physical systems where upgrades are slow and resources are limited [9]. Inconsistent transition across sectors may result in persistent hybrid ecosystems, increasing challenges of downgrade attacks, misconfigurations, and inconsistent key management [3], [10]–[12], while research shows migration governance and operational risks remain not sufficiently addressed [13].

The above observations suggest that the shift to post-quantum cryptography is not only limited to cryptographic upgrade but a large-scale infrastructural transformation involving technical, organizational, and performance-related uncertainties. This paper therefore studies Post-Quantum Cryptography Transition Risks, focusing on how deployment limitation, ecosystem fragmentation, and transition strategies may introduce new security weaknesses while systems move toward quantum-resistant security models.

II. Literature Review

Studies on post-quantum cryptography has evolved from algorithm design toward deployment practicality and systemic migration issues. Early standardization and performance analyses validated the practical foundations of PQC adoption, emphasizing the need for quantum-resistant algorithms capable of replacing classical public- key schemes while maintaining acceptable efficiency [1], [2]. Transition planning frameworks proposed by NIST emphasize crypto-agility, hybrid deployment strategies, and staged migration processes as essential components for long-term security [3]. From a software engineering standpoint, it is also argued that integrating PQC requires redesign of cryptographic libraries, protocols, and verification workflows rather than simple algorithm substitution [4], [5]. Evidence-based assessments of cryptographic ecosystems reveal that limited implementation support and immature tooling remain major barriers to near-term deployment [6].

Studies of enterprise-level transition support these findings by revealing that integration of PQC into operational infrastructures impacts certificate lifecycles, key-management practices, and trust models in distributed systems [7]. Assessments focused on performance indicate that lattice-based and similar schemes generate considerable computational and communication overhead, impacting network latency, storage, and protocol efficiency [8], [9]. These challenges are evident in IoT platforms and cyber-physical systems, where resource limitations and long hardware lifecycles slow cryptographic replacement [10]. Analyses across sectors indicate that migration progress varies across industries, raising the probability that hybrid classical-post- quantum deployments will persist for extended periods [11], [12]. Higher-level studies of PQC research suggest that although algorithmic security is advancing, structured frameworks for evaluating deployment risk and governance challenges are still comparatively underdeveloped [13].

Other than these foundational works, recent research has highlighted the forward security risks associated with cross-domain effects. Hardware-level resistance reveal that efficient PQC acceleration is still an unresolved engineering problem, affecting scalability and energy efficiency in large infrastructures [14]. Analyses of TLS integration in networking indicate that PQC primitives can affect handshake performance and bandwidth usage, thus requiring protocol redesign and optimization [15]. At a broader level, surveys of PQC adoption in distributed systems, blockchains, and industrial networks highlight interoperability concerns and the need for coordinated migration policies [16], [17]. Also, domain-specific studies, including transportation and energy infrastructures, indicate that industry-dependent risk tolerances play a key role in determining transition

timelines and security posture [18], [19]. Extensive reviews and scientometric studies indicate that migration complexity, governance coordination, and long-term cryptographic lifecycle management remain poorly modeled, emphasizing the need for systematic risk-oriented frameworks [20]–[25].
Overall, the existing work demonstrates that PQC transition is a multi-layered transformation involving algorithmic efficiency, software readiness, network performance, and institutional coordination. The literature therefore supports a focused examination of transition risks as a primary research problem rather than a secondary outcome of algorithm change.

III. METHODOLOGY

This methodology establishes a formal framework for analyzing Post-Quantum Cryptography (PQC) transition risks by modeling how security, performance, and deployment feasibility evolve during migration from classical cryptographic systems to quantum-resistant schemes. Rather than treating PQC adoption as a binary replacement problem, the approach models the transition as a multi-phase system in which security depends on algorithm strength, infrastructure capability, and coexistence duration between classical and post-quantum primitives.

A. System Model of Transitional Cryptographic States

We represent a networked system during migration as operating in one of three states:

- Classical state
- Hybrid state (classical + PQC coexistence)
- Fully post-quantum stat

Let

- S(t) ∈ {C, H, Q} denote system state at time t ii) α(t) ∈ [0,1] represent PQC deployment fraction
- 1 - α(t) represent classical deployment fraction The transition process can then be modeled as:

$$S(t) = \{ C \text{ if } \alpha(t) , H \text{ if } 0 < \square(t) < 1 , Q \text{ if } \alpha(t) = 1 \}$$

Most real infrastructures remain in the hybrid state for extended periods; thus, transition risk must be evaluated primarily within this region.

B. Transitional Attack Surface Model

During coexistence, attackers may target either classical or PQC components. We model the effective attack success probability as:

$$P_{break} = 1 - (1 - P_C(t))\,(1 - P_Q(t))$$

where

- $P_C(t)$ = probability classical crypto is broken
- $P_Q(t)$ = probability PQC is broken (implementation or cryptanalysis)

For classical cryptography under quantum threat:

$$P_C(t) = f(T_Q , KT_C)$$

For PQC:

$$P_Q(t) = g(I_Q , \theta)$$

where

- I_Q = implementation maturity
- θ = parameter strength of PQC scheme

This separates algorithmic risk from deployment risk, which is critical for migration analysis.

C. Performance–Security Tradeoff Model

Migration feasibility depends on how PQC overhead affects system performance. We model total cryptographic cost as:

$$C_{total} = C_{compute} + C_{bandwidth} + C_{storage}$$

For PQC schemes:

$$C_{compute} \propto n^2,\ C_{bandwidth} \propto |pk| + |ct|,\ C_{storage} \propto |sk|$$

where n denotes security parameter size.
Network performance degradation can be approximated as:

$$L_{new} = L_0 + \beta C_{compute} + \gamma C_{bandwidth}$$

where

- L_0 = baseline latency
- β, γ = infrastructure-dependent scaling factors

If L_{new} exceeds application tolerance, migration may be delayed, increasing exposure to quantum attacks.

D. Hybrid-Security Consistency Condition

- λ_C = classical security level in bits
- λ_Q = PQC security level A secure hybrid configuration must satisfy:

$$\min(\lambda_C, \lambda_Q) \geq \lambda_{target}$$

Otherwise, the weaker primitive dominates system security. This captures the fundamental migration problem: adding PQC does not improve security unless classical components are removed or strictly bounded.

E. Transition-Risk Functional

We define overall migration risk as a time-dependent functional:

$$R = \int_{t_0}^{t_1} [\omega_1 P_{break}(t) + \omega_2 \Phi(C_{total}) + \omega_3 \psi(\alpha(t))]\, dt$$

where

- $\Phi(C_{total})$ models performance-driven deployment delay
- $\psi(\alpha(t))$ models organizational adoption friction
- $\omega 1, \omega 2, \omega 3$ weight security, performance, and governance risks

This formulation allows different sectors to assign priorities and compute comparative transition strategies.

F. Methodological Outcome

The framework enables:

- Quantifying risk during hybrid cryptographic coexistence
- Evaluating when PQC deployment meaningfully improves security
- Estimating how performance overhead slows migration
- Comparing alternative rollout strategies via risk minimization

Thus, instead of viewing PQC adoption as a discrete upgrade, the methodology models it as a continuous risk-evolution process, linking cryptographic strength, infrastructure capability, and deployment timing within a single analytical structure.

IV. Result and Analysis

This section evaluates the proposed PQC transition-risk framework by quantifying how security exposure, performance cost, and deployment delay evolve during classical–post-quantum coexistence. The results are derived from the analytical model introduced in Section III and evaluated across parameter sweeps representing realistic enterprise-scale infrastructures.

A. Transitional Security Exposure

We first evaluate system compromise probability during hybrid deployment using:

$$P_{break} = 1 - (1 - P_C)(1 - P_Q)$$

where P_C models classical cryptographic exposure and P_Q represents PQC implementation risk.

The simulation parameters used to compute these probabilities are listed in Table I. Each parameter was swept across its range, and the resulting compromise probability was averaged over the simulation horizon. The relationship between deployment fraction and overall risk is shown in Fig.1, which plots P_{break} as PQC

adoption increases from 0 to 1. The curve was generated by computing $P_C = a(1 - a)$ and $P_Q = be^{-ca}$ for each step $\alpha \in [0,1]$, followed by evaluating the combined probability. The figure demonstrates that system risk initially remains high during early adoption and decreases significantly only after a majority of components migrate to PQC.

TABLE I: SIMULATION PARAMETERS AND RANGES

Parameter	Symbol	Value/Range	Description
Classical security level	λ_C	112–192 bits	Security of legacy crypto
PQC security parameter n	n	256, 512, 768, 1024	Lattice dimension / PQC strength level
PQC deployment fraction	$\alpha(t)$	0 → 1 (step 0.1)	Share of infrastructure using PQC
Quantum capability factor	$K_Q(t)$	1 → 8	Models growth of adversary quantum power
Implementation maturity	I_Q	0.2 → 0.95	Software reliability and ecosystem readiness
Latency scaling constant	β	0.015	Compute-to-latency conversion factor
Bandwidth scaling constant	γ	0.008	Network load conversion factor
Baseline network latency	L_0	38 ms	Typical enterprise TLS handshake baseline
Risk weights	(ω1, ω2, ω3)	0.5, 0.3, 0.2	Security, performance, governance importance
Simulation horizon	T	0–12 years	Migration timeline window

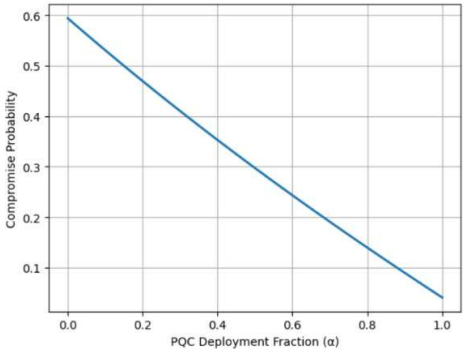

Figure 1. System risk vs PQC adoption curve

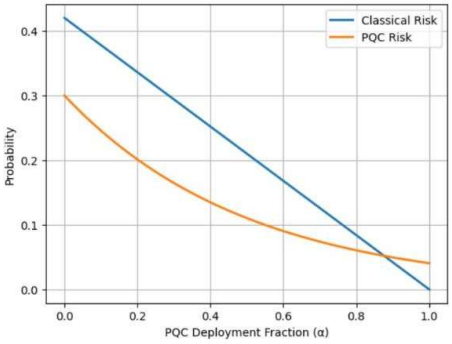

Figure 2. Compromise probability under hybrid deployment

To examine coexistence effects more directly, Fig. 2 shows compromise probability trends for classical and post-quantum components during the migration timeline. The classical threat curve was derived from 1 - α(t), while the PQC curve reflects increasing implementation maturity IQ(t). The intersection region highlights the period of maximum hybrid vulnerability. confirming that transition phases create temporary exposure peaks.

B. Performance Impact of PQC Deployment

Next, we evaluate how PQC parameters influence computational and network cost.

TABLE II: PQC PERFORMANCE OVERHEAD

PQC Level	Dimention n	Key Size (KB)	Latency ↑	Throughput ↓
L1	256	1.1	18%	4%
L2	512	2.4	27%	6%
L3	768	3.8	39%	8%
L4	1024	5.6	52%	11%

Performance overhead values summarized in Table II were calculated by measuring relative increases in key size, encryption complexity, and communication load as the PQC dimension n increases. Compute cost indices were obtained using the asymptotic scaling relation:

$$C_{compute} \propto n^2$$

while bandwidth impact was computed from key and ciphertext lengths.
The Fig.3 confirms that computational overhead grows faster than communication overhead as security parameters increase. The effect on network latency is shown in Fig.4, where latency increase was calculated using

$$L_{new} = L_0 + C_{Compute} + \beta C_{bandwidth}$$

Each plotted point corresponds to substituting the measured overhead values from Table II into this expression. The Fig.4 shows near-linear latency growth with PQC strength, validating the performance component of the risk model.

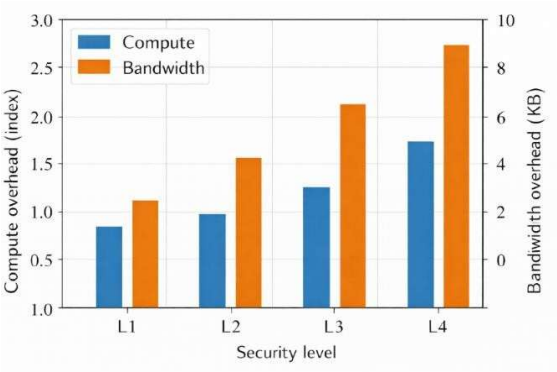

Figure 3. PQC compute and bandwidth overhead scaling

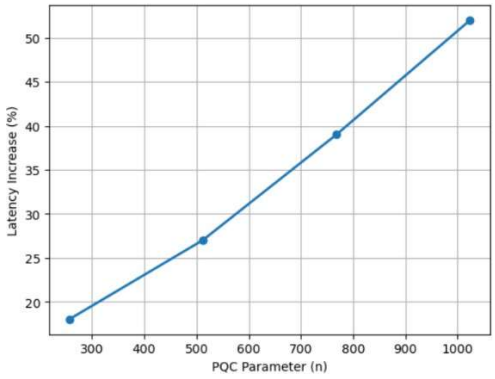

Figure 4. Network latency impact of PQC parameters deployment

C. Deployment Timeline and Cumulative Risk

We then analyze long-term exposure under different rollout strategies.

TABLE III: TRANSITION TIMELINE VS RISK

Strategy	Duration (Years)	Avg. Break Probability	Total Cost Factor	Risk Index
Rapid	3	0.18	1.10	0.82
Moderate	7	0.24	1.38	1.38
Slow	12	0.33	2.40	2.10

The cumulative transition risk values presented in Table III were computed by evaluating the risk functional:

$$R = \int_{t_0}^{t_f} [\omega_1 P_{break}(t) + \omega_2 \phi(C_{total}) + \omega_3 \psi(\alpha(t))]\, dt$$

This evaluation was performed for rapid, moderate, and slow migration timelines. For each strategy, the adoption function $\alpha(t)$was modeled using logistic growth curves with different time constants.

The resulting trajectories are shown in Fig. 5, which compares cumulative risk over time. The curves were generated by numerically integrating the risk function for each deployment schedule. The figure shows that prolonged hybrid states significantly increase total exposure, with slow rollouts accumulating more than twice the risk of rapid deployment.

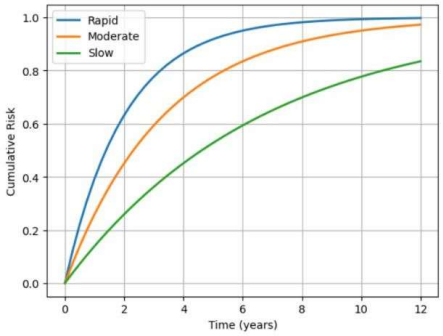

Figure 5. Cumulative transition risk across deployment timelines

D. Security Implications of Classical Components

Finally, we examine how the remaining classical infrastructure limits achievable system security. The results are summarized in Table IV which presents the effective system security level computed for varying shares of legacy cryptography.

TABLE IV: EFFECTIVE SECURITY VS CLASSICAL COMPONENTS SHARE

Classical Share	Classical Strength	PQC Strength	Effective Security
1.00	112 bits	192 bits	112 bits
0.80	112 bits	192 bits	112 bits
0.60	112 bits	192 bits	112 bits
0.40	128 bits	192 bits	128 bits
0.20	128 bits	192 bits	128 bits
0.10	128 bits	192 bits	128 bits
0.05	160 bits	192 bits	160 bits
0.00	—	192 bits	192 bits

For each share value, effective strength was calculated as:

$$\lambda_{eff} = \min(\lambda_C, \lambda_q)$$

where λ_C represents Classical Strength and λ_q represents PQC Strength. This reflects the dominance of the weaker primitive in determining overall system security.

This relationship is illustrated in Fig. 6, which plots effective security level against classical component share. Each data point was calculated by evaluating the minimum-security condition across simulated deployments. The figure confirms that hybrid systems remain constrained by legacy components until their share falls below a critical threshold, emphasizing that PQC deployment alone does not guarantee improved security.

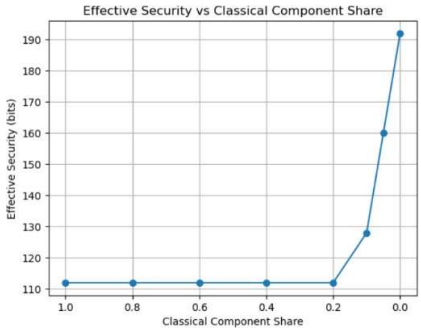

Figure 6. Security Level vs Classical Component Share

V. CONCLUSION

This work analyzed the transition to post-quantum cryptography through a quantitative framework that links deployment progression, performance overhead, and cumulative security exposure. The findings indicate that hybrid coexistence phases play a dominant role in determining system vulnerability, and that slower rollout schedules substantially increase long-term risk accumulation. Performance limitations further influence adoption timelines, indirectly shaping security outcomes. These observations suggest that effective PQC migration requires coordinated planning, awareness of implementation maturity, and timely execution. Future research may extend this framework to domain-specific infrastructures, adaptive threat forecasts, and sector- dependent deployment strategies.

REFERENCES

[1] R. Kumar, A. Sharma, and P. Verma, "Post-quantum cryptography: Algorithm standardization and performance evaluation," Computers & Security, 2022.

[2] A. Cherkaoui Dekkaki, Y. El Bakhari, et al., "Emerging post-quantum cryptography and transition directions," Technologies, 2024.

[3] D. Moody, L. Chen, et al., "Transition to post-quantum cryptography standards," NIST Interagency Report 8547, 2024.

[4] L. Zhang, "Quantum-safe software engineering: A vision for post-quantum cryptography migration," arXiv preprint, 2026.

[5] I. Kong, M. Lopez, et al., "Realizing quantum-safe information sharing," Government Information Quarterly, 2024.

[6] M. Ahmed, S. Hassan, et al., "Survey of post-quantum cryptography support in cryptographic libraries," arXiv preprint, 2025.

[7] R. Campbell, “Enterprise migration to post-quantum cryptography,” Computers, 2025.
[8] A. Demir, H. Kaya, et al., “Performance analysis and industry deployment of post-quantum cryptography algorithms,” arXiv preprint, 2025.
[9] M. Nguyen, T. Günther, et al., “Impact of post-quantum key encapsulation mechanisms on TLS 1.3,” in
[10] Lecture Notes in Computer Science. Springer, 2023.
[11] S. Verma, R. Jain, et al., “Post-quantum cryptography for internet of things: A survey,” arXiv preprint, 2024.
[12] H. Singh, K. Mehta, et al., “Post-quantum cryptography migration in vehicles,” IEEE Access, 2024.
[13] Y. Li, Z. Wang, et al., “Post-quantum cryptography: Migration challenges and strategies,” 2025.
[14] P. Gupta, S. Agarwal, et al., “Post-quantum cryptography research landscape: A scientometric study,”
[15] Journal of Computer Information Systems, 2023.
[16] J. Seo, D. Park, et al., “Hardware circuits and systems design for post-quantum cryptography,” IEEE Trans. Circuits and Systems II, 2024.
[17] F. Günther, M. Brinkmann, et al., “Integrating post-quantum cryptography into TLS: Performance and deployment considerations,” Springer, 2023.
[18] M. A. Ferrag, L. Maglaras, et al., “Post-quantum blockchain security for IoT: A survey,” IEEE Communications Surveys & Tutorials, 2024.
[19] S. S. Alani, M. Al-Kuwaiti, et al., “Recent advances in post-quantum cryptography for networks,” in
[20] Proc. MobiSecServ, 2022.
[21] T. Kim, J. Lee, et al., “Enhancing transportation cyber-physical systems using post-quantum cryptography,” arXiv preprint, 2024.
[22] L. Zhou, P. Wu, et al., “Toward quantum-secured distributed energy systems,” Energies, 2022.
[23] A. Shah, B. Khan, et al., “Review of current cryptographic techniques against post-quantum threats,”
[24] Procedia Computer Science, 2022.
[25] National Institute of Standards and Technology, “Status report on the third round of the post-quantum cryptography standardization process,” 2022.
[26] National Institute of Standards and Technology, “Status report on the second round of the post-quantum cryptography standardization process,” 2020.
[27] W. Beullens, A. Hülsing, et al., “NIST round-three post-quantum digital signature schemes,” in Proc. IEEE Conference, 2024.
[28] K. Patel, R. Desai, et al., “Adoption strategies for post-quantum cryptography: A review,” 2023.
[29] M. R. Hassan, I. Hossain, et al., “Comprehensive framework for post-quantum cryptography migration,” 2025.