electronics

MDPI

Systematic Review

Post-Quantum Cryptography Migration in Communication Networks: A Systematic Review of Protocol Integration, Performance Trade-Offs, and Transition Readiness

Merve Güllü [1,*,†] and Esra Söğüt [2,†]

[1] Turk Telekom R&D, Ankara 06080, Türkiye
[2] Department of Computer Engineering, Faculty of Technology, Gazi University, Ankara 06560, Türkiye; esrasogut@gazi.edu.tr
* Correspondence: merve.gullu@turktelekom.com.tr
† These authors contributed equally to this work.

Abstract

The prospect of a cryptographically relevant quantum computer (CRQC) undermines the public-key primitives that secure virtually every layer of modern communication networks, from subscriber authentication in cellular cores to transport-layer key exchange. Adversaries already following a harvest-now, decrypt-later (HNDL) strategy make this threat actionable today for any traffic whose confidentiality must outlast a decade. Following NIST's finalisation of the first post-quantum cryptography (PQC) standards, ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in August 2024, and the selection of HQC as a fourth key-encapsulation candidate in March 2025, research has shifted from algorithm design to network-level integration. This paper reports a PRISMA-2020-compliant systematic literature review of PQC migration in communication networks, structured around five research questions covering protocol and scenario coverage, quantitative performance impact, hybrid cryptography strategies, transition barriers, and open research gaps. Six databases (IEEE Xplore, Scopus, Web of Science, ACM Digital Library, SpringerLink, and MDPI) were searched (3229 records identified); after deduplication, title-keyword screening, full-text eligibility assessment, and a pre-specified quality appraisal (Q1–Q6, threshold $\geq 3/6$) applied to 310 eligible studies, a final synthesis corpus of 141 studies (68 journal articles, 68 conference papers, 4 conference-derived book chapters, 1 workshop paper) was screened, quality-appraised, and synthesised narratively with supporting evidence tables. The review finds that transport-layer protocols (TLS 1.3, QUIC, DTLS 1.3) dominate the literature, that lattice-based ML-KEM/ML-DSA offer the most favourable latency–bandwidth–energy trade-off among standardised families, and that classical–PQC hybrid schemes are the de facto transition strategy across 5G/6G, IoT, VPN, and automotive scenarios, at the cost of 10–100× larger keys/signatures and 8–40% handshake latency overhead. Persistent barriers include constrained-device resource limits, immature hardware acceleration, incomplete IETF/3GPP standardisation, and public-key-infrastructure scaling. We propose a five-level PQC transition-readiness maturity model and identify large-scale field validation, PQC–QKD integration, and lightweight signature schemes as priority directions for future work.

Keywords: post-quantum cryptography; 5G security; 6G; IoT protocols; hybrid KEM; crypto-agility; harvest-now decrypt-later; NIST standards; communication network security

Check for updates

Academic Editor: George Angelos Papadopoulos

Received: 31 August 2026
Revised: 23 September 2026
Accepted: 5 October 2026
Published: 11 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The emergence of large-scale quantum computers poses an existential threat to public-key cryptography. Shor's algorithm [1] renders RSA and ECC, the foundation of modern communication security, solvable in polynomial time, while Grover's algorithm [2] effectively halves the security margin of symmetric cyphers. Communication networks are, by their nature, among the most exposed systems: cryptographic mechanisms permeate every protocol layer, from physical-layer authentication to application-layer key exchange [3].

1.1. Motivation and Problem Statement

HNDL attack model [4] is particularly consequential for telecommunications. Adversaries can capture and archive encrypted traffic today, subscriber credentials, roaming authentication data, enterprise VPN sessions, and decrypt it once a CRQC becomes available. Since conservative estimates place CRQC availability between 2030 and 2040, any data whose confidentiality must persist beyond five years is already at risk [5–7].

1.2. The NIST Standardisation Milestone

In August 2024, NIST published its first three PQC standards: FIPS 203 (ML-KEM, based on CRYSTALS-Kyber), FIPS 204 (ML-DSA, based on CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, based on SPHINCS+). In March 2025, HQC was selected as a fourth KEM to provide algorithmic diversity. These developments mark the transition from research-stage algorithm evaluation to production-stage engineering, with far-reaching implications for the entire communication ecosystem.

1.3. The Gap in Communication-Specific Coverage

Although the PQC literature is broad, existing surveys largely evaluate cryptographic algorithms in isolation or against generic software benchmarks, rather than in situ within communication systems [8–13]. Communication networks, however, carry distinctive constraints: strict latency budgets for 5G URLLC, severely limited resources on IoT endpoints, backward-compatibility requirements at core-network interfaces, and multi-vendor interoperability in roaming scenarios [8,12,14–17]. These network-specific dimensions are scattered across the literature and lack a unifying synthesis [8,10,16,18,19].

1.4. Research Questions

This systematic review is structured around five research questions (RQs):

RQ1 Which communication protocol layers, network deployment scenarios, and PQC algorithm families have been studied in the existing literature?

RQ2 What is the quantitative performance impact (latency, bandwidth, computational cost, energy) of PQC algorithms across communication environments?

RQ3 How are classical–PQC hybrid cryptography strategies implemented in communication infrastructure, and what is their security and operational effectiveness?

RQ4 What technical, standardisation, and operational barriers impede PQC transition in telecommunication and communication infrastructure?

RQ5 Which communication scenarios and technical problems remain under-researched, and what are the priority directions for future work?

1.5. Scope and Contributions

This review covers primary studies published between January 2019 and March 2026, spanning the period from the second round of the NIST PQC competition to final standard-

isation and early post-standardisation deployment studies. The principal contributions are as follows:

(1) A PRISMA-2020-compliant systematic synthesis of PQC integration research across communication protocols and network scenarios;
(2) A quantitative performance-evaluation framework enabling cross-study comparison of PQC overhead in networked contexts;
(3) A classification of hybrid cryptography strategies used in real or emulated communication environments;
(4) A structured taxonomy of PQC transition barriers and a five-level maturity model for telecommunications readiness;
(5) A prioritised map of critically under-studied research gaps.

1.6. Paper Organisation

The remainder of this paper is organised as follows. Section 3 reviews related surveys. Section 4 details the systematic review methodology. Section 5 provides technical background on PQC standards and communication protocol security. Section 6 addresses RQ1 (protocol and scenario mapping). Section 7 addresses RQ2 (performance analysis). Section 8 addresses RQ3 (hybrid strategies). Section 9 addresses RQ4 (transition barriers). Section 10 addresses RQ5 (research gaps). Section 11 presents cross-cutting discussion and the maturity model, and Section 12 concludes.

2. Abbreviations

For readability, Table 1 lists the abbreviations used throughout this paper. Each term is spelled out at its first occurrence in the running text and abbreviated thereafter.

Table 1. List of abbreviations.

Abbrev.	Definition
PQC	Post-Quantum Cryptography
CRQC	Cryptographically Relevant Quantum Computer
HNDL	Harvest-Now, Decrypt-Later
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standard
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
KEM	Key-Encapsulation Mechanism
ECC/ECDH/ECDSA	Elliptic-Curve Cryptography/Diffie–Hellman/Digital Signature Algorithm
TLS	Transport Layer Security
QUIC	Quick UDP Internet Connections
DTLS	Datagram TLS
IKEv2	Internet Key Exchange, version 2
IPsec	Internet Protocol Security
MQTT/CoAP	Message Queuing Telemetry Transport/Constrained Application Protocol
DNSSEC	Domain Name System Security Extensions
SSH	Secure Shell
5G/6G	Fifth-/Sixth-Generation Mobile Network
SBA	Service-Based Architecture
VNF	Virtualised Network Function
SUCI/AKA	Subscription Concealed Identifier/Authentication and Key Agreement
URLLC	Ultra-Reliable Low-Latency Communication
IoT/IIoT	(Industrial) Internet of Things
WSN	Wireless Sensor Network
UAV/UTM	Unmanned Aerial Vehicle/UAV Traffic Management
IoV/V2X	Internet of Vehicles/Vehicle-to-Everything
CAN	Controller Area Network
STIN	Satellite–Terrestrial Integrated Network
QKD	Quantum Key Distribution
PLS	Physical-Layer Security
HSM	Hardware Security Module
FPGA/ASIC	Field-Programmable Gate Array/Application-Specific Integrated Circuit
PKI	Public Key Infrastructure
CRL/OCSP	Certificate Revocation List/Online Certificate Status Protocol

Table 1. *Cont.*

Abbrev.	Definition
HKDF	HMAC-Based Key Derivation Function
NTT	Number-Theoretic Transform
TTFB	Time-to-First-Byte
UE	User Equipment
RAM	Random-Access Memory
OTA	Over-the-Air (update)
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
AMSTAR-2	A MeaSurement Tool to Assess systematic Reviews, v.2
RQ	Research Question

3. Related Work

Following NIST's 2024 standardisation, the rapid growth of PQC research has produced a substantial body of survey literature. To contextualise the present work, we organise existing surveys into four thematic clusters and identify the gaps that these studies do not jointly address. A multi-dimensional comparison is presented in Table 2.

IoT-centric surveys form the largest cluster [10,11,18,20–22]. These studies consistently show that lattice-based schemes, CRYSTALS-Kyber in particular, offer the best security–efficiency trade-off for resource-constrained devices, and several adopt a PRISMA-based methodology [10,18,22]. However, their performance evaluation is almost entirely computation-centric (key size, CPU cycles, RAM), leaving network-layer behaviour out of scope.

5G/6G-centric surveys [12,16,17] examine PQC integration into next-generation cellular architectures, covering handshake protocols, AKA mechanisms, and hybrid QKD–PQC configurations. While these studies address transport- and application-layer integration effectively, they offer limited assessment of how PQC overhead propagates to the network and data-link layers, or of how operators should manage the transition from existing cellular infrastructure.

Hardware- and infrastructure-centric surveys [13,23,24] approach PQC from a deployment perspective, proposing ASIC/FPGA acceleration and evaluating lattice-based schemes for smart-grid and edge/fog deployments. Although they offer valuable implementation insights, they do not provide a structured transition roadmap for heterogeneous network environments.

Standards- and protocol-centric surveys [8,19] examine the integration of the finalised NIST cryptographic suite into existing internet and cellular protocols. These studies identify large parameter sizes as the principal engineering obstacle, but acknowledge that architectural solutions for distributing this parameter overhead and preventing downgrade attacks remain immature.

The multi-dimensional analysis presented in Table 2 reveals five structural gaps across the literature. First, protocol integration is almost always treated as a single-layer problem, and most studies do not descend below the transport layer; data-link-layer (MACsec) and network-layer (IPsec) integration are addressed only partially, and only by a limited number of studies [8,13,16]. Second, performance evaluation is confined to computational metrics; the effect of PQC-induced packet fragmentation on retransmission behaviour under degraded network conditions and on handshake completion rates is overlooked in nearly all studies. Third, transition is framed purely as an algorithm-selection problem; none of the existing studies offers a framework integrating system inventory, certification timelines, and regulatory-compliance processes. Fourth, crypto-agility, the ability to dynamically switch cryptographic primitives as new vulnerabilities emerge, is mentioned but not treated structurally. Fifth, the interaction of PQC overhead with the handshake mechanisms of lightweight IoT protocols (MQTT, CoAP, LoRaWAN) has only been partially examined;

even in the most protocol-aware studies, network-level stress factors are explicitly left out of scope [10].

This study addresses all five of these gaps within a unified systematic review framework, combining cross-layer protocol-integration analysis (from the physical to the application layer), network-condition-aware performance evaluation, and a structured organisational transition-readiness model. To the best of our knowledge, this is the first study to address these three dimensions simultaneously.

Table 2. Comparative scope analysis of PQC survey literature. Coverage indicators: ● Full, ◕ Partial, ○ Minimal, — Not addressed. Multi-layer protocol refers to systematic coverage spanning ≥3 OSI layers. Network-level metrics include packet loss, retransmission timeout, and handshake failure rate analysis. The proposed study (last row, shaded) addresses all five identified research gaps.

Study	Year	Algorithm and Cryptographic			Network and Protocol			Performance Evaluation			Migration	
		Algorithm Analysis	Hybrid Schemes	Standards Alignment	Multi-layer Protocol	IoT Protocols	5G/6G Integration	Computational Overhead	Network-level Metrics	Hardware Evaluation	Org. Transition Readiness	Crypto-Agility
Cluster A: IoT-Centric Surveys												
Fortifying Future IoT Security: Lightweight PQC [20]	2025	●	○	◕	—	◕	—	◕	—	●	—	—
Systematic Review on Securing IoT Systems with PQC [18]	2026	●	◕	●	○	●	—	◕	—	○	○	○
Resilience of PQC in Lightweight IoT Protocols [10]	2025	◕	○	◕	○	●	—	◕	◕	○	—	—
Resource-Efficient Cryptography for IoT [21]	2026	●	●	◕	○	◕	—	◕	—	◕	—	—
PQC in Blockchain and IoT: Advances and Applications [11]	2025	●	●	◕	○	◕	—	◕	—	○	○	○
PQC Standards for Future-Proof IoT Security [22]	2025	●	◕	●	○	◕	—	◕	—	○	○	○
Cluster B: 5G/6G Surveys												
Pre vs. Post Quantum Security for 5G-IoT [12]	2025	●	●	◕	○	◕	●	◕	○	◕	○	○
Quantum Cryptography in 5G Networks [16]	2024	●	◕	●	◕	○	●	◕	○	●	○	○
6G Authentication and Key Agreement (AKA) [17]	2026	●	●	●	◕	◕	●	◕	○	◕	◕	○
Cluster C: Hardware and Infrastructure Surveys												
Exploration of Cryptoprocessors for IoT [23]	2024	◕	—	◕	—	○	—	○	—	●	—	—
Edge-Fog Enhanced Post-Quantum Security [24]	2025	◕	◕	◕	○	○	○	◕	○	◕	○	○
Lattice-Based Security for Smart-Grid Networks [13]	2024	●	◕	◕	◕	—	—	◕	—	○	○	—
Cluster D: Standards and Protocol Surveys												
PQC in Networking Protocols: Challenges and Solutions [8]	2026	●	◕	●	◕	◕	◕	◕	○	○	○	○
Cybersecurity Threats to Wireless Infocommunications [19]	2025	●	●	◕	○	○	◕	◕	○	◕	○	○
This Study	2026	●	●	●	●	●	◕	●	●	◕	●	●

4. Methodology

This review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses, (PRISMA 2020) guidelines [25]. This review was not prospectively registered in a public register (e.g., PROSPERO), and no separate review protocol document was prepared prior to conducting the review. The research questions, search strategy, and eligibility criteria reported in this section were nonetheless defined in advance of full-text screening and were applied without post hoc modification.

4.1. Search Strategy

4.1.1. Databases

Six electronic bibliographic databases were searched: IEEE Xplore, Scopus, Web of Science, ACM Digital Library, SpringerLink, and MDPI. The latter two were included to capture pre-print and open-access venues given the rapid pace of PQC deployment research (see Section 4.4).

4.1.2. Boolean Query

The primary search string, adapted per database syntax, was: ("post-quantum" OR "postquantum" OR "PQC") AND ("communication" OR "network" OR "5G" OR "6G" OR "TLS" OR "IoT" OR "IPsec" OR "QUIC" OR "MQTT" OR "CoAP" OR "telecom").

Searches were limited to title, abstract, and keywords. No language restriction was imposed at the search stage; however, only English-language full texts were retained at the eligibility screening stage. All six database searches were executed on a single day, 24 March 2026, to ensure a consistent, reproducible snapshot of the literature across sources; the per-database record counts (IEEE Xplore: 656; Scopus: 1513; Web of Science: 751; ACM Digital Library: 127; SpringerLink: 33; MDPI: 149; total: 3229) reflect this search date.

4.2. Inclusion and Exclusion Criteria

Table 3 summarises the eligibility criteria applied during abstract and full-text screening.

Table 3. Inclusion and exclusion criteria.

Criterion	Description
Inclusion criteria	
IC1	Published January 2019 – March 2026
IC2	Peer-reviewed journal, conference, or workshop paper; or IACR ePrint/arXiv with $\geq$10 citations
IC3	Addresses at least one communication protocol, network architecture, or deployment scenario
IC4	Contains experimental measurements, protocol analysis, or systematic evaluation of PQC in a communication context
IC5	Full text available in English
Exclusion criteria	
EC1	Purely algorithmic analysis without communication-context evaluation
EC2	Considers only classical cryptography or QKD without PQC
EC3	Duplicate, extended abstract, poster, or non-archival workshop abstract
EC4	Grey literature (white papers, vendor reports) without peer review
EC5	Insufficient methodological detail to extract findings

4.3. Screening Process

Screening was conducted in two stages by two independent reviewers (Reviewers 1 and 2). In Stage 1, titles and abstracts of all retrieved records were screened against IC1–IC5 and EC1–EC5. In Stage 2, full texts of remaining candidates were assessed. Conflicts were resolved through discussion; unresolved conflicts were arbitrated by a third reviewer. The resulting study-selection process, from identification to inclusion, is summarised in the PRISMA 2020 flow diagram in Figure 1.

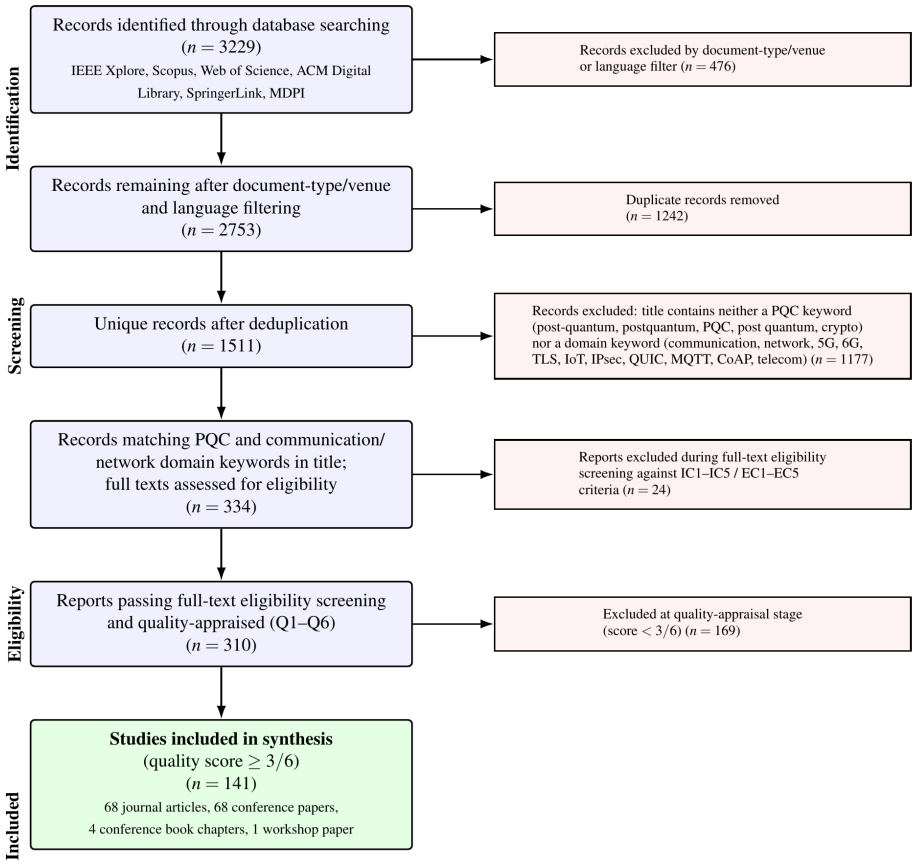


Figure 1. PRISMA 2020 flow diagram showing the study selection process across identification, screening, eligibility, and inclusion stages.

4.4. Quality Assessment

Included studies were assessed using a quality checklist adapted from AMSTAR-2 [26] and tailored for empirical computer-science research [27]. The checklist comprises six items, each scored 0 (absent), 0.5 (partial), or 1 (present), for a maximum score of 6:

Q1. Clear research question or objective stated.
Q2. Reproducible experimental or evaluation setup.
Q3. Defined baseline or comparison point.
Q4. Measurement validity and statistical rigour.
Q5. Real-network vs. simulation clearly distinguished.
Q6. Limitations and threats to validity discussed.

The quality appraisal against criteria Q1–Q6 was conducted independently by the same two reviewers (Reviewers 1 and 2) responsible for title/abstract and full-text screening (Section 4.3). Scoring discrepancies exceeding one point on any single criterion were resolved through discussion, with unresolved conflicts arbitrated by a third reviewer, consistent with the screening procedure. Studies scoring below the pre-specified threshold of 3/6 were excluded at the quality-appraisal stage; in addition, the score was used as a descriptive stratification variable and in the threshold-sensitivity analysis reported below to test how the size of the evidence base changes under progressively stricter quality cut-offs.

Each of the 310 records that passed full-text eligibility screening was appraised against six quality criteria (Q1–Q6), with every criterion scored as met (1), partially met (0.5), or not met (0), yielding a total quality score between 0 and 6. The six criteria assessed, respectively, whether the study (Q1) stated a clear objective, (Q2) described its experimental setup, (Q3) reported a comparative baseline, (Q4) applied rigorous measurement procedures,

(Q5) distinguished real-hardware from simulation-based evaluation, and (Q6) explicitly discussed its limitations. Of the 310 appraised records, 145 were journal articles and 165 were conference-venue records (conference papers, conference-derived book chapters, and workshop papers); all analyses below report results both for the full appraised pool and, where relevant, stratified by publication venue.

4.4.1. Quality-Score Distribution and the Inclusion Threshold

A pre-specified inclusion rule was applied to the appraised pool: studies scoring at least 3 out of 6 (i.e., meeting or exceeding 50% of the maximum attainable score) were carried forward into the synthesis corpus, while studies scoring below this threshold were excluded at the quality-appraisal stage. As shown in Figure 2, this rule is a clean separator of the appraised pool: no study scoring below 3 was retained and no study scoring 3 or above was excluded, so the threshold reproduces the recorded inclusion decision for all 310 records without a single exception. Applying it yields a final synthesis corpus of $n = 141$ studies, with the remaining $n = 169$ records excluded on quality grounds. The distribution is visibly bimodal around the cut-point: scores below 3 are concentrated at 1.5 and 2.5 points ($n = 69$ and $n = 96$, respectively), whereas scores at or above 3 are more evenly spread across 3, 4, 5, and 6 points ($n = 29$, 47, 39, and 26), indicating that the excluded studies form a fairly homogeneous low-quality cluster rather than being scattered arbitrarily below an otherwise continuous distribution.

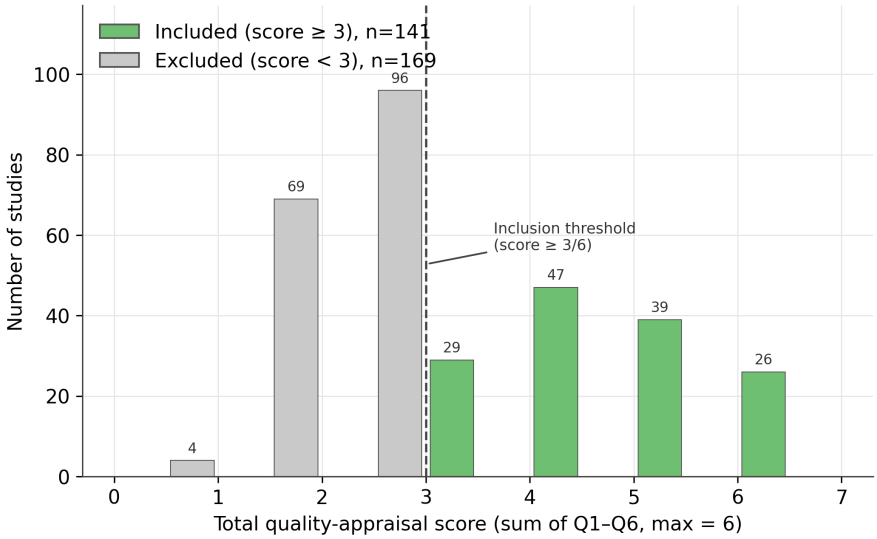


Figure 2. Distribution of total quality score (sum of Q1–Q6, $n = 310$ appraised studies), with the studies retained above the $\geq 3/6$ inclusion threshold shown in green ($n = 141$) and those excluded shown in grey ($n = 169$).

4.4.2. Sensitivity of the Corpus Size to the Quality Threshold

To assess whether the chosen cut-point was arbitrary, we recomputed the retained-study count at every integer threshold from 1 to 6 (Figure 3). Retention falls from 98.7% ($n = 306$) at ≥ 1 to 76.5% ($n = 237$) at ≥ 2, then drops sharply to 45.5% ($n = 141$) at ≥ 3, before declining more gradually to 36.1% ($n = 112$) at ≥ 4, 21.0% ($n = 65$) at ≥ 5, and 8.4% ($n = 26$) at ≥ 6. The steepest single-step decline in the entire curve occurs between the ≥ 2 and ≥ 3 thresholds (a 31-percentage-point drop), after which the curve flattens into a more gradual, near-linear decline. This inflexion identifies ≥ 3 as a natural separating point in the data, rather than an arbitrary round-number cut-off, and supports its use as the inclusion rule for the review.

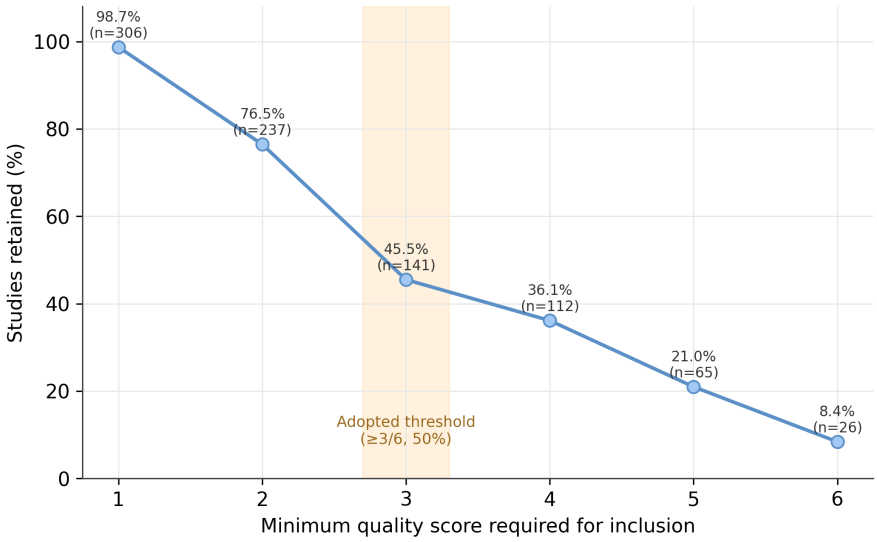


Figure 3. Cumulative proportion of the 310 appraised studies retained as a function of the minimum quality-score threshold. The adopted threshold (≥3/6, 50%) sits immediately after the steepest single-step drop in the retention curve.

4.4.3. Quality by Publication Venue: Ruling out Selection Bias

Because the inclusion rule operates purely on the total quality score, a valid concern is whether it implicitly favours one publication venue over another. We therefore compared quality scores between journal articles ($n = 145$) and conference-venue records ($n = 165$) across the full appraised pool, prior to threshold-based exclusion (Figure 4). Journal articles recorded a marginally higher mean quality score than conference-venue records (3.18 vs. 3.10), and both groups shared an identical median of 2.5, with substantially overlapping interquartile ranges. A Mann–Whitney U test confirmed that this difference was not statistically significant ($U = 12{,}642.5$, $p = 0.377$), with a negligible effect size (rank-biserial $r = 0.06$). Publication venue therefore does not meaningfully predict quality-appraisal outcome in this corpus, indicating that the quality-based inclusion rule does not systematically favour journal articles over conference-venue work, or vice versa.

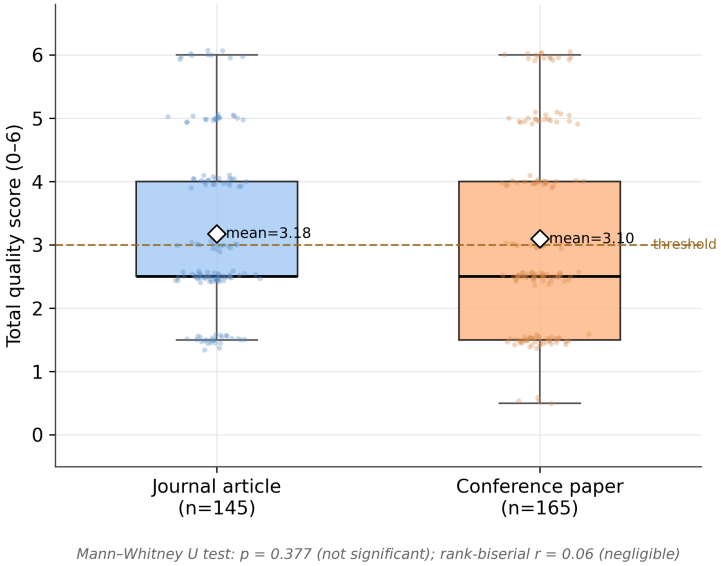


Figure 4. Total quality score by publication venue across the full appraised pool ($n = 310$). Diamonds denote group means; the annotation reports the Mann–Whitney U test result and rank-biserial effect size.

4.4.4. Fulfilment of Individual Criteria in the Included Corpus

Because the quantitative synthesis in Sections 6–10 draws exclusively on the $n = 141$ studies that passed the quality threshold, we additionally disaggregated criterion fulfilment (Q1–Q6) within this final corpus, split into 68 journal articles and 73 conference-venue records (Figure 5). Reporting of the study objective (Q1) was universal (100% in both groups). Fulfilment declined progressively across the remaining criteria for the corpus as a whole: description of the experimental setup (Q2) was met by 92.9% of included studies (91.2% journal, 94.5% conference), a comparative baseline (Q3) by 85.1% (86.8% journal, 83.6% conference), and rigorous measurement procedures (Q4) by 72.3% (75.0% journal, 69.9% conference). The distinction between real-hardware and simulation-based evaluation (Q5) was met by 61.0% of included studies overall, with conference-venue records slightly ahead of journal articles (64.4% vs. 57.4%). Explicit discussion of limitations (Q6) was the weakest criterion by a wide margin, met by only 32.6% of included studies overall, and was the only criterion on which conference-venue records clearly outperformed journal articles (42.5% vs. 22.1%). This pattern indicates that, even within the quality-filtered synthesis corpus, transparent reporting of threats to validity remains the field's most underdeveloped methodological practice, and that this gap is more pronounced among journal articles than among conference-venue records.

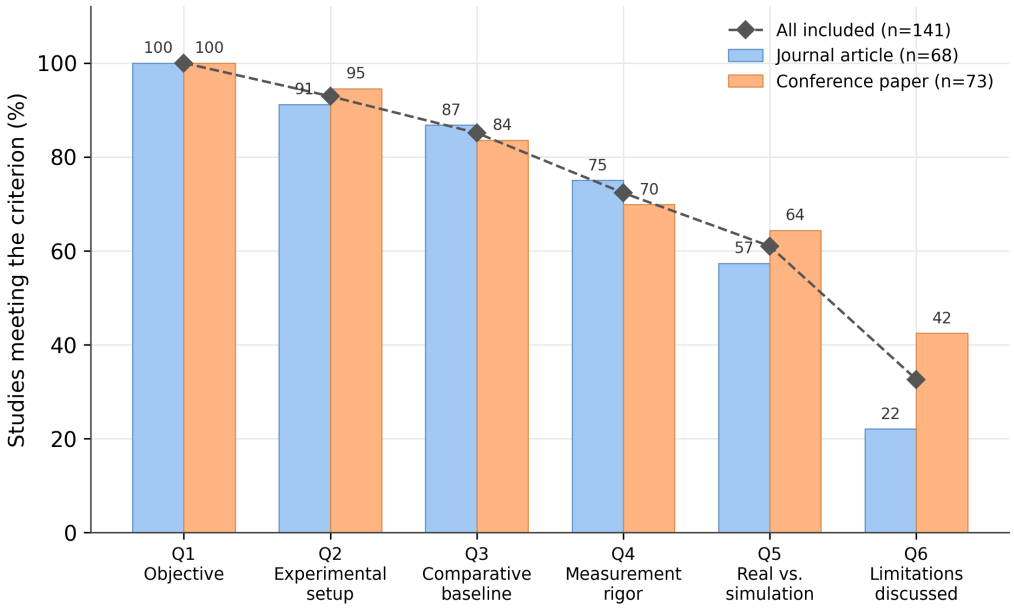


Figure 5. Proportion of the 141 included studies meeting each quality criterion (Q1–Q6), overall and by publication venue.

4.4.5. Composition of the Included Corpus

Figure 6 summarises the publication-venue composition of the final 141-study synthesis corpus: 68 journal articles (48.2%), 68 conference papers (48.2%), 4 conference-derived book chapters (2.8%), and 1 workshop paper (0.7%). The near-equal split between journal and conference-venue evidence, combined with the absence of a statistically significant quality difference between the two groups (Section 4.4, above), indicates that the corpus synthesised in this review draws on a balanced and quality-controlled evidence base rather than being dominated by, or biassed against, either publication type.

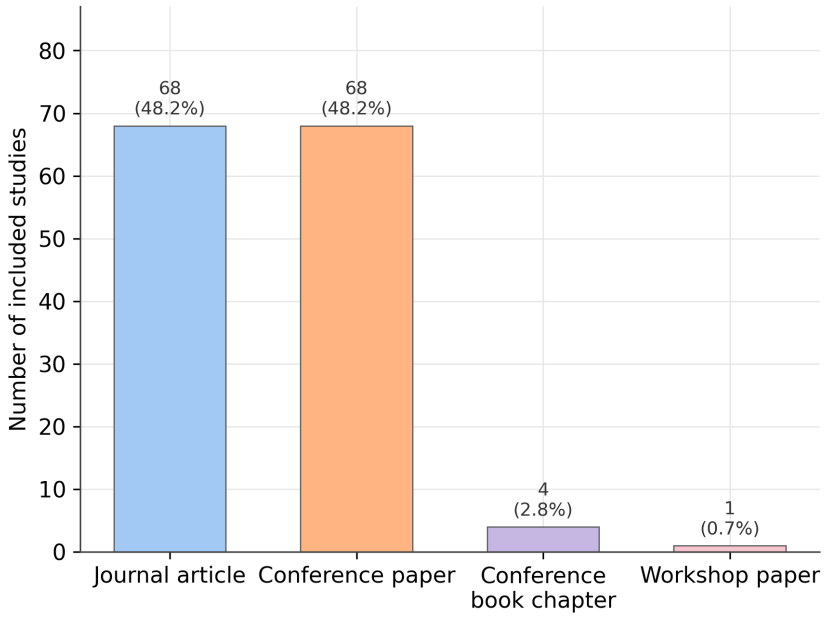


Figure 6. Publication-venue composition of the 141 studies included in the final synthesis corpus.

Taken together, these results indicate that publication venue is not a reliable proxy for methodological quality in this body of literature, and that the pre-specified $\geq 3/6$ quality threshold isolates a natural, defensible break in the score distribution rather than an arbitrary cut-off. Accordingly, inclusion decisions were based on the direct quality score rather than on venue; publication venue was retained only as a descriptive stratification variable during synthesis, and all quantitative findings reported in Sections 6–10 are grounded in the resulting 141-study corpus.

4.5. Data Extraction

A structured data-extraction form captured the following fields for each included study: reference, year, venue, study type (theoretical/simulation/emulation/real-network), PQC algorithm(s) evaluated, communication protocol(s) addressed, network scenario, performance metrics reported, and key findings. The extraction template is provided in the Supplementary Material.

Data extraction was performed independently by the two reviewers for each included study; extracted fields were subsequently cross-checked, and any discrepancies were resolved through discussion with reference to the original source text.

4.6. Synthesis Approach

Given the anticipated heterogeneity in measurement environments and reported metrics, a narrative synthesis augmented with structured tables and evidence maps was employed, following Popay et al. [28]. Where ≥ 3 studies reported the same metric under comparable conditions, a descriptive statistical summary (median, range, inter-quartile range) was computed. Formal meta-analysis was not deemed feasible given methodological heterogeneity. Consequently, pooled effect measures (e.g., risk ratios, standardised mean differences) were not applicable to this review. Correspondingly, a formal certainty-of-evidence assessment (e.g., using GRADE) was not conducted, as such frameworks are designed for effect estimates derived from comparative meta-analysis rather than for the heterogeneous, largely non-comparative performance metrics synthesised narratively here. Risk of bias arising from missing or selectively reported results (reporting bias) was not formally assessed using a structured tool, since no meta-analysis was performed and the

scope and type of outcome reporting varied substantially across the included studies; this is acknowledged as a limitation of the review process in Section 12.

5. Background

Table 4 summarises the hard mathematical problem, representative schemes, parameter sizes, and speed/quantum-resistance profile of the four PQC algorithm families discussed in this section, and Table 5 maps each family onto the network use cases surveyed throughout this review.

Table 4. Comparative analysis of post-quantum cryptography algorithm families. Key sizes reflect NIST security level 1 (128-bit quantum security). ✓ Favourable, ∼ Moderate, × Unfavourable relative to practical deployment. † Rainbow broken in 2022; listed for reference only.

Family	Hard Problem	Representatives	Parameter Sizes			Speed		Quantum Resist.
			Pub. Key	Sec. Key	Sig./CT	KeyGen	Enc./Sign	
Lattice-based	SVP, LWE (Learning with Errors)	ML-KEM (Kyber) ML-DSA (Dilithium) Falcon, NTRU	800 B (Kyber-512) 1312 B (Dil.-2) 897 B (Falcon-512)	1632 B (Kyber) 2528 B (Dil.-2) 1281 B (Falcon)	768 B CT (Kyber) 2420 B (Dil.-2) 666 B (Falcon)	✓ Fast	✓ Fast	Shor: ✓ Grover: ∼
Code-based	Decoding random linear codes (NP-hard)	Classic McEliece BIKE, HQC	261 KB (McEliece) 3138 B (BIKE-L1) 2249 B (HQC-128)	6452 B (McEliece) 3138 B (BIKE-L1) 2289 B (HQC-128)	128 B CT (McEliece) 4214 B (BIKE-L1) 4522 B (HQC-128)	✓ Fast	✓ Fast	Shor: ✓ Grover: ∼
Hash-based	One-way hash security (collision + preimage)	SLH-DSA (SPHINCS+) XMSS, LMS	32 B (SPHINCS + −128 s) 64 B (−256 s)	64 B (SPHINCS + −128 s) 128 B (−256 s)	7856 B Sig. (SPHINCS+−128 s) 29,792 B Sig. (SPHINCS+−256 f)	✓ Fast	× Slow	Shor: ✓ Grover: ∼ (highest assurance)
Multivariate (MQ-based)	Solving multivariate polynomial systems (MQ)	UOV, MAYO GeMSS Rainbow † (broken 2022)	∼150 KB (Rainbow-Ia) ∼1168 B (UOV)	∼100 KB (Rainbow-Ia) ∼24 B (UOV)	∼164 B Sig. (Rainbow-Ia) ∼128 B Sig. (MAYO)	∼ Mod.	✓ Fast	Shor: ✓ Grover: ∼ (structural weaknesses)

Abbreviations: SVP = Shortest Vector Problem; LWE = Learning With Errors; KEM = Key Encapsulation Mechanism; CT = Ciphertext; Sig. = Signature; B = Bytes; KB = Kilobytes; Dil. = Dilithium; AKA = Authentication and Key Agreement; Mod. = Moderate. Security note: All schemes (except Rainbow †) retain security against Grover's algorithm with appropriately sized parameters. Hash-based security reduces to the quantum security of the underlying hash function, providing the highest confidence level. Lattice-based schemes are the only family simultaneously meeting NIST standardisation, sub-MTU parameters, and fast keygen/enc. requirements. Deployment note: Packet fragmentation occurs when PQC parameters exceed the Ethernet MTU (1500 B). Kyber-512 CT (768 B) and Falcon-512 signatures (666 B) remain below this threshold; Classic McEliece public keys (261 KB) require dedicated offloading and are impractical for TLS or IoT handshakes [8].

Table 5. Deployment suitability of PQC algorithm families across network contexts. ✓ Suitable, ∼ Conditional, × Unsuitable.

Use Case	Lattice	Code	Hash	Multivar.
IoT/constrained devices	✓	×	∼	∼
TLS 1.3/DTLS handshake	✓	∼	×	∼
5G/6G AKA protocols	✓	∼	×	×
IPsec/VPN tunnels	✓	∼	×	∼
MACsec (data link layer)	✓	×	×	∼
MQTT/CoAP (lightweight IoT)	✓	×	×	×
Satellite/low-bandwidth links	✓	×	∼	∼
PKI/Certificate Authorities	∼	∼	✓	∼
Firmware signing (offline)	∼	∼	✓	∼
Blockchain/transaction signing	✓	×	∼	∼
Smart grid authentication	✓	∼	∼	×
High-security offline KEM	✓	✓	—	—
NIST standardised?	✓	∼	✓	× †
Hybrid-mode overhead ‡	Low	High	Med.	Med.

† Rainbow broken (2022); MAYO and UOV under NIST evaluation. ‡ Relative to classical baseline in a TLS 1.3 handshake.

5.1. Quantum Threat to Communication Cryptography

Shor's algorithm [1] breaks the integer-factorisation and discrete-logarithm problems underlying RSA, Diffie–Hellman, and ECC/ECDSA in polynomial time on a sufficiently large quantum computer, while Grover's algorithm [2] provides a quadratic speed-up against symmetric primitives, motivating a doubling of key lengths (e.g., AES-256 in place of AES-128). Because a CRQC is expected within the next one to two decades, communication systems that must protect long-lived secrets, authentication credentials, session keys, and firmware signatures are exposed to the HNDL threat model described in Section 1 [4,5].

5.1.1. ML-KEM (FIPS 203)

ML-KEM is NIST's standardised lattice-based KEM, derived from CRYSTALS-Kyber and based on the hardness of the Module Learning-With-Errors (Module-LWE) problem [29,30]. It is defined at three parameter sets (ML-KEM-512, -768, -1024) corresponding to roughly AES-128, AES-192, and AES-256 equivalent security, and its arithmetic is efficiently implementable via the NTT, which underlies the favourable computational-cost profile reported throughout Section 7.

5.1.2. ML-DSA (FIPS 204)

ML-DSA is NIST's standardised lattice-based digital-signature algorithm, derived from CRYSTALS-Dilithium and based on Module-LWE/Module-SIS hardness, using a Fiat–Shamir-with-aborts construction [31]. Compared with ECDSA, ML-DSA produces substantially larger public keys and signatures (cf., Section 7), which drives much of the certificate- and handshake-size growth discussed in Sections 7–9.

5.1.3. SLH-DSA (FIPS 205)

SLH-DSA is a stateless hash-based signature scheme derived from SPHINCS+ [32]. Its security relies solely on the collision resistance of an underlying hash function, giving it a conservative and well-understood security foundation, but at the cost of comparatively large signatures and higher signing latency, which Section 7 shows can dominate time-to-first-byte in real-time communication settings.

5.2. Communication Protocol Security Overview

5.2.1. Transport Layer Security (TLS 1.3)

TLS 1.3 [33] performs an ephemeral Diffie–Hellman-style key exchange in a single round trip and authenticates the handshake with a digital signature. PQC integration replaces (or hybridises) the classical key-exchange group with an ML-KEM encapsulation and the certificate signature scheme with ML-DSA or a composite classical/PQC signature, as detailed in Sections 6 and 8.

5.2.2. IPsec/IKEv2

IKEv2 [34] negotiates IPsec security associations through a Diffie–Hellman key exchange; PQC transition proposals introduce additional key-exchange payloads carrying ML-KEM ciphertexts alongside the classical exchange, enabling hybrid VPN and core-network tunnelling as surveyed in Sections 6 and 8 [35–37].

5.2.3. 5G Security Architecture

The 3GPP 5G security architecture [38] relies on the 5G-AKA/EAP-AKA' protocols for subscriber authentication and on TLS-protected HTTP/2 for inter-network-function communication within the SBA. PQC integration targets both the SUCI/AKA authentication vectors and the inter-VNF TLS layer, as discussed in Section 6 [39–41].

5.2.4. Lightweight IoT Protocols

Constrained IoT devices [42] typically communicate over MQTT, CoAP, or DTLS 1.3 with tight RAM, flash, and energy budgets. PQC adaptation for these protocols must reconcile ML-KEM/ML-DSA (or, where signature size is prohibitive, SLH-DSA) with kilobyte-scale memory ceilings, as quantified in Sections 7 and 9 [43–45].

5.3. Crypto-Agility

Crypto-agility denotes a system's ability to swap cryptographic primitives without redesigning the surrounding protocol or application, and is identified by NIST as a prerequisite for an orderly PQC transition [46]. In communication networks, this translates into negotiable algorithm identifiers, composite/hybrid certificate formats, and runtime-adaptive security policies, all of which recur as barriers and future-work priorities in Sections 9 and 10.

6. RQ1: Protocol and Scenario Coverage

RQ1: Which communication protocol layers, network deployment scenarios, and PQC algorithm families have been studied in the existing literature?

PQC migration research concentrates on critical protocols across the different layers of the OSI/TCP-IP stack.

- Transport layer: This is the most intensively studied area, with particular emphasis on TLS 1.3 and QUIC [43,47–50]. Integration of Kyber (ML-KEM) key exchange and Dilithium (ML-DSA) signatures into the TLS 1.3 handshake has been tested with both pure-PQC and hybrid (classical + PQC) configurations [9,50,51]. Beyond hybrid classical-PQC schemes, the addition of external Pre-Shared Keys (PSK) and QKD mechanisms to the TLS 1.3 handshake has also been examined as a supplementary safeguard against potential algorithmic weaknesses [52]. QUIC, owing to its UDP-based design and rapid connection establishment, has been examined for its ability to tolerate the larger packet sizes (fragmentation) introduced by PQC [47,49,51,53,54]. DTLS 1.3 for IoT devices has likewise served as a baseline for performance analysis under resource constraints [43–45,55], with DTLS also identified as a foundational building block for PQC key-exchange (KEM) and signature (DS) integration [52,56].
- Network layer: Recent studies focus on secure tunnelling scenarios via IPsec and IKEv2 [35,36,57,58]. The addition of PQC KEMs to the IKEv2 handshake has been analysed for enterprise VPN and data-centre interconnection [35,36]. Integration of PQC into modern VPN protocols such as WireGuard (e.g., qTrustNetVPN) has also appeared in the literature [59,60]. Cellular network authentication has also received substantial attention: the 5G-AKA mechanism has been reinforced with quantum-resistant KEMs (Kyber) and lightweight algorithms (ASCON), yielding proposals such as PQAKA and KyberPQ-AKA, whose compliance with standard 3GPP signalling flows has been tested [61,62]. RLWE-based key-exchange protocols have similarly been proposed for unmanned aerial vehicle (UAV) communications at this layer [63].
- Application layer: At this level, securing the IoT-prevalent MQTT and CoAP protocols with PQC has been investigated [45,64], including MQTT deployments in IIoT settings protected through hybrid TLS configurations [65,66]. PQC adaptation of DNSSEC (for DNS security) and SSH (for secure remote access) has also been studied [45,67,68]. Domain-specific application protocols have also been addressed: "Post-SECS/GEM" solutions have been developed for the SECS/GEM protocol used in semiconductor manufacturing, improving message integrity and authentication latency [69], while integration of ML-KEM-512 with AES-256 has been proposed for the ZigBee protocol used in smart-home systems [70].

- Data-link and physical layers: The CAN bus protocol used in automotive networks is a distinctive research area owing to the requirement to fragment PQC keys and signatures into 8-byte packets [71,72]. In the context of the 6G vision, research also addresses PLS and PQC-based authentication of QKD channels [73,74]. At this level, lattice-based protocols built on the Bi-ISIS problem have been investigated for resource-constrained RFID tags [75], and Kyber-based secure session-key establishment over LiFi (visible light communication) channels has been proposed for indoor IoT nodes [76]. Mathematical models have further shown that lattice- and code-based mechanisms at the physical layer (PHY) can meet the URLLC requirements envisioned for 6G [77].

Table 6 summarises which protocol layer, network scenario, and algorithm family each set of reviewed studies concentrates on.

Table 6. Summary of post-quantum cryptography studies across communication protocol layers.

Protocol Layer	Representative References	Network Scenario	Algorithm Family
Application Layer	[39,45,64,78–82]	IoT (MQTT, CoAP), smart cities, high-performance computing (SSH, RDP, DNSSEC), industrial systems (Modbus), cloud and embedded systems	Lattice-based (Kyber, Dilithium, NTRU), hash-based (SPHINCS+)
Transport Layer	[9,15,39,49,51,55,79,80]	TLS, QUIC, UE-to-UE communication, consumer IoT (BLE/Wi-Fi), cloud services	Lattice-based (Kyber, Dilithium, Falcon, Frodo), code-based (HQC, BIKE), hash-based (SPHINCS+)
Network Layer	[35,36,40,58,59,71,73,80,83–85]	5G core (VNF), IPsec/IKEv2, secure VPN (WireGuard/qTrustNet), cloud–edge continuum, SUCI/AKA, smart grids, Internet of Vehicles (IoV)	Lattice-based (Kyber, Dilithium, Falcon), code-based (Classic McEliece, HQC, BIKE), isogeny-based (CSIDH/SIKE), QRNG-assisted PQC
Data Link/ Physical Layer	[64,73,86–88]	CAN bus, in-vehicle networks, LDACS, 5G/6G QKD integration, physical-layer security (PLS)	Lattice-based (Kyber, Dilithium, Falcon, NTRU+), code-based (Classic McEliece), isogeny-based (SQISign)
Cross-Layer/ Full Stack	[59,68,74,81,89–92]	6G layered architecture, SDN-based quantum-resistant stack (QRC-Stack), military/tactical networks, smart hospitals, national HPC testbeds (FABRIC)	Hybrid PQC schemes, NIST standardised algorithms and Round-4 candidates (lattice, code, hash, multivariate)

Network deployment scenarios for PQC integration are shaped by the distinct requirements of modern network architectures:

- 5G/6G core and access networks: Securing HTTP/TLS traffic between virtualised network functions (VNFs) within the SBA is a primary focus [40,79]. Protecting SUCI (Subscription Concealed Identifier) and AKA (Authentication and Key Agreement) with Kyber has been tested under the latency sensitivity and high subscriber density of the 5G core [39,79,80,93], while 6G scenarios face ultra-low-latency (URLLC) as their principal challenge [74].
- IoT and IIoT: Limited memory (RAM/flash), low CPU power, and tight energy budgets are the central challenges [94–97]. Kyber and SPHINCS+ performance has been measured across a wide hardware range, from ARM Cortex-M4 systems down to more constrained 8-bit AVR microcontrollers [43,64,98]. Additional deployment studies include three-tier server-gateway-device architectures for smart-agriculture scenarios [99], smart-home control systems [100], and mobile IIoT truck (MMT) fleets [65].
- UAV and drone networks: Real-world UAV testbeds, including Raspberry-Pi-integrated hexacopters, have been used to analyse the power consumption and latency overhead of PQC algorithms in flight [101,102].
- Data centres and cloud environments: IPsec tunnel resilience and DoS resistance at high-speed (100 Gbit/s and above) links have been studied [36], where the key challenge is achieving line-rate PQC encryption [36].

- Connected and autonomous vehicles (IoV/V2X): The low bandwidth of CAN networks and V2V real-time constraints pose serious obstacles for PQC [59,87,103–105]. In 5G-based V2X communication, secure authentication protocols such as PQAKA have been developed and formally verified using ProVerif [61,63].
- Edge, fog, and dew computing: Offloading PQC computations to edge servers or fog nodes is a common strategy for reducing the processing burden of PQC operations [56,106,107], and Kubernetes-native frameworks such as Thoth have been proposed to orchestrate PQC workloads across heterogeneous edge clusters [66].
- Consumer electronics and eSIM: Integration of Kyber and Dilithium with blockchain-based verification has been tested for eSIM provisioning in smart-home hubs and wearable devices [108].
- Smart grids: Distributed-energy-resource (DER) networks and smart-metering systems (e.g., IEEE 2030.5) have been tested with PQC [79,85,109].
- Military and critical infrastructure: Dynamic algorithm switching and hybrid QKD/PQC models are studied across strategic, operational, and tactical network tiers [74,78,90].
- Other scenarios: Cloud computing/data centres [36,81,87,110,111], satellite communication [55,112–114], and smart-hospital/e-health systems [55,89,115,116] are other important application domains covered in the literature. At the physical layer of low-altitude wireless networks (LAWN), a "Quantum Skyshield" architecture combining BB84 QKD with Lamport OTS has been proposed to protect free-space optical (FSO) links against atmospheric turbulence [117].

Regarding PQC algorithm families, lattice-based schemes (Kyber/ML-KEM, Dilithium/ML-DSA, Falcon, SABER, NTRU, and NTRU Prime) remain the most extensively analysed family in terms of latency, memory footprint, and energy efficiency [76,101,118], while hash-based schemes such as SPHINCS+ (SLH-DSA) and Lamport one-time signatures are favoured in particularly low-power scenarios [117,118]. Unsupervised clustering (DBSCAN) has further been used to classify algorithm suitability by deployment context, identifying SLH-DSA-fast as best suited to mobile devices, SLH-DSA-small to IoT devices, and ML-DSA/Falcon to server environments [118]. Beyond the algorithmic layer, operational-assurance frameworks such as PQC-OAV have been proposed to passively monitor network traffic and detect implementation flaws in PQC deployments, such as low-entropy random-number generation, via an auditable evidence ledger [119], and PKI/PQC-based EAP-TLS models have been proposed to remove SIM-card dependency and reduce device-management overhead in next-generation IoT networks with billions of connected devices [56].

7. RQ2: Performance Analysis

RQ2: What is the quantitative performance impact (latency, bandwidth overhead, computational cost, energy) of PQC algorithms across communication environments?

Integrating PQC algorithms into communication protocols has consequences that extend well beyond security, directly affecting latency, bandwidth, computational cost, and energy consumption.

Latency impact. The latency impact of PQC is most visible in key exchange, digital signing, and secure session establishment (handshake). Experimental studies on modern protocols such as TLS 1.3 and QUIC show that lattice-based algorithms can compete with, or outperform, classical methods [49,54,120]. For example, a TLS handshake using the Kyber-1024/Falcon-1024 combination takes approximately 2.78 ms, whereas a comparable classical RSA-2048-based handshake reaches up to 3.57 ms in some scenarios [47]. By contrast, the hash-based signature scheme SPHINCS+, owing to its very large signature size,

raises time-to-first-byte (TTFB) to between 198.46 ms and 385.60 ms, causing significant performance penalties for real-time applications [47,120].

A similar pattern is seen in key encapsulation and decapsulation. On an ARM Cortex-M4 platform, Kyber-512 encapsulation takes approximately 5.4 ms, versus 21.3 ms for classical ECDH x25519 [121]. Conversely, the code-based BIKE-L1 incurs substantially higher latency, with operation times ranging from 219.6 ms to 435.8 ms [121]. In evaluations of the 5G Authentication and Key Agreement (5G-AKA) protocol, Kyber-512 integration increased total latency by approximately 7.94% relative to a classical RSA-based TLS solution, although user-equipment connection-establishment times were shorter for some Kyber variants than for RSA-ECDHE-based solutions [39,122]. In a separate 5G-AKA implementation, Kyber-512 key generation, encapsulation, and decapsulation were reported to complete in approximately 0.006 ms, 0.010 ms, and 0.015 ms, respectively, allowing the PQC-enhanced protocol to outperform the conventional 5G-AKA baseline on these sub-operations [62]. However, on resource-constrained IoT hardware such as the ESP32, the Kyber-512 handshake latency has been observed to reach up to 180 ms, roughly four times the 45 ms measured for classical ECDH on the same platform [76].

Handshake-level latency has also been examined under edge-assisted deployment models. On a constrained IoT device, a full PQC-based TLS handshake was measured at 3.48 s; offloading the computationally intensive operations to an edge server reduced this duration by approximately 96%, to 0.12 s [56]. In IIoT settings, a Kyber-768-secured hybrid TLS handshake introduced an approximately 13% latency increase relative to the classical baseline (from 95.6 ms to 108.8 ms), remaining within the sub-300 ms real-time requirement typical of such deployments [65]. In the context of 6G, hybrid PQC models have been reported to achieve an average handshake latency of 0.847 ms, representing a 44.4% improvement over classical RSA/ECC-based systems [77].

Algorithm-level comparisons further reveal that hardware and workload characteristics shape relative latency outcomes: on unmanned aerial vehicle (UAV) platforms, the SABER cypher has been shown to outperform other NIST finalists, including Kyber and NTRU, in terms of hardware/software efficiency, CPU-cycle count, and timing [101]. On the signature side, Dilithium has been identified as the lowest-overhead option for computationally constrained IoT devices, whereas Falcon is preferred for more capable gateway and server units owing to its smaller component sizes [99].

Bandwidth and communication overhead. A key disadvantage of PQC algorithms is their substantially larger key and signature sizes relative to classical methods [58]. In general, PQC algorithms can generate 10 to 100 times more transmission overhead than classical schemes [36,54,58,96,103]. For instance, whereas a classical ECDSA P-256 public key is only 33 bytes, the corresponding figure is 800 bytes for Kyber-512 and 1312 bytes for Dilithium-2 [53,55,103]. The gap is even larger for digital signatures: ECDSA produces 64-byte signatures, versus approximately 2420 bytes for Dilithium-2 and 17,088 bytes for SPHINCS+ (Level 1) [53,96,103]. Consistent with this pattern, SPHINCS+ has been identified as carrying the largest signature footprint among evaluated schemes, whereas Falcon offers the smallest component sizes and thus minimises communication overhead [99].

The growth in key and signature sizes also substantially inflates certificate structures: PQC-based X.509 certificates have been reported to be 4.6 to 48.8 times larger than classical ECC-based certificates [123,124]. Comparable figures have been reported at the leaf-certificate level, where classical certificates of 1–2 KB grow to 8–20 KB under Kyber/Dilithium, with a complete TLS handshake payload correspondingly rising from 5 to 10 KB to 25–70 KB [56]. This is especially problematic for low-bandwidth systems such as NB-IoT, where a single TLS handshake can reach 34 KB of transmitted data, introducing packet-fragmentation problems [96,125]. Similarly, comparing the transmission overhead of

different KEMs, Kyber-512 requires approximately 768 bytes, BIKE-L1 1573 bytes, and HQC-128 4497 bytes [121,125]. Protocol-specific overheads have also been documented: adopting ML-KEM-512 in ZigBee networks increases packet-transmission time by approximately 207% relative to the classical baseline (from 132 µs to 406 µs) [70].

Computational cost and resource usage. PQC computational performance varies with the underlying hardware architecture (x86, ARM, or RISC-V), but lattice-based algorithms in particular offer substantial computational-efficiency advantages. ML-KEM and ML-DSA achieve highly parallelisable operations via the NTT, with $O(n \log n)$ computational complexity, more efficient than the $O(n^2)$ complexity of many classical ECC operations [64,104,126]. Accordingly, using Kyber in 5G-AKA has been shown to reduce computational cost by approximately 13.3% relative to classical RSA-based solutions [87].

Despite this computational efficiency, PQC algorithms impose higher memory requirements. On an ESP32 platform, a classical cryptographic implementation uses approximately 22 KB of RAM, whereas a hybrid PQC framework requires approximately 41 KB [125]. Some lattice-based algorithms have even higher memory needs: NewHope, for example, can require up to 512 KB of RAM in certain implementations, limiting its feasibility on resource-constrained IoT devices [94]. Hardware acceleration, however, yields substantial gains: using FPGA-based solutions (Artix-7 and Kintex-7) and NVIDIA's cuPQC GPU-acceleration platform, Kyber has been reported to run approximately 46 to 54 times faster than software-only implementations [49,127]. Complementary results indicate that dedicated NTT cores and custom crypto-coprocessors can execute PQC operations approximately 60% faster and with approximately 65% lower energy consumption than software-only implementations [128].

Energy consumption. Energy consumption is a critical performance indicator, especially for battery-powered IoT devices, WSNs, and mobile terminals [96,121,129–132]. Per-operation energy measurements on a Raspberry Pi show Kyber-512 consuming approximately 0.299 mWh per operation, versus 1.25 mWh for classical secp256r1, i.e., approximately 76% lower energy per operation for Kyber-512 [93]. However, once the additional data transmitted is accounted for, total system energy consumption has been observed to increase by 30% to 60% owing to the larger PQC keys and signatures [43,45,87,94,121,125,133]. On constrained hardware such as the ESP32, a Kyber-512 handshake has been measured to consume approximately 38 mJ, compared with only 12 mJ for classical ECDH [76].

Adaptive PQC mechanisms aimed at improving energy efficiency have shown positive results, particularly in WSNs. Adaptive algorithms have been reported to extend network lifetime by 10–15% relative to static approaches, while adding only 5–7% overhead to daily energy consumption [133]. In handshake-specific comparisons, a Kyber-512-based connection consumes approximately 0.36 mJ, versus 25.2 mJ for RSA-2048 and 18.7 mJ for ECC-256, underscoring the per-operation energy advantage of lattice-based algorithms [134,135]. At the protocol level, quantum-resilient communication protocols (QRCP) combining optimised lattice-based key exchange with lightweight AES-GCM encryption have been reported to achieve approximately 40.2% energy savings relative to conventional ECC-based protocols [136], while also reducing packet loss by approximately 46.7% (from 6.0% to 3.2%) compared with ECC, indicating that PQC-based reliability gains are not limited to raw speed metrics [136]. Hybrid schemes combining PQC with symmetric cryptography have likewise been shown to reduce per-operation energy consumption from approximately 1.9 mJ for pure PQC implementations to approximately 1.1 mJ, a reduction of roughly 42% [128]. Notably, when QKD is layered onto the TLS handshake, the effective key rate drops to approximately 300 kbps and handshake duration rises to approximately 25 ms—roughly twice the 12 ms observed for a pure-PQC handshake—although this configuration provides information-theoretically unconditional security [137].

8. RQ3: Hybrid Cryptography Strategies

RQ3: How are classical–PQC hybrid cryptography strategies implemented in communication infrastructure, and what is their security and operational effectiveness?

Because PQC algorithms are relatively new and long-term security analysis is still ongoing, hybrid cryptography, rather than an outright switch from classical cryptography, has been widely adopted [74,138,139]. Hybrid strategies combine the proven, years-long track record of classical algorithms with the quantum-resistant structure of PQC algorithms, aiming to preserve both security and interoperability during the transition. Hybrid approaches have accordingly become an important area of research and deployment in communication infrastructure, spanning implementation methods, security gains, and operational impact.

Implementation methods. The central goal of hybrid cryptography is to combine the reliability of classical key-exchange mechanisms (e.g., ECDH or RSA) with the quantum-resistant mathematical structures of PQC algorithms such as Kyber and Dilithium [35,47,49]. The most widely used approach in the literature is the key-combiner (chaining) mechanism, in which the shared secret from a classical key-exchange protocol (e.g., X25519) is combined with the shared secret produced by a PQC-based KEM [47,50,140]. Combination is typically performed via an HKDF (HMAC-based Key Derivation Function) or XOR-based method, although structural key-derivation mechanisms that jointly guarantee the security of both components are preferred over simple secret concatenation [127,138–140]. This pattern, in which a classical exchange such as ECDHE is combined with a PQC component such as ML-KEM (Kyber) within the TLS 1.3 handshake, is commonly referred to in the literature as a "PQ/T" (Post-Quantum/Traditional) hybrid construction, and it preserves communication security even if one of the two constituent algorithms is subsequently broken [52,65]. An analogous construction has been applied at the cellular-authentication layer, where ML-KEM and lightweight algorithms such as ASCON have been integrated into the 5G-AKA protocol (PQAKA) while preserving compliance with 3GPP standards [61,62].

Another common approach is the dual-handshake mechanism. In secure communication protocols such as TLS 1.3 and SSH, classical and PQC-based key-exchange processes are executed in parallel or sequentially [140,141], allowing the system to fall back safely to classical mode when PQC support is absent on the client or server side, thereby preserving compatibility with existing infrastructure [140]. At the authentication layer, composite X.509 certificates are used, embedding both classical (e.g., ECDSA) and PQC (e.g., Dilithium or Falcon) digital signatures within the same structure, enabling interoperability between legacy and next-generation systems [55,123,142]. Mixed-certificate chains that combine classical (RSA/ECDSA) and PQC (Dilithium/Falcon) signatures within the same trust chain have similarly been proposed for authentication workflows, with the choice of signature type blended according to the processing capacity of the endpoint in order to optimise communication overhead [99].

In the most security-critical infrastructures, PQC is planned to be used alongside QKD [73,87,143,144]. In such hybrid architectures, QKD secures key generation with information-theoretic security at the physical layer, while PQC algorithms render authentication, key management, and higher-layer security mechanisms quantum-resistant, together providing integrated physical and cryptographic security [73,74,133,143,145]. In this combined model, QKD is responsible for unconditional security at the physical layer, while PQC enables the scalable and verifiable distribution of the resulting keys at higher protocol layers [117,137].

Orchestration and edge-offloading strategies have also emerged as an implementation dimension of hybrid deployment. Kubernetes-native frameworks such as Thoth distribute PQC workloads across heterogeneous edge clusters (e.g., ARM and RISC-V nodes), improving infrastructure flexibility [66], while computationally heavy PQC operations (such

as KEM decapsulation) on resource-constrained IoT devices are offloaded to trusted edge servers [56,128].

Security effectiveness. The core security rationale of hybrid strategies rests on a "best of both worlds" principle, with defence-in-depth as its primary benefit [35,50,127,138]: as long as at least one of the classical or PQC components remains secure, communication security is preserved. Consequently, should an as-yet-unknown vulnerability emerge in a PQC algorithm, classical cryptography continues to provide protection, while should classical algorithms be broken by sufficiently powerful quantum computers, the PQC component maintains communication security [50,127,139,140]. This defence-in-depth property is underpinned mathematically by the Module-Learning-with-Errors (MLWE) and Ring-Learning-with-Errors (RLWE) lattice problems, which remain resistant to both Shor's and Grover's quantum algorithms [102,106], in contrast to classical RSA/ECC schemes, which have been shown to be solvable by sufficiently capable quantum computers within seconds [101].

Hybrid key exchange also provides important protection against the HNDL attack model, preventing adversaries from recording encrypted traffic today for decryption by future quantum computers and thereby preserving forward secrecy [113,138–140,142]. Consistent with this, hybrid constructions generate ephemeral session keys via ML-KEM at every session [61], so that the compromise of a long-term key does not enable decryption of previously recorded communications [100]. Hybrid architectures additionally support backward compatibility during transition while guarding against downgrade attacks, since the system requires successful validation of both the classical and PQC components before a connection can be established, preventing an adversary from forcing the communication down to a weaker classical algorithm [81,83,87,127]. In quantitative terms, the security effectiveness of hybrid deployment has also been benchmarked in critical scenarios such as eSIM provisioning, where integration of Kyber and Dilithium was reported to achieve a 97.5% security-effectiveness score relative to classical-only approaches [108].

Operational effectiveness. Implementing hybrid cryptography strategies brings operational costs alongside their security benefits. Latency is foremost among these: hybrid handshakes typically incur 8% to 40% higher latency than classical methods [68,123,139]. Nonetheless, when high-performance lattice-based algorithms such as Kyber (ML-KEM) are used, the resulting increase in processing time remains within acceptable bounds for many communication scenarios, including 5G networks and cloud-computing infrastructure [47,50,54,74]. In some deployments, thanks to the high computational performance of PQC algorithms, the total latency of hybrid systems can even be lower than that of classical RSA-based systems [67,103,139]. In IIoT deployments specifically, a Kyber-768-based hybrid TLS handshake was found to introduce only an approximately 13% latency increase (108.8 ms) relative to classical methods, remaining within the sub-300 ms real-time requirement typical of industrial settings [65], and edge-server assistance has been shown to reduce such latencies by up to 96% [56]. In high-throughput 6G-oriented infrastructures, hybrid PQC models have similarly been reported to outperform classical systems, achieving an average latency approximately 44.4% lower [77].

The largest operational burden arises in bandwidth requirements [47,103,127,146]. Owing to the large key and signature sizes of PQC algorithms, hybrid certificates and key-exchange messages can generate 10 to 48 times more transmission overhead than classical ECC-based systems [123,127]. This is particularly problematic in low-bandwidth environments such as CAN bus and NB-IoT, causing packet fragmentation, increased communication load, and consequently higher energy consumption [71,72,125,140]. Similarly, in low-data-rate networks such as ZigBee, the large key and signature sizes characteristic

of PQC components have been shown to increase packet-transmission time by more than 200% [70].

Hybrid strategies also place heavier demands on processor and memory resources; as noted in the memory-overhead analysis of Section 7, a hybrid classical–PQC framework on an ESP32 platform requires roughly twice the RAM of a classical-only implementation (∼41 KB vs. ∼22 KB) [125]. FPGA- and ASIC-based hardware accelerators can speed up hybrid cryptographic operations by up to 145 times, substantially reducing processor load [127]. In terms of energy consumption, hybrid strategies can add approximately 28 mJ of additional energy overhead per operation, particularly on battery-powered IoT devices [127]; adaptive re-keying and intelligent session-management strategies can, as noted in Section 7, keep the resulting reduction in network lifetime to around 10–15% [133]. Optimised hybrid protocols such as quantum-resilient communication protocols (QRCP), which combine intelligent key exchange with lightweight AES-GCM encryption, have been reported to yield energy savings of approximately 40.2% relative to classical ECC-based systems [136], and the use of hardware accelerators such as dedicated NTT cores has been shown to improve energy efficiency by up to 65% [128]. A related lightweight variant, combining a simplified 3×3-matrix formulation of AES with QKD for simulation on constrained IoT devices, has been reported to reduce processing time by approximately 17% while preserving security [147].

Beyond raw performance metrics, operational assurance has also been addressed directly: auditable evidence-ledger frameworks such as PQC-OAV have been proposed to passively monitor network traffic during PQC migration and detect implementation flaws, such as low-entropy key generation [119]. Unsupervised-learning approaches (e.g., DBSCAN-based clustering) have additionally been used to automatically classify algorithm suitability by device type, identifying SLH-DSA-fast as most efficient for mobile devices and SLH-DSA-small for IoT devices [118]. At the physical layer, a "Quantum SkyShield" architecture combining BB84 QKD with Lamport OTS has been proposed for low-altitude UAV networks (LAWN), providing reliable authentication even over free-space-optical (FSO) links subject to atmospheric turbulence [117].

Taken together, the reviewed studies indicate that classical–PQC hybrid strategies represent the strongest available approach for securing communication infrastructure during the transition to the quantum era, providing both security assurance and infrastructure compatibility [50,54,140,148]. The additional latency, bandwidth, memory, and energy overheads introduced by hybrid systems can be reduced to manageable levels through high-efficiency lattice-based algorithms such as Kyber (ML-KEM) and Dilithium (ML-DSA), combined with FPGA- and ASIC-based hardware acceleration [111,127,149]. Hybrid cryptography thus preserves backward compatibility with existing communication infrastructure while securing long-term data confidentiality and improving system resilience against future cryptanalytic advances [74].

9. RQ4: Transition Barriers and Readiness

RQ4: What technical, standardisation, and operational barriers impede PQC transition in telecommunication and communication infrastructure?

Because PQC algorithms have computational and storage requirements that differ from classical cryptographic methods, they pose significant technical barriers, particularly on resource-constrained communication devices. IoT devices, unmanned aerial vehicles (UAVs), WSNs, and microcontroller-based embedded systems struggle to run PQC algorithms efficiently owing to limited RAM, flash memory, processing capacity, and energy budgets [43,64,94,98,110,121]. Typical low-power IoT sensor nodes operate within an extremely narrow hardware envelope, often limited to 8–24 MHz processor

clocks and 8–16 KB of RAM, which makes deploying PQC schemes with markedly higher computational, memory, and storage requirements than classical algorithms particularly difficult [99,108]. Hash-based signature schemes such as SPHINCS+, in particular, can cause high memory consumption and RAM overflows on 8-bit microcontrollers, limiting their applicability on resource-constrained platforms [43,55].

A further technical challenge, already quantified in Section 7, is that PQC key and signature sizes are 10 to 100 times larger than their classical RSA/ECC counterparts [99]; lattice-based keys in particular can reach the kilobyte scale, posing a serious obstacle for low-memory IoT devices [128]. This growth substantially increases communication overhead and, particularly in low-bandwidth environments such as NB-IoT and CAN bus, leads to packet fragmentation, higher latency, and reduced network efficiency. The transmission of larger cryptographic payloads likewise increases energy consumption on battery-powered devices, with total transmission-related energy demand rising by 30–60% in the studies reviewed in Section 7. Timing constraints compound this problem in emerging use cases: URLLC scenarios envisioned within the 6G roadmap require latencies well under 1 ms, a window within which the complex mathematical operations underlying PQC algorithms are difficult to complete [77].

A further barrier to widespread PQC adoption is the limitation of existing hardware infrastructure. Current Hardware Security Modules (HSMs) and cryptographic accelerators are, in general, not designed to natively support lattice-based PQC algorithms [30,71,72]. Developing and commercially integrating PQC-compatible FPGAs, ASICs, and security processors therefore requires design and certification cycles spanning many years [36,71,72]. Dedicated hardware accelerators such as NTT cores can mitigate the computational burden of PQC operations, but the fact that a large share of currently deployed devices lack support for such specialised accelerators continues to slow the transition [76,128]. In addition, the resilience of new-generation PQC algorithms against side-channel attacks, timing analysis, power analysis, and electromagnetic leakage is not yet as mature as that of classical algorithms, posing a significant technical risk for secure hardware implementation [43,59,140,150].

Global deployability of PQC depends not only on algorithm development but also on the maturation of international standards. Although NIST has published core PQC standards such as ML-KEM and ML-DSA, standardisation of alternative algorithms (Round-4 candidates) and additional digital-signature schemes is still ongoing [40,67,146,151–154]. Confidence in the newly standardised algorithms has also not yet reached the level enjoyed by classical algorithms such as RSA and ECC, which have been tested over decades; this concern has been reinforced by the rapid cryptanalytic breaking of certain earlier candidate algorithms, such as Rainbow [52,77]. This creates uncertainty for technology vendors and service providers regarding which algorithms will prevail in the long term, delaying investment decisions [94]. Sector-specific standards gaps compound this uncertainty: automotive standards such as ISO 15118 and AUTOSAR have not yet fully defined PQC support, leaving a substantial research and standardisation gap for in-vehicle networks and V2X ecosystems [61]. A number of PQC-based AKE protocols proposed in the literature have likewise been noted as not yet fully satisfying core security properties such as anonymity, traceability, and formal verification [63,102].

Similarly, a significant portion of the IETF drafts defining PQC integration into widely used communication protocols such as TLS 1.3, IKEv2, and QUIC have not yet reached final status [48,58,74]. In particular, the lack of standardised application programming interfaces (APIs) for hybrid key exchange and PQC–QKD integration limits interoperability across vendors [74,140]. In addition, the absence of standardised measurement methods for evaluating the quantum-attack security levels provided by PQC algorithms complicates

the choice of the most appropriate algorithm for a given use case [45]. International standardisation is further complicated by countries developing their own national PQC standards [74,123], for example, South Korea's KpqC initiative alongside NIST's standards, making global harmonisation and certification more complex [123].

Technical feasibility does not by itself guarantee smooth deployment across large-scale communication infrastructure. Because legacy and PQC-enabled systems will need to co-exist for an extended period, hybrid cryptography becomes mandatory during the transition, increasing system-architecture complexity and complicating key management, certificate management, and security-policy administration [39,68,150]. Existing PKI architectures are similarly not designed to efficiently manage the much larger PQC certificates, CRLs, and OCSP responses [55,122,148], so re-issuing millions of digital certificates in PQC-compatible form constitutes a substantial operational and logistical burden [148]. Determining which devices across an organisation's existing infrastructure use which algorithms, and maintaining an accurate cryptographic inventory, has itself been identified as a considerable operational burden in preparing for migration [119]. HNDL threat model further heightens the urgency of PQC transition, yet the inability of existing infrastructure to keep pace with this urgency constitutes an operational risk in its own right [69,119]. Hardware accessibility and cost also remain limiting factors, particularly for QKD-based solutions, where detectors and synchronisation modules remain expensive and constrain large-scale accessibility [117]. Lifecycle management poses an additional challenge: managing billions of IoT devices through SIM-based AKA mechanisms raises scalability and key-revocation concerns, given that such devices are typically long-lived and often operate without human intervention [56].

A further factor slowing PQC adoption is the low uptake rate within the current internet ecosystem. Although PQC support has begun to appear in some platforms, such as OpenSSH and Chrome, overall PQC usage in general internet traffic is still reported at approximately 0.03% [81]. The historically slow, multi-year global adoption of protocols such as TLS 1.3 suggests that PQC migration will likewise proceed gradually [40,81]. PQC deployment further entails high costs from software and hardware upgrades, new security-infrastructure rollout, and specialised human-resource requirements [87,94,150], complicating transition planning particularly for large telecom operators and critical infrastructure. Finally, many devices with 10–20-year service lifetimes, smart grids, industrial control systems, and telecommunications equipment lack OTA update support or the hardware capacity to run PQC algorithms, leaving them vulnerable to future quantum-based attacks [125,142,155].

A notable and underappreciated barrier concerns visibility into PQC traffic itself: existing Network Security Monitoring (NSM) solutions are frequently unable to interpret the new IANA code points introduced by PQC key exchange, causing PQC sessions to appear as opaque data and preventing the detection of configuration errors such as low-entropy key generation [119]. Attested edge offloading, in which computationally heavy operations are delegated from constrained IoT devices to trusted edge servers, has nonetheless been shown to reduce PQC handshake latency on such devices by approximately 96% (from 3.48 s to 0.12 s), bringing it down to operationally acceptable levels [56]. In some deployment contexts, the barriers to PQC adoption are not purely cryptographic: in systems such as low-altitude wireless networks (LAWNs), integrating PQC and QKD requires contending not only with algorithmic constraints but also with physical-layer obstacles such as atmospheric turbulence and weather conditions [117]. Against this backdrop, the use of hybrid models combining both classical and PQC algorithms until full transition is achieved is presented in the literature as the only realistic path for preserving operational continuity and backward compatibility during the interim period [52,65].

The findings across this literature indicate that PQC transition in telecommunication and communication networks is not limited to replacing cryptographic algorithms; it requires reconfiguring the entire ecosystem, from hardware infrastructure to standards, protocol design, certificate management, and operational processes. In this process, crypto-agility stands out as the core design principle enabling systems to be updated quickly and securely as new standards, algorithms, and threat models emerge. Overcoming these technical, standardisation, and operational barriers therefore depends not only on further algorithm development but also on building flexible, interoperable, and sustainable security architectures [58,83,142,156].

10. RQ5: Research Gaps and Future Directions

RQ5: Which communication scenarios and technical problems are under-researched, and what are the priority directions for future work?

Examination of the PQC literature reveals substantial research gaps concerning real-world communication scenarios, large-scale networks, resource-constrained platforms, and complex security architectures. A significant share of existing studies has been conducted in controlled laboratory or simulation-based settings, leaving the behaviour of PQC algorithms under many real network conditions insufficiently examined [43]. In particular, studies of the scalability and long-term performance of PQC algorithms in large-scale WSNs comprising hundreds or thousands of nodes with continuously changing topology remain limited; memory constraints, dynamic node join/leave behaviour, and the additional processing overhead introduced by side-channel protection mechanisms in such environments remain important, largely unanalysed research topics [43].

Similarly, studies on the performance of PQC algorithms under realistic radio-channel conditions in direct User-Equipment-to-User-Equipment (UE-to-UE) communication and in mutual authentication among microservices within the SBA of 5G/6G systems remain quite limited [15,40]. In addition, developing PQC mechanisms suited to multicast security and swarm communication in UAV swarms and Unmanned Traffic Management (UTM) systems remains an important open topic [121,157]. A related and largely unexplored gap concerns multi-party group key establishment: the overwhelming majority of existing work addresses two-party key exchange, whereas PQC-based Group Authenticated Key Exchange (PQC-GAKE) constructions for dynamic groups and n-participant cooperative networks remain poorly understood and potentially vulnerable to implementation-focused attacks [158]. Likewise, although performance data exist for PQC in static laboratory settings, empirical studies of hybrid TLS deployment in dynamic, real-time Mobile IIoT networks, such as mobile manufacturing trucks (MMT), remain scarce [65]. Integration of PQC into Light Fidelity (LiFi) sensor nodes and indoor IoT deployments is likewise a nascent area, and end-to-end secure architectures that jointly exploit the physical-isolation properties of LiFi and the cryptographic resistance of PQC have not yet matured [76]. SIM-less authentication is another emerging research direction: PKI-based, PQC-enabled authentication models delivered over EAP-TLS, aimed at removing dependence on traditional SIM cards across billions of devices in FutureG networks, have only recently been identified as a distinct research path [56].

STINs, where satellite and terrestrial networks operate jointly, are another insufficiently studied application domain. More comprehensive research is needed on the effects of channel characteristics such as long propagation delay, high packet loss, and limited bandwidth on PQC algorithms with large key and certificate sizes, and on managing the resulting packet fragmentation [113,159]. In V2X and autonomous-driving applications, digital-signature verification delays under high vehicle density, the scalability of key

management, and secure message-verification processes likewise remain insufficiently researched [58,87,160].

10.1. Unresolved Technical Problems and Research Gaps

Although significant progress has been made in PQC standardisation, several technical problems remain unresolved at the deployment layer. One is the performance of post-quantum digital signatures: while KEMs offer high processing efficiency, the large signature sizes and high computational cost of schemes such as SPHINCS+ create significant bottlenecks in TLS handshakes, and work on optimising these algorithms has not yet reached a sufficient level of maturity [9,48,135,161,162].

Another important research area is hardware implementation resilient to side-channel attacks. Implementing standardised algorithms such as Kyber and Dilithium in a manner resistant to timing, power-analysis, and electromagnetic-leakage attacks remains a significant technical challenge, particularly on resource-constrained embedded systems [54,81,146]. Resilience to side-channel and physical-capture attacks is a particularly acute gap for devices operating in open, physically exposed environments, such as UAVs, where the risk of device capture and subsequent timing- or power-analysis attacks is markedly higher than in controlled settings [66,102]. Relatedly, further work is needed on hardware-acceleration strategies (e.g., FPGA- or ASIC-based NTT cores) capable of overcoming the substantial handshake-latency penalties observed on constrained IoT devices, together with a clearer understanding of the cost and area efficiency of such accelerators [69,128]. Similarly, the use of hybrid digital-signature mechanisms within complex Web PKI hierarchies involving numerous certificate authorities, and the effect of validating long hybrid certificate chains (path validation) on network performance, have not yet been evaluated in detail [9,50].

Significant gaps also remain in the literature on energy consumption. Much of the existing work estimates the energy requirements of PQC algorithms through analytical models or simulations, with limited long-term, comprehensive experimental measurements on real hardware [48,121,163,164]. In addition, the formal verification of key-combination methods used in hybrid classical/post-quantum key-exchange mechanisms (KEM combiners) under a quantum adversary model, and their protocol-level security guarantees, remain insufficiently mature research areas [138,146,150]. Full formal security proofs for PQC-based AKE protocols under the Quantum Random Oracle Model (QROM) likewise remain an underdeveloped area of the literature [102]. At the network layer, most simulation studies fail to model real-world phenomena such as propagation delay, packet jitter, and congestion-induced loss, which prevents a full assessment of how the large packet sizes and consequent fragmentation introduced by PQC affect real network performance [61].

10.2. Priority Directions for Future Research

The literature highlights crypto-agility as a priority focus for future PQC research [78,87,165]: developing adaptive security architectures capable of switching cryptographic algorithms at runtime based on dynamic parameters such as network conditions, threat level, latency requirements, and device energy state is considered an important research priority [78,87,165].

Another priority area is hybrid security architectures combining PQC with QKD. Developing scalable architectures with standardised APIs that integrate PQC's computational security with QKD's information-theoretic security is of critical importance for future communication infrastructure [36,73,74]. In addition, developing dedicated FPGA-, GPU-, and ASIC-based PQC accelerators to support high connection density in data centres, cloud infrastructure, and 5G/6G core networks is another key research area [36,149,166].

Developing lightweight post-quantum digital-signature algorithms for resource-constrained devices is also expected to gain importance. In particular, research into low-size, low-energy PQC signature schemes supporting security mechanisms such as secure boot, remote attestation, and software-integrity verification should be expanded [59,74,83,167]. The integration of artificial intelligence and TinyML into cryptographic protocols is likewise emerging as a priority direction, both for the predictive offloading of PQC workloads to edge nodes and for embedding lightweight machine-learning models for anomaly detection directly within cryptographic protocols [66,128]. For 6G, mathematically optimised cross-layer PQC architectures capable of meeting ultra-low-latency (sub-1 ms) and ultra-high-reliability (99.999%) requirements represent an important design target [77]. Decentralised trust models are also gaining relevance: recording PQC certificates and key-exchange proofs on blockchain-based ledgers to provide transparent auditability is regarded as critical for industrial compliance [108,137]. For UAV/UGV networks specifically, developing autonomous cryptographic defence mechanisms triggered by on-device sensor data (e.g., LiDAR) together with dynamic re-keying policies is highlighted as an important future direction [66]. Finally, because much existing work remains simulation-based, large-scale, longitudinal field testing on real IoT platforms such as ARM Cortex-M and ESP32 is critical for evaluating PQC algorithm performance under genuine operating conditions [125,133,163].

Several further observations from the literature merit specific attention as priorities for future work. First, existing Network Security Monitoring (NSM) tools are frequently unable to recognise PQC-specific code points, meaning that configuration errors can go undetected even in sessions that otherwise appear secure; this "PQC blind spot" underscores the need for evidence-based assessment tools such as PQC-OAV [119]. Related testing has also identified a low-entropy anomaly in which short-lived, container-based OpenSSL instances generate poor-quality keys, a weakness that the use of PQC algorithms alone does not resolve [119]. A further counterintuitive finding is what might be termed a hybrid efficiency paradox: hybrid classical–PQC models have been shown to reduce per-operation energy consumption by approximately 42% relative to pure PQC implementations, an unexpected efficiency advantage that warrants further systematic study [128]. Finally, environmental sensitivity deserves greater attention in future architectures: in systems such as Quantum Skyshield, PQC/QKD security must be "weather-aware," accounting not only for cyber-attacks but also for the increase in Quantum Bit Error Rate (QBER) caused by atmospheric phenomena such as fog, rain, and snow [117].

11. Discussion

Synthesising RQ1–RQ5, three cross-cutting patterns emerge. First, the transport and network layers (TLS 1.3, QUIC, IKEv2) receive disproportionately more attention than the application and physical/data-link layers, leaving MQTT/CoAP-based application-layer deployments and CAN-bus/automotive scenarios comparatively under-evaluated relative to their real-world exposure (RQ1). Second, the quantitative evidence base is dominated by lattice-based ML-KEM/ML-DSA, for which latency and computational-cost figures are consistently favourable, whereas hash-based SLH-DSA/SPHINCS+ and several code-based candidates (BIKE, HQC) carry order-of-magnitude larger overheads that are reported far less consistently across studies, limiting cross-study comparability (RQ2). Third, hybridisation is treated in the literature less as an optional safeguard than as the only currently viable transition path, yet its long-term security guarantees (formal verification of KEM combiners) and its interaction with legacy PKI at scale remain open (RQ3–RQ5).

A Five-Level PQC Transition-Readiness Maturity Model

Building on the barriers identified in RQ4 and the gaps identified in RQ5, we propose the following maturity levels for assessing an organisation's or network's PQC transition readiness:

Level 0, Classical-only. No crypto-agility mechanism; algorithms are hard-coded; no PQC risk assessment has been performed.
Level 1, Awareness and inventory. Cryptographic assets and HNDL-exposed data flows have been inventoried; crypto-agility gaps have been identified, but no PQC code has been deployed.
Level 2, Hybrid pilot. Hybrid classical–PQC key exchange (e.g., X25519 + ML-KEM) has been piloted in non-production TLS/IKEv2/VPN environments, with latency and bandwidth impact quantified.
Level 3, Hybrid production rollout. Hybrid schemes are deployed in production across at least one major protocol (TLS, IPsec, or 5G-core signalling), supported by composite/hybrid PKI and hardware-accelerated PQC operations where needed.
Level 4, Full PQC/PQC–QKD integration. Legacy-classical fallback is retired where policy permits; crypto-agile algorithm negotiation is standard; PQC–QKD hybrid architectures are used in the highest-assurance segments.

This model is proposed as a synthesis of the barriers/readiness signals identified in this review rather than as an empirically validated instrument; its calibration against real deployment data is itself a direction for future work (cf., RQ5).

12. Conclusions

This systematic review synthesised the communication-network-specific post-quantum cryptography (PQC) migration literature through a PRISMA-2020-compliant process spanning 3229 identified records and culminating in a quality-appraised corpus of 141 studies (68 journal articles, 68 conference papers, 4 conference-derived book chapters, and 1 workshop paper), structured around five research questions. Five principal findings emerge from this synthesis.

First, protocol- and scenario-level coverage in the literature is markedly uneven: transport-layer protocols, particularly TLS 1.3, QUIC, and DTLS 1.3, dominate current research attention, whereas data-link-layer (e.g., MACsec, CAN bus) and cross-layer integration studies remain comparatively scarce despite their operational relevance to automotive, industrial, and 6G physical-layer scenarios (RQ1). Second, the quantitative evidence base is asymmetric across algorithm families: lattice-based ML-KEM and ML-DSA consistently offer the most favourable latency–bandwidth–energy trade-off among NIST-standardised families, owing largely to their $O(n \log n)$ Number-Theoretic-Transform arithmetic, whereas hash-based SLH-DSA and several code-based candidates (BIKE, HQC) trade this efficiency for more conservative security assumptions or cryptographic diversity, at the cost of order-of-magnitude larger signatures or ciphertexts (RQ2). Third, classical–PQC hybrid cryptography emerges not as an optional transitional safeguard but as the de facto migration strategy across essentially every communication scenario surveyed, from 5G/6G core signalling to automotive and IoT deployments, at a quantifiable and, for lattice-based configurations, generally manageable operational cost (8–40% handshake-latency overhead; 10–48$\times$ certificate and key-exchange bandwidth overhead) (RQ3). Fourth, transition is impeded less by a shortage of viable algorithms than by ecosystem-level friction: constrained-device resource ceilings, immature hardware acceleration for side-channel-resistant PQC implementations, incomplete IETF and 3GPP standardisation of hybrid key-exchange and certificate formats, and the operational burden of migrating public-key-infrastructure certificate chains at scale (RQ4). Fifth, large-scale field valida-

tion on real network infrastructure, standardised PQC–QKD integration architectures, and lightweight post-quantum signature schemes for resource-constrained endpoints remain the most consequential open research gaps, with the majority of existing performance evidence still derived from simulation or laboratory testbeds rather than production deployments (RQ5).

Building on the barriers and gaps identified under RQ4 and RQ5, the five-level PQC transition-readiness maturity model proposed in Section 11 offers telecommunications operators, network architects, and standards bodies a structured instrument for benchmarking organisational readiness, from classical-only baselines through hybrid piloting and production rollout to full PQC–QKD integration in the highest-assurance network segments. This framework is intended as a synthesis of the readiness signals surfaced by the reviewed literature rather than as an empirically validated maturity instrument; its calibration against longitudinal deployment data constitutes a natural extension of the priority directions identified under RQ5.

Several limitations of the present review should be acknowledged. The quality-appraisal process relied on a single quantitative threshold (a total score of $\geq 3/6$ across six criteria) rather than a categorical risk-of-bias judgement, a choice validated post hoc through threshold-sensitivity analysis (Section 4.4) but one that necessarily trades some interpretive nuance for reproducibility. Given the heterogeneity of measurement environments, hardware platforms, and reported metrics across the included studies, a narrative synthesis with structured evidence tables was adopted in place of formal meta-analysis; this preserves contextual fidelity but limits the precision of any pooled quantitative estimate. Finally, the review is necessarily time-bound to the state of PQC standardisation and communication-network deployment as of the search date (24 March 2026); given the pace of both NIST post-quantum standardisation activity and 3GPP/IETF protocol drafting in this domain, periodic updating of this evidence base is warranted.

Taken together, the findings indicate that the transition of communication networks to post-quantum security is technically tractable at the algorithmic level but remains an unresolved systems-engineering problem at the ecosystem level. Realising a secure, interoperable, and crypto-agile communication infrastructure in the post-quantum era will depend as much on coordinated advances in standardisation, hardware acceleration, and public-key-infrastructure tooling as on continued refinement of the underlying cryptographic primitives.

Supplementary Materials: The following supporting information can be downloaded at https://www.mdpi.com/article/10.3390/electronics15204652/s1, Table S1: Structured data-extraction template used in this review.

Author Contributions: Conceptualization, M.G. and E.S.; methodology, M.G. and E.S.; validation, M.G. and E.S.; formal analysis, M.G.; investigation, M.G. and E.S.; data curation, M.G. and E.S.; writing—original draft preparation, M.G.; writing—review and editing, M.G. and E.S.; visualization, M.G.; supervision, E.S.; project administration, M.G.; funding acquisition, M.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Scientific and Technological Research Council of Türkiye (TÜBİTAK) through the 1515 Frontier R&D Laboratories Support Program for Türk Telekom 6G R&D Lab, grant number 5249902.

Data Availability Statement: The structured data-extraction template used to collect study characteristics and findings (Section 4.5) is available as Supplementary Material accompanying this article.

Conflicts of Interest: Author Merve Güllü is employed by the company Turk Telekom. The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. This study is carried out under the TÜBİTAK 1515 Frontier R&D Laboratories Support Program for the Türk Telekom 6G R&D Lab. The funder is not involved in the study design, collection, analysis, interpretation of data, the writing of this article or the decision to submit it for publication.

References

1. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
2. Grover, L.K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1996; Volume STOC '96, pp. 212–219. [CrossRef]
3. Zhou, R.; Guo, H.; Teo, F.E.C.; Bakiras, S. A Survey on Post-Quantum Cryptography for 5G/6G Communications. In *Proceedings of the 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6. [CrossRef]
4. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
5. Geremew, A.; Mohammad, A. Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing. *Int. J. Eng. Sci. Technol.* **2024**, *6*, 338–365. [CrossRef]
6. Bowen, B.D.; Martin, K. Sizing up the Quantum Threat to Cyber Security: Making Sense of Quantum Computing Headlines. *Cyber Secur. Peer-Rev. J.* **2026**, *9*, 338–349. [CrossRef]
7. Vermeer, M.J.D.; Heitzenrater, C.; Parker, E.; Moon, A.; Lumpkin, D.; Awan, J. Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems. *J. Crit. Infrastruct. Policy* **2024**, *5*, 88–110. [CrossRef]
8. Chang, S.Y.; Khan, Q. Post-Quantum Cryptography in Networking Protocols: Challenges, Solutions, and Future Directions. *Cryptography* **2026**, *10*, 12. [CrossRef]
9. Montenegro, J.A.; Rios, R.; Lopez-Cerezo, J. A performance evaluation framework for post-quantum TLS. *Future Gener. Comput. Syst.* **2026**, *175*, 108062. [CrossRef]
10. Almutairi, M.; Sheldon, F.T. Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. *Eng* **2025**, *6*, 346. [CrossRef]
11. Wang, Y.; Shahril Ismail, E. A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT. *IEEE Access* **2025**, *13*, 112962–112977. [CrossRef]
12. Choudhury, B.; Hota, A.; Karmakar, M.; Saha, S.; Nag, A.; Nandi, S. A Comprehensive Survey on Pre Versus Post Quantum Security Schemes for 5G-Enabled IoT Applications. *IEEE Access* **2025**, *13*, 159305–159333. [CrossRef]
13. Shekhawat, H.; Gupta, D.S. A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8080. [CrossRef]
14. Almutairi, M.G.; Sheldon, F.T. Methodology and Architecture for Benchmarking End-to-End PQC Protocol Resilience in an IoT Context. *IoT* **2026**, *7*, 17. [CrossRef]
15. Hoque, S.; Aydeger, A.; Zeydan, E.; Liyanage, M. Analysis of Post-Quantum Cryptography in User Equipment in 5G and Beyond. In *Proceedings of the 2025 IEEE 50th Conference on Local Computer Networks (LCN)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9. [CrossRef]
16. Mehic, M.; Michalek, L.; Dervisevic, E.; Burdiak, P.; Plakalovic, M.; Rozhon, J.; Mahovac, N.; Richter, F.; Kaljic, E.; Lauterbach, F.; et al. Quantum Cryptography in 5G Networks: A Comprehensive Overview. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 302–346. [CrossRef]
17. Turnip, T.N.; Andersen, B.; Vargas-Rosales, C. Toward 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. *IEEE Commun. Surv. Tutor.* **2026**, *28*, 3311–3345. [CrossRef]
18. Adere, K.; Hailu, S.; Tseghai, A.; Haile, G.; Tamirat, B.; Bitew, W.; Abebe, M.; Kemal, A.; Silassie, S.W.; Regassa, D.; et al. Systematic review on securing IoT systems with post quantum cryptography emerging threats, countermeasures, and future research needs. *Discov. Internet Things* **2026**, *6*, 14. [CrossRef]
19. Laktionov, I.; Diachenko, G.; Moroz, D.; Getman, I. A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography. *IoT* **2025**, *6*, 61. [CrossRef]
20. Mahdi, L.H.; A. Abdullah, A. Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 21812–21821. [CrossRef]
21. Haider, Z.A.; Zeb, A.; Islam, A.; Rahman, T.; Arishi, A.; Ullah, I. Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms. *Comput. Sci. Rev.* **2026**, *59*, 100861. [CrossRef]

22. Nelufule, N. Post-Quantum Cryptography Standards for Future Proof IoT Security: A Literature Review. In Proceedings of the 2025 International Conference on Intelligent Digitization of Systems and Services (IDSS), Valencia, Spain, 18–21 August 2025; pp. 179–184. [CrossRef]
23. Kakoulli, E.; Zacharioudakis, E. Exploration of the Role of Cryptoprocessors in Advancing IoT Security. In *Proceedings of the 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*; IEEE: Piscataway, NJ, USA, 2024; pp. 524–531. [CrossRef]
24. Moon, S.Y.; Jo, B.H.; Azzaoui, A.E.; Singh, S.K.; Park, J.H. Edge-Fog Enhanced Post-Quantum Network Security: Applications, Challenges and Solutions. *Comput. Mater. Contin.* **2025**, *84*, 25–55. [CrossRef]
25. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ* **2021**, *372*, n160. [CrossRef] [PubMed]
26. Shea, B.J.; Reeves, B.C.; Wells, G.; Thuku, M.; Hamel, C.; Moran, J.; Moher, D.; Tugwell, P.; Welch, V.; Kristjansson, E.; et al. AMSTAR 2: A critical appraisal tool for systematic reviews that include randomised or non-randomised studies of healthcare interventions. *BMJ* **2017**, *358*, j4008. [CrossRef] [PubMed]
27. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report EBSE-2007-01; Keele University and Durham University: Keele, UK, 2007.
28. Popay, J.; Roberts, H.; Sowden, A.; Petticrew, M.; Arai, L.; Rodgers, M.; Britten, N.; Roen, K.; Duffy, S. *Guidance on the Conduct of Narrative Synthesis in Systematic Reviews*; ESRC Methods Programme; Lancaster University: Lancaster, UK, 2006.
29. *FIPS PUB 203*; Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, MD, USA, 2024.
30. Kwala, A.K.; Kant, S.; Mishra, A. Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. *Discov. Internet Things* **2024**, *4*, 13. [CrossRef]
31. *FIPS PUB 204*; Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, MD, USA, 2024.
32. *FIPS PUB 205*; Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, MD, USA, 2024.
33. Rescorla, E. *The Transport Layer Security (TLS) Protocol*, Version 1.3; Technical Report RFC 8446; IETF: Wilmington, DE, USA, 2018. Available online: https://www.rfc-editor.org/rfc/rfc8446 (accessed on 10 April 2026).
34. Kaufman, C.; Hoffman, P.; Nir, Y.; Eronen, P.; Kivinen, T. *Internet Key Exchange Protocol*, Version 2 (IKEv2); Technical Report RFC 7296; IETF: Wilmington, DE, USA, 2014. Available online: https://www.rfc-editor.org/rfc/rfc7296 (accessed on 10 April 2026).
35. Cano, A.; Garcia, C.R.; Frantz, R.; Monroy, I.T.; Imaña, J.L.; Vegas, J.J. Integrating Post-Quantum Cryptography Plugins for IPsec Offloads to Data Processing Units in the Cloud-Edge Continuum. In *Proceedings of the 2024 IEEE 32nd International Conference on Network Protocols (ICNP)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6. [CrossRef]
36. Lawo, D.C.; Abu Bakar, R.; Cano Aguilera, A.; Cugini, F.; Imaña, J.L.; Tafur Monroy, I.; Vegas Olmos, J.J. Wireless and Fiber-Based Post-Quantum-Cryptography-Secured IPsec Tunnel. *Future Internet* **2024**, *16*, 300. [CrossRef]
37. Liu, H.; Zhang, Z.; Zhou, M.; Hancke, G.P. Lightweight Hybrid Post-Quantum Communication VPN Architecture for Building-Wide IoT Systems. In *Proceedings of the 2025 IEEE 23rd International Conference on Industrial Informatics (INDIN)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
38. 3GPP. *Security Architecture and Procedures for 5G System*; Technical Specification TS 33.501, Release 18; 3rd Generation Partnership Project (3GPP): Sophia Antipolis, France, 2024. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (accessed on 10 April 2026).
39. Hanna, Y.; Pineda, D.; Veksler, M.; Paudel, M.; Akkaya, K.; Anastasova, M.; Azarderakhsh, R. Integrating Post-Quantum TLS into the Control Plane of 5G Networks. In *Proceedings of the 2024 IEEE International Performance, Computing, and Communications Conference (IPCCC)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–8. [CrossRef]
40. Corsi, A.; Gür, S.; Brighente, A.; Conti, M. Evaluation of Post-Quantum Key Encapsulation Methods in 5G Core Network. In *Proceedings of the 2025 IEEE Wireless Communications and Networking Conference (WCNC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
41. Yadav, A.K.; Choudhary, E.; Garg, O.; Liyanage, M. Post-Quantum Secure Lattice-Based 5G-AKA Protocol Resistant to Malicious Serving Networks with Perfect Forward Secrecy. In *Proceedings of the 2025 IEEE Conference on Communications and Network Security (CNS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9. [CrossRef]
42. Bormann, C.; Ersue, M.; Keranen, A. *Terminology for Constrained-Node Networks*; Technical Report RFC 7228; IETF: Wilmington, DE, USA, 2014. Available online: https://www.rfc-editor.org/rfc/rfc7228 (accessed on 10 April 2026).
43. Señor, J.; Portilla, J.; Portela-García, M. Performance Analysis of Postquantum Cryptographic Schemes for Securing Large-Scale Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2024**, *20*, 12339–12349. [CrossRef]

44. Banerjee, U. Energy-Efficient and Secure Clustering with Post-Quantum DTLS in Wireless Sensor Networks. In *Proceedings of the 2024 IEEE Symposium on Computers and Communications (ISCC)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6. [CrossRef]
45. Blanco-Romero, J.; Lorenzo, V.; Almenares, F.; Sánchez, D.D.; Campo, C.; Rubio, C.G. Integrating Post-Quantum Cryptography into CoAP and MQTT-SN Protocols. In *Proceedings of the 2024 IEEE Symposium on Computers and Communications (ISCC)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6. [CrossRef]
46. National Institute of Standards and Technology. *Transition to Post-Quantum Cryptography Standards*; Technical Report NIST IR 8547 (Initial Public Draft); NIST: Gaithersburg, MD, USA, 2024.
47. Kempf, M.; Gauder, N.; Jaeger, B.; Zirngibl, J.; Carle, G. A Quantum of QUIC: Dissecting Cryptography with Post-Quantum Insights. In *Proceedings of the 2024 IFIP Networking Conference (IFIP Networking)*; IEEE: Piscataway, NJ, USA, 2024; pp. 195–203. [CrossRef]
48. Rios, R.; Montenegro, J.A.; Muoz, A.; Ferraris, D. Toward the Quantum-Safe Web: Benchmarking Post-Quantum TLS. *IEEE Netw.* **2025**, *39*, 247–253. [CrossRef]
49. Rigon, P.; Fu, H.; Cordeiro, W.; Fung, C. Comprehensive Post-Quantum Cryptography Performance Evaluations for QUIC Protocol. In *Proceedings of the 2025 IEEE Conference on Communications and Network Security (CNS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9. [CrossRef]
50. Catoni, L.; Puliafito, C.; Dini, G. Fast and Secure Service Continuity in the Edge-Cloud Continuum: A Study of TLS 1.3 Resumption and Post-Quantum Key Exchange. In *Proceedings of the 2025 IEEE International Conference on Smart Computing (SMARTCOMP)*; IEEE: Piscataway, NJ, USA, 2025; pp. 396–401. [CrossRef]
51. Dong, B.; Wang, Q. EPQUIC: Efficient Post-Quantum Cryptography for QUIC-Enabled Secure Communication. In *Proceedings of the Great Lakes Symposium on VLSI 2025*; ACM: New York, NY, USA, 2025; Volume GLSVLSI '25, pp. 141–146. [CrossRef]
52. Frauenschläger, T.; Füreder, L.; Mottok, J. Enhancing Quantum-Safe Cryptography in TLS: The Role of Pre-Shared Keys. In *Proceedings of the 2025 International Conference on Applied Electronics (AE)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–8. [CrossRef]
53. Khan, Q.; Purification, S.; Cheruiyot, R.; Kim, J.; Kim, I.; Chang, S.Y. Post-Quantum Digital Signature and Authentication for eSIM in 5G Mobile Networking. In *Proceedings of the 2025 Silicon Valley Cybersecurity Conference (SVCC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–7. [CrossRef]
54. Montenegro, J.A.; Rios, R.; Bonilla, J. Comparative analysis of post-quantum handshake performance in QUIC and TLS protocols. *Comput. Netw.* **2026**, *275*, 111957. [CrossRef]
55. Hanna, Y.; Bozhko, J.; Tonyali, S.; Harrilal-Parchment, R.; Cebe, M.; Akkaya, K. A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. *Internet Things* **2025**, *33*, 101650. [CrossRef]
56. Jha, A.K.; Kashani, S.; Kim, S.W.; Khokhar, A.; Nait-Abdesselam, F. Post-Quantum SIM-Less Authentication: Scalable and Secure Solutions for FutureG IoT Networks. In *Proceedings of the MILCOM 2025—2025 IEEE Military Communications Conference (MILCOM)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
57. Sheldon, J.; Campbell, S.; Sanchez, J.; Pritchett, J.; Brizendine, B. Post-Quantum Cryptography on Constrained Networks: A Comparison of Algorithm Performance at Low Bandwidths. In *Proceedings of the 2025 ACM Southeast Conference*; ACM: New York, NY, USA, 2025; Volume ACMSE 2025, pp. 291–292. [CrossRef]
58. Liu, D.; Jang, S.I.; Sultan, N.; Lai, S.; Chau, S.C.K.; Chan, J.; Suzuki, H. Post-Quantum Cryptography Migration of a Physical 5G Testbed. In *Proceedings of the 2025 1st Workshop on Quantum-Resistant Cryptography and Security*; ACM: New York, NY, USA, 2026; Volume QRSEC '25, pp. 63–72. [CrossRef]
59. Sawant, S.V.; Rudra, B. Utilization of Quantum Random Numbers in Crystal-Kyber Based Post Quantum Virtual Private Network for Vehicular Communication. *IEEE Trans. Netw. Serv. Manag.* **2026**, *23*, 997–1013. [CrossRef]
60. Shim, H.; Kang, B.; Im, H.; Jeon, D.; Kim, S.M. QTrustNet Virtual Private Network (VPN): Enhancing Security in the Quantum Era. *IEEE Access* **2025**, *13*, 17807–17819. [CrossRef]
61. Raja, G.; Theerthagiri, S.; Raja, K.; Alagar Ramanujam, J.; Sadhasivam, T.; Vasudevan, P.; Arumugam, P.; Khowaja, S.A.; Dev, K. PQAKA: Post Quantum Authentication and Key Agreement Protocol for Intelligent Internet of Vehicles Over 5G. *IEEE Open J. Commun. Soc.* **2026**, *7*, 196–210. [CrossRef]
62. Joudah, R.H.; Manaa, M.E. A new approach to improving the security of the 5G-AKA using Crystals-Kyber post-quantum technologies and ASCON algorithm. *Int. J. Saf. Secur. Eng.* **2024**, *14*, 1729–1742. [CrossRef]
63. Bera, B.; Saha, S.; Das, A.K.; Rodrigues, J.J.P.C.; Sikdar, B. Fortifying V2RSU Communication with Post Quantum Security in the Green Internet of Vehicles. In *Proceedings of the ICC 2025—IEEE International Conference on Communications*; IEEE: Piscataway, NJ, USA, 2025; pp. 2026–2032. [CrossRef]
64. Kim, Y.; Seo, S.C. An Optimized Instantiation of Post-Quantum MQTT protocol on 8-bit AVR Sensor Nodes. In *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*; ACM: New York, NY, USA, 2025; Volume ASIA CCS '25, pp. 248–266. [CrossRef]

65. Setyowati, D.; Rimbawa, H.A.D.; Wadjdi, A.F. Performance Evaluation of Hybrid TLS with ML-KEM-768 for Post-Quantum Secure MQTT in Mobile IIoT Systems. In *Proceedings of the 2025 IEEE 11th International Conference on Computing, Engineering and Design (ICCED)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5. [CrossRef]
66. El-Hadedy, M.; Hwu, W.M. Thoth: Reliable Orchestration of Post-Quantum Secure Communication in Multi-Architecture Edge Clusters. In *Proceedings of the 2025 IEEE 36th International Symposium on Software Reliability Engineering Workshops (ISSREW)*; IEEE: Piscataway, NJ, USA, 2025; pp. 197–204. [CrossRef]
67. Ojetunde, B.; Kurihara, T.; Yano, K.; Sakano, T.; Yokoyama, H. Performance Evaluation of Post-Quantum Cryptography Algorithms for Secure Communication in Wireless Networks. In *Proceedings of the 2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9. [CrossRef]
68. Makka, S.; Ganesan, E.; Goswami, S.; Goyal, W.; Sahu, P.K.; Singh, A. Quantum Resilient Cryptographic Protocols in Modern Networks. *J. Internet Serv. Inf. Secur.* **2025**, *15*, 408–422. [CrossRef]
69. Al-Mekhlafi, Z.G.; Altmemi, J.M.H.; Al-Shareeda, M.A.; Al-Al-Hchaimi, A.A.J.; Gaber, T.; Homod, R.Z.; Mohammed, B.A.; Alshammari, G.; Al-Dhlan, K.A.; Alrashdi, R.; et al. A Post-Quantum Secure Solution for SECS/GEM Communications in Industrial Internet of Things (IIoT) Application. *IEEE Open J. Commun. Soc.* **2026**, *7*, 670–684. [CrossRef]
70. Styn, T.; Pitera, M.; Okoń, M.; Harasik, P.; Niemiec, M. Application of Post-Quantum Cryptography in IoT Networks. In *Proceedings of the MILCOM 2025—2025 IEEE Military Communications Conference (MILCOM)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
71. Smith, S.; Owens, K.; Kozan, K. Post-Quantum Cryptography on Constrained Networks. In *Proceedings of the 2025 IEEE International Carnahan Conference on Security Technology (ICCST)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–4. [CrossRef]
72. Smith, S.; Owens, K.; Kozan, K. Post Quantum Cryptography on Intravehicular Networks. In Proceedings of the 2025 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium, Novi, MI, USA, 12 August 2025. [CrossRef]
73. Atutxa, A.; Sanz, A.; Salegi, E.; Huarte, M.; Astorga, J.; Jacob, E. Authentication of the QKD classical channel through Post-Quantum Cryptography in a multi-site 5G/6G quantum-safe communication network. In *Proceedings of the 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 648–654. [CrossRef]
74. Sharma, A.; Rani, S. QCS-6G: A Standards-Aligned Quantum-Resilient Cryptographic Stack for Next-Generation Wireless Networks. *IEEE Commun. Stand. Mag.* **2025**, 1–7. [CrossRef]
75. Soni, L.; Chandra, H.; Gupta, D.S. LB-RFID: Provably Secure Post-quantum Authentication Protocol for RFID Devices in Resource-constrained IoT Environment. *Wirel. Pers. Commun.* **2025**, *144*, 205–230. [CrossRef]
76. Nurmurodov, J.; Askaraliyev, O.; Sharma, R.R.; Mamirov, K. ESP32-Enabled Secure LiFi Sensor Nodes with Lightweight Post-Quantum Cryptography for Indoor IoT. In *Proceedings of the 2025 Optical Communication, Photonics, Telecommunications, and Intelligent Machine Applications (OPTIMA)*; IEEE: Piscataway, NJ, USA, 2025; pp. 429–435. [CrossRef]
77. Dhatterwal, J.S.; Dipesh. Mathematically-Driven Architectures and Cryptographic Protocols for Ultra-Reliable, LowLatency, and Scalable Secure Networking in PostQuantum 6G Communication Systems. In *Proceedings of the 2025 International Conference on Power Electronics and Energy (ICPEE)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
78. U, S.; Gudodagi, R.; H T, M. Quantum-Resistant Cryptography for Military Communications. In *Proceedings of the 2025 IEEE Space, Aerospace and Defence Conference (SPACE)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
79. Scalise, P.; Garcia, R.; Boeding, M.; Hempel, M.; Sharif, H. An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics* **2024**, *13*, 4258. [CrossRef]
80. Khan, Q.; Purification, S.; Chang, S.Y. Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber). *Information* **2025**, *16*, 617. [CrossRef]
81. Sowa, J.; Hoang, B.; Yeluru, A.; Qie, S.; Nikolich, A.; Iyer, R.; Cao, P. Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways. In *Proceedings of the 2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*; IEEE: Piscataway, NJ, USA, 2024; Volume 1, pp. 1835–1846. [CrossRef]
82. Dong, B.; Wang, Q. Optimizing Post-Quantum Crypto Algorithms in Embedded IoT Systems. In *Proceedings of the 2025 26th International Symposium on Quality Electronic Design (ISQED)*; IEEE: Piscataway, NJ, USA, 2025. [CrossRef]
83. Braeken, A.; Yadav, A.K.; Munilla, J. A Practical Transition to Post-Quantum Security in 5G-AKA. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 13071–13084. [CrossRef]
84. Martins, I.B.; Lima, M.P.; Cruz, A.P.; Immich, R.; Fontes, R.D.R. Redefining the Security of the Routing Protocol for Low-Power and Lossy Networks (RPL) with Post-Quantum Cryptography. In *Proceedings of the 2025 21st International Conference on Network and Service Management (CNSM)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5. [CrossRef]
85. Kumar, G.; Killi, B.R.; Das, A.K.; Park, Y. Post-Quantum Secure Lattice-Based Lightweight Authentication and Key Agreement Scheme for Multilayer IoT-Enabled Smart Grid System. *IEEE Internet Things J.* **2026**, *13*, 24604–24617. [CrossRef]
86. Castiglione, A.; Elia, T. Securing in-vehicle communications through post-quantum cryptography and network segmentation. *Comput. Electr. Eng.* **2025**, *126*, 110488. [CrossRef]

87. Nsour, A. Quantum-Resilient Secure Onboard Communication (QRSecOC): Integrating Post-Quantum Cryptography for Robust Automotive Network Security. *Int. J.* **2025**, *12*, 27–48. [CrossRef] [PubMed]
88. Spalas, K.; Kolokotronis, N. Post-Quantum Security Evaluation of Aeronautical Communications. In *Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience (CSR)*; IEEE: Piscataway, NJ, USA, 2025; pp. 295–301. [CrossRef]
89. Devaraj, P.; Chaman Basha, S.A.; Panarkuzhiyil Santhosh, N.N.; Panda, N. A Post-Quantum Secure Architecture for 6G-Enabled Smart Hospitals: A Multi-Layered Cryptographic Framework. *Future Internet* **2026**, *18*, 165. [CrossRef]
90. Hasan Somrat, M.M.; Tuli, E.A.; Lee, J.M.; Kim, D.S. Performance Analysis of Post-Quantum Cryptography for Military Communications. In *Proceedings of the 2025 International Conference on Mobile, Military, Maritime IT Convergence (ICMIC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 198–201. [CrossRef]
91. Mrinal, K.; S, V. Performance Analysis of Post-Quantum Cryptographic Algorithms in Software-Defined Networks. In *Proceedings of the 2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
92. Satish, E.G.; Mounika, B.V.S.; Anand, A.; Kumar Pamidi Venkata, A.; Chandrashekar, G. Adaptive Sdn-Based Lightweight Cryptographic Framework for Post-Quantum Secure Smart Home Iot Networks. In *Proceedings of the 2025 2nd International Conference on Software, Systems and Information Technology (SSITCON)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–8. [CrossRef]
93. Khan, Q.; Purification, S.; Chang, S.Y. Post-Quantum Key Exchange and ID Encryption Analyses for 5G Mobile Networking. In *Proceedings of the NOMS 2025—2025 IEEE Network Operations and Management Symposium*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9. [CrossRef]
94. Maqsood, T.B.; Hameed, K.; Junaid, M.; Tahir, N. Enhancing IoT Healthcare Security with Post-Quantum Cryptography: A Performance and Case Study Analysis. In *Proceedings of the 2025 6th International Conference on Advancements in Computational Sciences (ICACS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–8. [CrossRef]
95. Zaheer, A.N.; Farhan, M.; Rehan Naeem, M.; Alnfiai, M.M. Quantum-Resilient Cryptographic Frameworks: Design and Analysis of Post-Quantum Algorithms for Secure and Efficient Edge-Assisted IoT Ecosystems in Consumer Electronics Devices. *IEEE Trans. Consum. Electron.* **2025**, *71*, 11258–11268. [CrossRef]
96. Mansoor, K.; Afzal, M.; Iqbal, W.; Abbas, Y. Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Clust. Comput.* **2024**, *28*, 93. [CrossRef]
97. Ladino, I.; Gomez, C.; Corredor, C.; Toro, L. Low-Compute Cryptography for IoT: Challenges, Solutions, and Perspectives. In *Proceedings of the 2024 Congreso Internacional de Innovación Y Tendencias en Ingeniería (CONIITI)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5. [CrossRef]
98. Nielsen, M.V.; Kjeldsen, M.R.; Turnip, T.; Andersen, B. Post-Quantum Digital Signature Algorithms on IoT: Evaluating Performance on LoRa ESP32 Microcontroller. In *Proceedings of the 22nd International Conference on Security and Cryptography—SECRYPT*; SciTePress: Setúbal, Portugal, 2025; pp. 592–600. [CrossRef]
99. Samandari, J.; Gritti, C. Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures. In *Proceedings of the 2024 21st Annual International Conference on Privacy, Security and Trust (PST)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–11. [CrossRef]
100. Ghaban, W. Lightweight Post-Quantum Authentication and Key Agreement Protocol for Secure Smart Home IoT Control. *IEEE Trans. Consum. Electron.* **2026**, *72*, 1890–1903. [CrossRef]
101. Sandanamudi, P.K.; Agrawal, N.; Tripathi, N.; N, P.K.B. Securing UAV Communications: A Comparative Performance Analysis of Post-Quantum Cryptographic Techniques. In *Proceedings of the 2025 17th International Conference on Communication Systems and NETworks (COMSNETS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1096–1101. [CrossRef]
102. Roodsari, P.D.; Sarmadi, S.B.; Boorani, H.M. Post-Quantum Authentication and Communication Security for Drone Networks. *IEEE Trans. Dependable Secur. Comput.* **2026**, *23*, 3452–3463. [CrossRef]
103. Chen, A.C.H.; Lin, B.Y. Hybrid Scheme of Post-Quantum Cryptography and Elliptic-Curve Cryptography for Certificates A Case Study of Security Credential Management System in Vehicle-to-Everything Communications. In *Proceedings of the 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*; IEEE: Piscataway, NJ, USA, 2024; Volume 1, pp. 426–430. [CrossRef]
104. Aslam, A.M.; Bhardwaj, A.; Chaudhary, R. Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography. *Veh. Commun.* **2025**, *52*, 100880. [CrossRef]
105. Alsaadi, M.; Aldawsari, H.; Prasad Kasaraneni, B.; Kanth Kondapaka, K.; Reddy Gayam, S.; Thuniki, P.; Putha, S.; Zulfizar Alimovna, P.; Gupta, S. Post-Quantum Verifiable Decryption for Secure and Scalable V2I Communication in Consumer Driven-Intelligent Transportation Systems. *IEEE Trans. Consum. Electron.* **2025**, *71*, 11248–11257. [CrossRef]
106. Mishra, D.; Pursharthi, K.; Singh, M.; Mishra, A. Construction of post quantum secure authenticated key agreement protocol for dew-assisted IoT systems. *Int. J. Inf. Secur.* **2024**, *24*, 19. [CrossRef]
107. Roy, K.S.; Deb, S.; Kalita, H.K. A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks. *Digit. Commun. Netw.* **2024**, *10*, 989–1000. [CrossRef]

108. Sethu Subramanian, N.; Jain, K.; Krishnan, P.; Prabu, P.; Ganeshkumar, P. Embedded SIM (eSIM)-Based PQC-Enabled Authentication and Provisioning Techniques for Enhancing Security in Edge-Based IoT Ecosystem. *IEEE Trans. Consum. Electron.* **2025**, *71*, 11183–11197. [CrossRef]
109. Nakka, K.; Ahmad, S.; Kim, T.; Atkinson, L.; Ammari, H.M. Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks. In *Proceedings of the 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–5. [CrossRef]
110. Hoque, S.; Aydeger, A.; Zeydan, E. Post-Quantum Secure UE-to-UE Communications. In *Proceedings of the 2024 15th International Conference on Network of the Future (NoF)*; IEEE: Piscataway, NJ, USA, 2024; pp. 28–30. [CrossRef]
111. Cíbik, P.; Ricci, S.; Dobiáš, P.; Hajný, J.; Malina, L.; Havlín, J. Quantum-resistant hardware-accelerated IoT traffic encryptor. *Internet Things* **2025**, *31*, 101554. [CrossRef]
112. Bera, B.; Parameswarath, R.P.; Sikdar, B. Fortifying the Security of Smart Grid Networks with Post-Quantum Communication. *IEEE Trans. Smart Grid* **2025**, *16*, 5430–5445. [CrossRef]
113. Akram, M.A.; Biswas, A.K.; O'Neill, M.; Khalid, A.; Mian, A.N. HBQS: Lightweight Post-Quantum Secure Authentication for Satellite Networks Leveraging Hardware TRNG and PUFs. *IEEE Internet Things J.* **2026**, *13*, 25256–25273. [CrossRef]
114. Ghosh, T.; Nath, I. Secure Satellite Communication in the Post-Quantum Era: A Lattice-Based Cryptographic Approach. *Int. J. Satell. Commun. Netw.* **2026**, *44*, 524–543. [CrossRef]
115. Ahmad, A.; Jagatheswari, S. Lattice-Based Three Party Authenticated Key Agreement Scheme in Medical IoT for Post-Quantum Environment. *IEEE Access* **2024**, *12*, 157247–157259. [CrossRef]
116. Cao, Z.; Geng, B.; Yu, D. Consumer Technology in Focus: Post-Quantum Security for Fog Computing IoT Systems Against Eavesdropping. *IEEE Trans. Consum. Electron.* **2025**, *71*, 4972–4982. [CrossRef]
117. Kaleem, Z.; Khan, M.U.; Suleman, A.; Khalid, W.; Wong, K.K.; Yuen, C. Quantum Skyshield: Quantum Key Distribution and Post-Quantum Authentication for Low-Altitude Wireless Networks in Adverse Skies. *IEEE Wirel. Commun.* **2026**, *33*, 235–243. [CrossRef]
118. Aguilar, W.; Calderon, G.; Alfaro, C. Comparison and Grouping of Post-Quantum Digital Signature Algorithms for Mobile Applications, IoT, and Servers. In *Proceedings of the 2025 IEEE Central America and Panama Student Conference (CONESCAPAN)*; IEEE: Piscataway, NJ, USA, 2025;, pp. 1–6. [CrossRef]
119. Mills, M.O.; Ghorbani, A.A. PQC-OAV in Action: A High-Fidelity Prototype for Evidential Assurance of PQC in TLS. In *Proceedings of the 2025 International Conference on Intelligent Computing and Next Generation Networks (ICNGN)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5. [CrossRef]
120. Raavi, M.; Khan, Q.; Wuthier, S.; Chandramouli, P.; Balytskyi, Y.; Chang, S.Y. Security and Performance Analyses of Post-Quantum Digital Signature Algorithms and Their TLS and PKI Integrations. *Cryptography* **2025**, *9*, 38. [CrossRef]
121. Aissaoui, R.; Deneuville, J.C.; Guerber, C.; Pirovano, A. Evaluating Post-Quantum Key Exchange Mechanisms for UAV Communication Security. In *Proceedings of the 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–10. [CrossRef]
122. Mansoor, K.; Afzal, M.; Iqbal, W.; Abbas, Y.; Mussiraliyeva, S.; Chehri, A. PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet Things* **2024**, *27*, 101228. [CrossRef]
123. Sim, M.; Song, G.; Eum, S.; Lee, M.; Yoon, S.; Baksi, A.; Seo, H. Integrating and Benchmarking KpqC in TLS/X.509. *Electronics* **2025**, *14*, 3717. [CrossRef]
124. Maya, W.R.; Arif, T.Y.; Riza, H.; Adriman, R. Optimized and Secure Hybrid Key Exchange Model for Post-Quantum Digital Communications. In *Proceedings of the 2025 3rd International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*; IEEE: Piscataway, NJ, USA, 2025; pp. 133–138. [CrossRef]
125. Do, T.B.; Tran, Q.H. A hybrid lightweight and post-quantum communication framework for NB-IoT networks. *Microsyst. Technol.* **2026**, *32*, 37. [CrossRef]
126. Magyari, A.; Chen, Y. Post-Quantum SecureSensor Networks: Combining Ascon and SPHINCS+. In *Proceedings of the 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*; IEEE: Piscataway, NJ, USA, 2024; pp. 139–144. [CrossRef]
127. Zhang, B.; Hong, J.; Mao, G.; Shen, S.; Yang, H.; Li, G.; Lyu, S.; Hung, P.S.Y.; Cheung, R.C.C. HySecure: FPGA-Based Hybrid Post-Quantum and Classical Cryptography Platform for End-to-End IoT Security. *Electronics* **2025**, *14*, 3908. [CrossRef]
128. Elnour, A.A.H. Integrating Post Quantum Cryptography (PQC) for End-to-End Security in Edge and IoT Environments. *IEEE Trans. Consum. Electron.* **2026**, 1. [CrossRef]
129. Cruz-Piris, L.; Marín-López, A.; Álvarez Campana, M.; Sanz, M.; Moreno, J.I.; Arroyo, D. Measuring the impact of post quantum cryptography in Industrial IoT scenarios. *Internet Things* **2025**, *34*, 101793. [CrossRef]

130. Jang, S.; Lee, H.S.; Agrawal, R.S.; Maji, S.; Gierlach, A.; Byrne, C.A.; Flaumenhaft, B.; Schmidt, K.; Li, J.; Traverso, G.; et al. Post Quantum Secure Communication Protocol with Ultra Low-Power Hardware Solution for Ingestible Medical Device. In *Proceedings of the 2025 47th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–7. [CrossRef] [PubMed]
131. Holgado-Moreno, A.; Portilla, J.; López-Fernández, D.; Redondo, L. Energy Consumption Benchmarking of Post-Quantum Cryptography on Resource-Constrained IoT Nodes. *IEEE Internet Things J.* **2026**, *13*, 19562–19573. [CrossRef]
132. Sharma, R.; Syed, M.K.; Ajmera, S.; Sandhiya, S.; Dash, M.; Balakumar, A. Post Quantum Secure Framework for IoT Based EV Battery Swapping Stations in Sustainable Transport Networks. In *Proceedings of the 2025 IEEE 2nd International Conference on Green Industrial Electronics and Sustainable Technologies (GIEST)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5. [CrossRef]
133. Hayouni, H. Adaptive post-quantum security framework for wireless sensor networks using lightweight cryptography and context-aware key management. *J. Supercomput.* **2025**, *81*, 1426. [CrossRef]
134. Solijon Ugli, I.S.; Abed Hussein, A.; Mohammed, N.Q.; Qays, A.; Abbas, H.H. Post-Quantum Key Exchange for IoT Devices Using Kyber512 Lattice-Based Encryption Algorithm. In Proceedings of the 2025 International Conference on Next Generation Computing Systems (ICNGCS), Coimbatore, India, 21–22 August 2025; pp. 1–7. [CrossRef]
135. S, L.B.; Kaulgud, N. Integrating Post-Quantum Cryptography in Transport Layer Security 1.3 for Iot: A Performance Analysis on Resource-Constrained Hardware. In *Proceedings of the 2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–8. [CrossRef]
136. Katragadda, N.D.; Fatima, A.; Yadla, J.; ReshmaReddy, T.; Shital, C.; Parvathi, B. Quantum-Resilient Communication Protocol for Secure IoT Networks using Post-Quantum Cryptography and HMAC Integration. In *Proceedings of the 2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1317–1323. [CrossRef]
137. Vellela, S.S.; Anusha, P.; Vullam, N.R.; Jala, J.; Bellapu, V.S.; Vindhya, A.S. Quantum Cryptography and Key Distribution for Secure Communication in the Post Quantum World. In *Proceedings of the 2025 International Conference on Sustainable Communication Networks and Application (ICSCN)*; IEEE: Piscataway, NJ, USA, 2025; pp. 619–624. [CrossRef]
138. Blanchet, B.; Jacomme, C. Post-Quantum Sound CryptoVerif and Verification of Hybrid TLS and SSH Key-Exchanges. In *Proceedings of the 2024 IEEE 37th Computer Security Foundations Symposium (CSF)*; IEEE: Piscataway, NJ, USA, 2024; pp. 543–556. [CrossRef]
139. Aljamal, M.; Khassawneh, B.S.; Alsarhan, A.; Okour, S.; Almusfar, L.A.; AlThani, B.F.; Aldossary, W. A Novel Dual-Layer Quantum-Resilient Encryption Strategy for UAV–Cloud Communication Using Adaptive Lightweight Ciphers and Hybrid ECC–PQC. *Computers* **2026**, *15*, 101. [CrossRef]
140. Zafar, A.; Iqbal, S.S. Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework. *Discov. Comput.* **2025**, *28*, 202. [CrossRef]
141. Sanon, S.P.; Schotten, H.D. Securing Mobile Networks in the Quantum Era: Imperative Role of Post-Quantum Cryptography. In *Proceedings of the 2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*; IEEE: Piscataway, NJ, USA, 2025; pp. 721–726. [CrossRef]
142. Shahid, A.B.; Mansoor, K.; Bangash, Y.A.; Iqbal, W.; Mussiraliyeva, S. Post-quantum cryptographic authentication protocol for industrial IoT using lattice-based cryptography. *Sci. Rep.* **2026**, *16*, 9582. [CrossRef] [PubMed]
143. Maurya, S.; Kasture, S.; Shukla, A. Quantum Cryptography for Secure Communications in Industrial Mechatronics and Embedded Systems. In *Proceedings of the 2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–8. [CrossRef]
144. Sepúlveda, J.; Marchsreiter, D.; Cardano, F.M. Hybrid Quantum-secure Group-based Communication with PQC and QKD. In *Proceedings of the 2025 28th Euromicro Conference on Digital System Design (DSD)*; IEEE: Piscataway, NJ, USA, 2025; pp. 515–522. [CrossRef]
145. Aquina, N.; Rommel, S.; Monroy, I.T. Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution. In *Proceedings of the 2024 24th International Conference on Transparent Optical Networks (ICTON)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–4. [CrossRef]
146. Ojetunde, B.; Kurihara, T.; Yano, K.; Sakano, T.; Yokoyama, H. A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication. *Network* **2025**, *5*, 20. [CrossRef]
147. Binti Mustaffa, N.M.; Balqis Binti Mat Daud, N.; Sase, T. Feasibility of Quantum Cryptography with AES for Secure Communication. In *Proceedings of the 2025 10th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
148. Astrizi, T.L.; Custódio, R. Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption. *Sensors* **2024**, *24*, 7300. [CrossRef] [PubMed]
149. Zhou, R.; Guo, H.; Teo, F.E.C. Investigating Post-Quantum Cryptography to Secure Transmitted Data via Mobile Communication. *Electronics* **2026**, *15*, 1275. [CrossRef]

150. Logeshwaran, J.; Dhanasekaran, S.; Sama, M.; Sati, D.C.; Kumar, J.; Garg, A. Post-Quantum Cryptography for Securing Next-Generation Communication Networks. In *Proceedings of the 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)*; IEEE: Piscataway, NJ, USA, 2025; pp. 805–810. [CrossRef]
151. National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism*; Technical Report FIPS 203 (Initial Public Draft); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [CrossRef]
152. National Institute of Standards and Technology. *Special Publication 800-227: Recommendations for Key Encapsulation Mechanisms*; Technical Report NIST SP 800-227; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024.
153. National Institute of Standards and Technology. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024.
154. Souvatzidaki, K.; Limniotis, K. Post-Quantum Key Exchange in TLS 1.3: Further Analysis on Performance of New Cryptographic Standards. *Cryptography* **2025**, *9*, 73. [CrossRef]
155. Saluja, I.; Desai, L.R.; Bhardwaj, A.; Deshpande, V.; Singh, N.; Gawade, P. Utilizing post-quantum cryptography to secure Internet of Things (IoT) devices against quantum attacks. *J. Discret. Math. Sci. Cryptogr.* **2026**, *29*, 589–597. [CrossRef]
156. José Díaz Rivera, J.; Vilalta, R.; Muñoz, R.; Alemany, P.; Renom, L.G. Leveraging PQC and Blockchain for Secure and Verifiable SDN Controller Communication. In *Proceedings of the 2025 IEEE 11th International Conference on Network Softwarization (NetSoft)*; IEEE: Piscataway, NJ, USA, 2025; pp. 567–572. [CrossRef]
157. Minton, J.; Collins, D.; Creech, M.; Grossman, J.; Manspeaker, A.; Hwang, G.; Rea, C. Post-Quantum UAV Communications Encryption Tester (P-QUAVCET)*. In *Proceedings of the 2025 International Conference on Unmanned Aircraft Systems (ICUAS)*; IEEE: Piscataway, NJ, USA, 2025; pp. 595–601. [CrossRef]
158. Vasco, M.I.G.; Steinwandt, R. Scalable Authenticated Group Key Establishment in Quantum and Post-Quantum Networks. *Informatica* **2025**, *36*, 315–335. [CrossRef]
159. Yang, Y.; Zhao, R.; Yin, F.; Wang, K. K-PAKE: Post quantum password authentication key exchange protocol for satellite networks. *Clust. Comput.* **2025**, *28*, 223. [CrossRef]
160. Narayanan, S.; Archana, K.S.; Rajesh, A.; Parthiban, N.; Srinivasan, V.; Sheela, S.N. Quantum-Resilient IoT Communication Framework Using Post-Quantum Cryptography and Blockchain for Secure Edge Devices. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2026**, *50*, 203–221. [CrossRef]
161. De Zoysa, D.B.K.; Perera, M.V.V.; Weerasinghe, H.D. A Hybrid Framework for Quantum-Resistant TLS Handshakes with PQC, QKD and Classical Cryptography. In *Proceedings of the 2025 International Conference on Advances in Technology and Computing (ICATC)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–7. [CrossRef]
162. Ehsan, M.A.; Alayed, W.; Rehman, A.U.; Hassan, W.U.; Zeeshan, A. Post-Quantum KEMs for IoT: A Study of Kyber and NTRU. *Symmetry* **2025**, *17*, 881. [CrossRef]
163. Rahmati, M.; Rahmati, N. Lightweight post-quantum cryptographic frameworks for real-time secure communications in IoT edge networks. *Telecommun. Syst.* **2025**, *88*, 136. [CrossRef]
164. Mezrag, F.; Chikouche, N.; Bahache, A.N. A Comparative Analysis of Classical and Post-Quantum Public-Key Cryptography on Resource-Constrained IoT Devices. In *Proceedings of the 2025 2nd International Conference of Advanced Technology in Electronic and Electrical Engineering (ICATEEE)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
165. Ramagundam, S.; Karamchandani, H.; Patil, G.U.; Subramanium, P. Context-aware lightweight and post-quantum cryptographic framework for secure wireless communication. *J. Discret. Math. Sci. Cryptogr.* **2025**, *28*, 2037–2047. [CrossRef]
166. Rawal, D.; Seedorf, J.; Jha, N. Performing Classical and Post-Quantum Cryptography on IoT Data: An Evaluation. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2025**, *XLVIII-4/W16-2025*, 91–97. [CrossRef]
167. Upadhyay, N.K.; Periyasamy, S.; Kumar, V. Lightweight Cryptographic Protocols for Enhanced Security in the Iot: A Survey. In *Proceedings of the 2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]

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