

Toward Evidence-Based Post-Quantum Cryptography Migration: A Structured Review of Recent IEEE Access and Related Literature and a Validation-Ready Architecture for a Quantum-Ready Encryption Migration Assistant

Gavhane Vaishnavi Sharad, Prof. Bhosale S.B., Prof. Bangar Abhishek

Dept. of Computer Engineering
Jaihind College of Engineering, Pune, India

Abstract — Post-quantum cryptography (PQC) migration is moving from algorithm design to organisational practice, yet the evidence that should guide migration tools is scattered across process studies, performance experiments, agility surveys and risk models. This paper presents a structured review guided by three research questions: what migration process is supported by the literature, what is known about the performance cost of the new algorithms, and what is missing for automated migration support. Eleven sources were analysed in depth, including recent IEEE Access papers and related surveys, experiments and guidance documents. The review finds that process terminology is still inconsistent, that performance evidence is mostly laboratory-based and per algorithm, that crypto-agility and risk scoring remain largely conceptual, and that cryptographic inventory is the prerequisite for everything else. These findings are converted into seven traceable requirements, which shape a seven-layer architecture for a Quantum-Ready Encryption Migration Assistant mapped to a four-phase migration process. A validation protocol with hypotheses, metrics, baselines and threats to validity is specified so that the assistant can be evaluated in future work. The architecture is conceptual and no experimental results are claimed.

Keywords— Post-Quantum Cryptography, Migration, Crypto-Agility, Cryptographic Inventory, Quantum Risk Assessment, IEEE Access.

I. INTRODUCTION

Public-key cryptography based on factoring and discrete logarithms is vulnerable to Shor's algorithm [1], and resource estimates for breaking RSA-2048 have fallen from about twenty million noisy qubits [2] to under one million [3]. Adversaries can record encrypted traffic now and decrypt it later, so the time data must stay secret plus the time needed to migrate may exceed the time until a capable quantum computer exists [4]. NIST published ML-KEM, ML-DSA and SLH-DSA in 2024 [5] and proposes deprecating quantum-vulnerable algorithms by 2030 and disallowing them by 2035 [6].

Standards define algorithms, but organisations must still find their cryptography, rank risk, choose replacements and execute changes without breaking systems. This paper asks three questions. **RQ1:** what migration process and roles does the literature support? **RQ2:** what is known about the performance and size cost of PQC in realistic protocols and devices? **RQ3:** what is missing for tool support covering inventory, risk, agility and planning? The contributions are a structured comparison of

recent sources, a traceable mapping from evidence gaps to requirements, a seven-layer architecture aligned with a four-phase process, and a validation protocol for future evaluation.

II. REVIEW METHOD

1. Search and Selection

Records were located through web searches of IEEE Access entries (via DOAJ and publisher or institutional repository records), IACR ePrint, arXiv, MDPI and standards bodies, using combinations of post-quantum, migration, crypto-agility, TLS performance, IoT and risk assessment.

The target period was 2021–2025, with one 2020 IEEE Access experiment and one 2020 ETSI report kept as baselines. A source was included if it addressed migration process, algorithm performance in protocols, crypto-agility, inventory or risk assessment and gave a stated method or finding. Opinion pieces and vendor marketing were excluded.

2. Appraisal

Each source was labelled by type (systematic review, survey, experiment, prototype, model, guidance) and its limitation for tooling was recorded (Table I). Evidence from experiments and systematic reviews was weighted above surveys, and theoretical models were treated as proposals. Where only an abstract or repository record could be read, the finding was limited to what that record states.

3. Scope Statement

This is not a Scopus or Web of Science systematic review and no counts of screened records are claimed. Only three IEEE Access papers were verified directly [7]–[9], and the 2021–2023 IEEE Access coverage is therefore thin. Section VIII lists the resulting threats to validity.

III. FINDINGS

1. Migration Process (RQ1)

The systematic review by Näther et al. covers migration approaches for IP networks and reports that terminology, steps and roles are not defined consistently across the literature [7]. From the studies it distils four phases (diagnosis, plan, execution, maintenance) and archetypal roles such as migration manager, asset and risk manager, security expert and developer or administrator [7]. ETSI guidance likewise begins with inventory compilation [17]. A domain survey of migration in vehicles shows that sector-specific constraints are treated separately [8].

2. Performance and Size (RQ2)

TLS experiments agree that the lattice-based schemes are practical. Dilithium and NewHope were studied in TLS with x86 servers and x86 and ARM clients [9]. On embedded devices running TLS 1.3, Kyber, Saber, Dilithium and Falcon performed well in handshake time and energy, with Falcon much faster than Dilithium in the handshake [10]. A later TLS 1.3 study reports no performance drawback from hybrid modes and finds Kyber and HQC comparable to current algorithms [11]. For IoT, a survey concludes that PQC may be feasible on reasonably lightweight devices but that optimisation proposals lack standardisation [12]. Evidence is mostly per algorithm and laboratory based.

3. Agility and Risk (RQ3)

A survey of crypto-agility seeks a unified definition and argues that agility is needed beyond PQC itself [13]. An enterprise approach orchestrates cryptographic providers through policy and has been prototyped in a service mesh [14]. On risk, a quantum-adjusted risk score extends Mosca's inequality into a

multi-factor formula [15], but it is presented as a theoretical and methodological contribution. A broad 2025 survey covers taxonomy, performance, hardware acceleration, side-channel resistance and hybrid migration [16]. Algorithm confidence can also change, as the breaks of Rainbow [21] and SIDH [22] show.

IV. COMPARATIVE ANALYSIS

Table I compares the sources. They differ in type and scope, so no single metric is computed.

Table 1: Comparison of Analysed Sources

Source, year	Type	Relevant finding	Limit for tooling
Näther et al., 2024, IEEE Access [7]	Systematic review	Four migration phases (diagnosis, plan, execution, maintenance) and archetypal roles; terminology and steps inconsistent across the literature	Process level; no tool evaluated
Lohmiller et al., 2025, IEEE Access [8]	Survey (vehicles)	Domain-specific survey of PQC migration in vehicles	Full text not accessed in this review
De Abiega-L'Eglise et al., 2020, IEEE Access [9]	Experiment	Dilithium and NewHope in TLS; x86 server, x86 and ARM clients	Pre-standard variants; TLS only
Tasopoulos et al., 2021 [10]	Experiment	Kyber, Saber, Dilithium, Falcon in TLS 1.3 on embedded devices; Falcon handshake much faster than Dilithium	Round-3 candidates; embedded boards only
Sosnowski et al. [11]	Experiment	No performance drawback from hybrid modes; Kyber and HQC comparable to current algorithms; Dilithium and Falcon faster	Laboratory network emulation
Liu et al., 2024 [12]	Survey (IoT)	PQC feasible on reasonably lightweight IoT; optimisation work lacks standardisation	No planning method

Alnahawi et al., 2023 [13]	Survey	Unifies crypto-agility definitions, requirements and challenges	No operational tool
Sikeridis et al., 2023 [14]	Prototype	Policy-driven orchestration of cryptographic providers, prototyped in a service mesh	One architecture; scale evidence limited
Grigaliūnas, Brūzgienė, 2025 [15]	Model	Quantum-Adjusted Risk Score extends Mosca's inequality to several factors	Theoretical and methodological
ETSI TR 103 619, 2020 [17]	Guidance	Stage-based migration starting with inventory compilation	Manual; not automated
Chhetri et al., 2025 [16]	Survey	Taxonomy, performance, hardware acceleration, side channels, agility, hybrid migration	Broad; not tool-focused

Three patterns emerge. First, process knowledge [7], [17] and performance knowledge [9]–[12] exist separately, and no source joins them. Second, agility [13], [14] and risk [15] work is conceptual or prototype-level. Third, inventory is a prerequisite stated in guidance [17] and supported by the CBOM format [19], but automated discovery is not demonstrated in the sources reviewed.

Table 2: From Evidence Gaps to Requirements

Gap in evidence	Derived requirement	Basis
Inconsistent process terms and roles	R1: follow a four-phase process and role-aware outputs	[7]
Inventory must precede risk assessment	R2: automated discovery with CBOM output	[17], [19]
Risk models are mostly theoretical	R3: transparent, configurable risk score with input provenance	[4], [15]
Performance reported per algorithm in labs	R4: impact estimator from published benchmarks, checked by local tests	[9]–[12]
Agility lacks operational tooling	R5: policy-driven algorithm selection and plans with rollback	[13], [14]
Algorithm status can change	R6: update feed and hybrid default	[21], [22]
Domain constraints (IoT, vehicles)	R7: device-profile constraints in recommendations	[8], [12]

V. PROPOSED ARCHITECTURE

The architecture in Fig. 1 realises requirements R1–R7. Layers 1–3 correspond to the diagnosis phase [7], layers 4–6 to planning and execution support, and layer 7 to maintenance. It is conceptual and not experimentally validated.

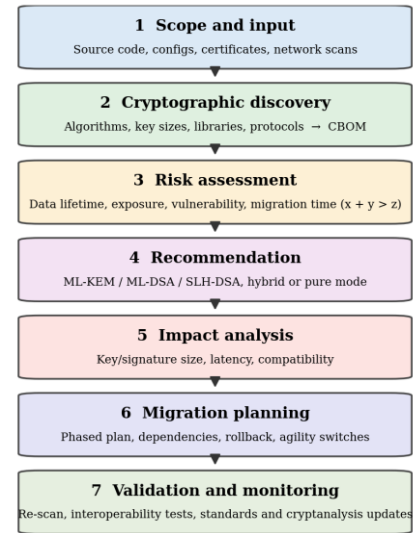


Fig. 1. Seven-layer conceptual architecture of the Quantum-Ready Encryption Migration Assistant.

- *Scope and input* (R1). Repositories, configurations, certificates, scan results and role information.
- *Discovery* (R2). Detects algorithms, key sizes, libraries and protocols and emits a CBOM [19].
- *Risk assessment* (R3). Scores assets from data lifetime, exposure and migration time using Mosca's inequality [4], with every input traceable.
- *Recommendation* (R5, R6, R7). Maps vulnerable assets to ML-KEM, ML-DSA or SLH-DSA, hybrid by default, under device-profile constraints [5].
- *Impact analysis* (R4). Estimates size and latency effects from published measurements [9]–[12] and flags assets needing local tests.
- *Migration planning* (R5). Phased plans, dependencies, rollback and configuration-driven switches.
- *Validation and monitoring* (R6). Re-scans, interoperability tests and updates when algorithm status changes [21], [22].

Validation Protocol

The following protocol is specified so that the assistant can be evaluated; no results are reported here. **H1**: automated

discovery finds at least as many cryptographic usages as a manual audit, measured by precision and recall against a ground-truth set of repositories with known cryptographic calls. **H2:** risk rankings agree with expert rankings, measured by rank correlation on the same assets. **H3:** estimated handshake size and latency are close to measured values on a testbed built with Open Quantum Safe tools [20]. Baselines are manual audit and keyword search. Planned reporting includes the repository selection rule, versions of all libraries, repeated measurements with spread, and grouped splits so that related projects do not appear in both calibration and test data.

VI. RESEARCH GAPS

(i) No source reviewed couples inventory, risk, impact and planning. (ii) Performance data are per algorithm and mostly laboratory based [9]–[12]. (iii) Risk and agility proposals lack empirical validation [14], [15]. (iv) Process terminology and roles need standardising [7]. (v) Algorithm status must be monitored [21], [22]. (vi) Domain-specific constraints in vehicles and IoT need to be encoded in tools [8], [12].

Threats to Validity

Search was web-based and not a database-logged systematic search, so relevant papers may be missing. Only three IEEE Access papers were verified, and for [8] only bibliographic details were available. Several sources are preprints or repository records. Findings from abstracts may omit caveats in full texts. The architecture and protocol are proposals, not results.

VII. CONCLUSION

The recent literature gives a process model, performance evidence, agility concepts and risk formulas, but no integrated and validated migration tool. Converting these gaps into seven requirements shows where an assistant adds value: discovery, traceable risk, impact estimation and agile planning. Future work should implement the assistant and evaluate it with the stated protocol.

REFERENCES

1. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.
2. C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.
3. C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv:2505.15917, 2025.
4. M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.
5. National Institute of Standards and Technology, "FIPS 203, FIPS 204 and FIPS 205: ML-KEM, ML-DSA and SLH-DSA standards," Aug. 2024.
6. National Institute of Standards and Technology, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547, initial public draft, Nov. 2024.
7. C. Näther, D. Herzinger, S.-L. Gazdag, J.-P. Steghöfer, S. Daum, and D. Loebenberger, "Migrating software systems toward post-quantum cryptography – A systematic literature review," *IEEE Access*, vol. 12, pp. 132107–132126, 2024, doi: 10.1109/ACCESS.2024.3450306.
8. N. Lohmiller, S. Kaniewski, M. Menth, and T. Heer, "A survey of post-quantum cryptography migration in vehicles," *IEEE Access*, vol. 13, pp. 10160–10176, 2025, doi: 10.1109/ACCESS.2025.3528562.
9. A. F. De Abiega-L'Eglise et al., "Performance of New Hope and CRYSTALS-Dilithium postquantum schemes in the Transport Layer Security protocol," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3040324.
10. G. Tasopoulos, J. Li, A. P. Fournaris, R. K. Zhao, A. Sakzad, and R. Steinfeld, "Performance evaluation of post-quantum TLS 1.3 on embedded systems," *IACR Cryptol. ePrint Arch.*, Paper 2021/1553, 2021.
11. M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, and G. Carle, "The performance of post-quantum TLS 1.3," in *Proc. Companion 19th Int. Conf. Emerging Netw. Exp. Technol. (CoNEXT Companion '23)*, Paris, France, Dec. 2023, doi: 10.1145/3624354.3630585.
12. T. Liu et al., "Post-quantum cryptography for Internet of Things: A survey on performance and optimization," arXiv:2401.17538, 2024.
13. N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann, and T. Grasmeyer, "On the state of crypto-agility," *IACR Cryptol. ePrint Arch.*, Paper 2023/487, 2023.
14. D. Sikeridis et al., "ELCA: Introducing enterprise-level cryptographic agility for a post-quantum era," *IACR Cryptol. ePrint Arch.*, Paper 2023/1539, 2023.
15. Š. Grigaliūnas and R. Brūzgienė, "Towards a unified quantum risk assessment," *Electronics*, vol. 14, no. 17, Art. 3338, 2025, doi: 10.3390/electronics14173338.
16. G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," arXiv:2510.10436, 2025.

17. ETSI, “Migration strategies and recommendations to quantum safe schemes,” ETSI TR 103 619 V1.1.1, Jul. 2020.
18. N. Ott, C. Peikert, et al., “Identifying research challenges in post quantum cryptography migration and cryptographic agility,” arXiv:1909.07353, 2019.
19. OWASP CycloneDX, “Cryptography Bill of Materials (CBOM),” CycloneDX specification v1.6, 2024.
20. D. Stebila and M. Mosca, “Post-quantum key exchange for the Internet and the Open Quantum Safe project,” in *SAC 2016*, LNCS 10532, Springer, 2017.
21. W. Beullens, “Breaking Rainbow takes a weekend on a laptop,” in *CRYPTO 2022*, LNCS 13508, Springer, 2022.
22. W. Castryck and T. Decru, “An efficient key recovery attack on SIDH,” in *EUROCRYPT 2023*, LNCS 14008, Springer, 2023.
23. [Add citation: 2025 research paper.pdf]
24. [Add citation: CRYSTALS-Dilithium paper]