social Informatics Business, Politics, Law, Environmental Sciences & Technology Journal

Vol 12, No 1, March, 2026 Series

A Risk-Aware Digital Forensic Intelligence Framework for Post-Quantum Authentication Codes: A Systematic Literature Review

[1]Ojeniyi, J.O., [1]Fasola, O.O., [2]Onyeabor, G.A., [1]Joshua, D.H., [1]Attahiru, H., [1]Usiju, A.M., [1]Solomon, O.O. & [1]Sheriffdeen, Y.

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[2]Department of Data Science, Federal University of Technology, Minna, Nigeria
E-mail: ojeniyija@futminna.edu.ng, Sanjo.fasola@futminna.edu.ng, grace.onyeabor@gmail.com, attahiruhmte25266@st.futminna.edu.ng, Antawamumte25252@st.futminna.edu.ng, solozo@futminna.edu.ng, Yunussmte25282@st.futminn.edu.ng

ABSTRACT

The rapid progress of quantum computing poses a significant risk to the security principles of current cryptographic systems, highlighting the urgent need to adopt post-quantum cryptography (PQC). At the same time, digital forensic investigations are grappling with growing difficulties in preserving the integrity, authenticity, and chain-of-custody compliance of evidence amid increasingly complex threat landscapes. This systematic literature review explores the intersection of risk-aware digital forensic intelligence frameworks and post-quantum authentication codes, focusing on the theoretical underpinnings, practical applications, and emerging challenges. A comprehensive analysis of over 120 peer-reviewed publications in post-quantum cryptography, digital forensics, risk management, and authentication systems identifies critical research gaps and proposes an integrated framework that connects forensic investigation methodologies with quantum-resistant authentication mechanisms. The findings indicate that hybrid cryptographic approaches, which combine classical and post-quantum primitives, offer superior performance in transitional environments. Additionally, AI-enhanced forensic frameworks substantially improve threat detection accuracy and evidence preservation. This study formulates research questions focused on framework integration, risk assessment methodologies, and regulatory compliance, thereby offering structured guidance for researchers, practitioners, and policymakers during the quantum-safe transition era.

Keywords: Post-quantum Cryptography, Digital Forensics, Risk Management, Authentication Codes, Evidence Integrity, Hybrid Cryptography, Forensic Intelligence.

Journal Reference Format:
Ojeniyi, J.O., Fasola, O.O., Onyeabor, G.A., Joshua, D.H., Attahiru, H., Usiju, A.M., Solomon, O.O. & Sheriffdeen, Y. (2026): A Risk-Aware Digital Forensic Intelligence Framework for Post-Quantum Authentication Codes: A Systematic Literature Review. Social Informatics, Business, Politics, Law, Environmental Sciences & Technology Journal. Vol. 12, No. 1. Pp 61-84.. www.isteams/socialinformaticsjournal. dx.doi.org/10.22624/AIMS/SIJ/V12N1P7

1. INTRODUCTION

The current cryptography infrastructure faces an existential threat from the development of large-scale quantum computers (Shaikh et al., 2024). Widely used asymmetric cryptographic systems like RSA and Elliptic Curve Cryptography (ECC), which form the basis for digital authentication, secure communication, and digital signatures, can be effectively broken by quantum algorithms like Shor's

and Grover's algorithms (Banait et al., 2024). This issue directly affects digital forensic investigations, since the authenticity and integrity of evidence heavily rely on soon-to-be-outdated cryptographic techniques. Because it allows for the methodical investigation of cybercrimes, incident response, and digital evidence collecting, digital forensics has become a key discipline in modern law enforcement and cybersecurity operations (Alqahtany & Syed, 2024). However, upholding chain-of-custody compliance, avoiding tampering, and guaranteeing admissibility in court are major obstacles for conventional digital forensic frameworks (Nath et al., 2024). These difficulties become significantly more serious when combined with the threat posed by quantum computing, since cryptographically sealed forensic artifacts and digitally signed evidence will be useless against sufficiently sophisticated quantum attackers.

One important area of research is the merging of digital forensic intelligence with post-quantum cryptography. Building reliable forensic systems that are resistant to both conventional and quantum attacks requires risk-aware frameworks that methodically evaluate threat landscapes, rank mitigation techniques, and incorporate strong authentication methods (Olaniyi et al., 2024). This shift is made more urgent by the "Harvest Now, Decrypt Later" threat model, in which attackers gather encrypted forensic evidence for later decryption after quantum capabilities are developed (Bekarystankyzy & Zhailin, 2025).

Modern digital forensic investigations work inside a crucial window of vulnerability. Forensic evidence is still produced, gathered, and archived by organizations employing traditional cryptographic safeguards that offer no guarantee against upcoming quantum attacks. Concurrently, NIST's August 2024 standardization of post-quantum cryptographic primitives offers a chance for proactive adoption, although there are still major implementation issues that need to be addressed (Abbasi et al., 2025).

Important issues consist of:

1. Cryptographic Obsolescence: Historical forensic evidence may no longer be accepted due to the cryptographic invalidity of traditional RSA and ECC-based authentication codes (Tadepalli, 2024).
2. Forensic Integrity Assurance: Quantum-resistant cryptographic foundations are absent from current chain-of-custody techniques (Ghozali et al., 2025).
3. Risk Assessment Gaps: According to Ogbole et al. (2025), digital forensic frameworks lack thorough risk models that incorporate post-quantum threat environments with evidence retention needs.
4. Performance-Security Trade-offs: Post-quantum techniques complicate deployment in forensic systems with limited resources by introducing computational complexity, latency penalties, and larger key sizes (Borges et al., 2020).
5. Uncertainty in Regulation: Standards for quantum-safe evidence management have not yet been developed by legal and compliance frameworks (Kong et al., 2024).

The following research questions are addressed in this systematic review:

- **RQ1:** How do performance characteristics differ in various deployment contexts, and what are the theoretical underpinnings and real-world applications of post-quantum cryptographic algorithms for authentication code generation?
- **RQ2:** How can risk-aware frameworks prioritize mitigation techniques across organizational hierarchies and methodically evaluate quantum computing vulnerabilities to digital forensic operations?
  RQ3: What integration techniques and architectural patterns allow post-quantum authentication codes to be easily integrated into current digital forensic frameworks while preserving backward compatibility?
  RQ4: How might AI-driven intelligence improve forensic analysis, threat detection, and evidence gathering in quantum-resistant environments?
  RQ5: What legal requirements are necessary, and how should chain-of-custody protocols develop to offer cryptographic assurance resistant to both conventional and quantum adversaries?

Publications from 2020 to 2026 are included in this systematic literature review, which focuses on the intersection of:

1. NIST-standardized algorithms (Kyber, Dilithium, SPHINCS+, BIKE, Classic McEliece) and their uses in post-quantum cryptography.
2. Digital Forensics: Methods for gathering, storing, analyzing, and maintaining evidence.
3. Risk Management: Frameworks for risk prioritization, vulnerability assessment, and threat modeling.
4. Cryptographic key management, continuous authentication, and multi-factor authentication are examples of authentication systems.
5. New technologies: AI/ML for forensic automation, block-chain for evidence integrity, and integration of quantum key distribution.

The review aims to:

1. Compile the most recent findings in digital forensics and post-quantum cryptography.
2. Determine design patterns and integration obstacles for quantum-safe forensic frameworks.
3. Examine risk assessment techniques that are relevant to quantum transition planning.
4. Analyze deployment viability and performance attributes.
5. Suggest future lines of inquiry and priorities for standardization

2. RELATED WORK

2.1 Post-Quantum Cryptography Foundations.

2.1.1 Quantum Computing Threats to Classical Cryptography.

Classical cryptographic security methods are seriously threatened by quantum computing, which is a paradigm shift in processing power (Shakeel & Batool, 2025). The biggest threat comes from quantum algorithms, which effectively solve challenging mathematical issues that are essential to RSA and ECC security.

Compared to sub-exponential classical methods, Shor's approach can factor big integers and compute discrete logarithms in polynomial time, breaking both RSA and ECC in roughly O(log3 N) time complexity (Shaikh et al., 2024). Although there is disagreement over when practical quantum threats will materialize, it is generally accepted that Cryptographically Relevant Quantum Computers (CRQCs) that can crack 2048-bit RSA encryption could appear in ten to fifteen years (Mobilon et al., 2025). This makes the switch to quantum-resistant encryption urgently necessary, especially for data with long-term confidentiality requirements or systems needing decades-long non-repudiation guarantees.

2.1.2 NIST Standardization and PQC Algorithm Categories.

Post-quantum cryptography standardization was started by the National Institute of Standards and Technology in 2016, and final choices were announced in August 2024 (Sahu et al., 2026). The chosen algorithms fall into four main categories:

1. **lattice-based cryptography:** Key encapsulation using CRYSTALS-Kyber (ML-KEM) and digital signatures using CRYSTALS-Dilithium (ML-DSA). Kyber exhibits signature latencies of less than one millisecond with key sizes ranging from 768 to 1024 bytes (Al-Fatlawi et al., 2025). With security levels ranging from NIST Level 1 (equal to 128-bit classical security) to Level 5, lattice-based systems offer robust security assurances based on the Learning With Errors (LWE) problem (Abbasi et al., 2025).
2. **Hash-Based Signatures:** Using hash chains, SPHINCS+ provides stateless signature generation with security based on SHA-256 collision resistance. Compared to lattice-based alternatives, SPHINCS+ produces larger signatures (4KB) and needs longer generation times, but providing superior security assurance (Borges et al., 2020).
3. **Code-Based Cryptography:** For security, classic McEliece and BIKE use error correction codes. These algorithms have significant key size penalties (13KB–49KB), which restricts adoption in bandwidth-constrained situations despite providing robust security assurances and resistance to known attacks (Maduni et al., 2025).
4. **Multivariate Polynomial Cryptography:** Rainbow and other similar systems rely on the challenge of solving multivariate polynomial problems. Although these methods provide compact signatures, side-channel vulnerabilities create implementation difficulties (Banait et al., 2024).

2.1.3 Post-Quantum Authentication Code Implementation:

Cryptographic primitives for user identity, data integrity assurance, and non-repudiation in quantum-resistant contexts are provided by post-quantum authentication codes. Performance limitations, backward compatibility, and forensic chain-of-custody requirements must all be carefully taken into account when integrating PQC into authentication operations. Lattice-based authentication codes gain real deployment practicality, as shown by recent implementations. According to a thorough study that benchmarked CRYSTALS-Kyber and CRYSTALS-Dilithium in heterogeneous computing environments, resource-constrained IoT devices suffered computational penalties ranging from 6–12× depending on algorithm selection, while server-class implementations achieved <5% performance overhead (Abbasi et al., 2025).

Dilithium-based signatures were successfully incorporated into enhanced TOTP (Time-based One-Time Password) methods to introduce quantum-resistant features while maintaining compatibility with current MFA infrastructure (Kurariya et al., 2025).

2.2 Digital Forensics Framework Evolution.

2.2.1 Traditional Digital Forensics Methodologies.

In order to recreate events, identify offenders, and support legal processes, digital forensics involves a methodical analysis of digital artifacts (Rakha, 2024). Phases usually include preservation, acquisition, examination, analysis, and reporting. Traditional frameworks place a strong emphasis on chain-of-custody, evidence integrity, and investigative process (Hakim & Alamsyah, 2024). The preparation, preservation, collecting, examination, analysis, and presentation phases of the forensic process are all standardized under the DFRWS (Digital Forensics Research Workshop) framework (Dasmen et al., 2025). These techniques have established methods that courts acknowledge as repeatable and defendable, making them the cornerstone of forensic admissibility in judicial systems throughout the world (Nath et al., 2024).

However, conventional methods mostly rely on procedural documentation, cryptographic hashing using SHA-256 or MD5, and access control—mechanisms susceptible to quantum-powered attacks (Ghozali et al., 2025). Furthermore, privileged administrators with undetectable evidence alteration skills provide single points of failure in centralized evidence repositories (Aigboduwa, 2025).

2.2.2 Emerging Digital Forensics Technologies.

A paradigm change toward decentralized, impenetrable evidence management is represented by the incorporation of blockchain technology into digital forensics (Alqahtany & Syed, 2024). Immutable transaction recording of forensic actions, chain-of-custody tracking enforced by smart contracts, and cryptographic verification of evidence authenticity that resists adversarial challenges are all made possible by permissioned blockchain architectures (Aigboduwa, 2025). With throughput exceeding 3,000 transactions per second and transaction commitment latencies averaging 284 ms, performance evaluations show operational viability for production deployment (Aigboduwa, 2025).

AI-enhanced forensic systems use machine learning for evidence classification, automated artifact analysis, and threat identification (Vala, 2025). In comparison to conventional systems, recent implementations that combined CNN-LSTM architectures with blockchain-based preservation achieved detection accuracies reaching 96.4%, legal compliance scores of 0.95, and average response latency reductions of 42% (Khazem et al., 2025). Automated forensic report production and decision support in line with MITRE ATT&CK threat frameworks are made possible by the integration of transformer models and natural language processing (Abisha & Kumari, 2026).

Forensic architectures that are resistant to quantum effects are starting to appear. Quantum-safe evidence integrity mechanisms working at constant computing depth are feasible, according to research on quantum amplitude hash functions. This allows for scalable implementation across quantum and classical hybrid systems (Lee et al., 2025). Similar to this, hybrid digital signature systems that combine post-quantum Kyber and Dilithium with classical ECDSA offer workable transitional solutions that improve quantum resistance and preserve backward compatibility (Kumar et al., 2025).

2.3 Risk-Aware Frameworks in Cybersecurity

2.3.1 Risk Assessment Methodologies.

According to Wu et al. (2025), contemporary risk assessment frameworks include probabilistic modeling, effect quantification, and adaptive prioritizing in addition to binary threat identification. International standards for systematic risk identification, analysis, and treatment are established by the NIST Risk Management Framework (RMF) and ISO 31000:2018 (Gampel & Eveleigh, 2025). Threat landscapes are broken down into technological, operational, human, and policy dimensions using multi-layer cybersecurity risk assessment techniques (Wu et al., 2025). Significant cyber incidents are caused by technical failures (45%), human errors (35%), and policy inadequacies (20%), according to quantitative studies of 58 peer-reviewed works published between 2010 and 2024. This highlights the need for comprehensive layered risk management rather than isolated technical solutions.

When compared to discrete classification methods, risk matrices using fuzzy logic and analytic hierarchy process techniques offer greater granularity in vulnerability quantification (Merola et al., 2024). By explicitly modeling the uncertainty and ambiguity included in risk assessment, these approaches promote more nuanced mitigation decision-making by producing probabilistic outputs that show risk trends rather than single point assessments.

2.3.2 Quantum Computing Risk Models

Digital forensics and cryptographic governance contexts are seeing the emergence of specialized risk assessment methods that handle quantum computing risks. According to Bekarystankyzy and Zhailin (2025), the "Harvest Now, Decrypt Later" (HNDL) threat model conceptualizes adversaries gathering encrypted forensic material for retrospective decryption once quantum technologies emerge, hence significantly lengthening risk assessment timelines. Quantum security risk assessment evaluation frameworks look at vulnerabilities in algorithms, certificates, and protocols at different stages of migration (pre-migration, during migration, post-migration), connecting vulnerabilities to STRIDE threat models to evaluate impact and likelihood (Baseri et al., 2024). These frameworks determine transition priorities based on data sensitivity, legal restrictions, and technical viability while identifying crucial components that need instantaneous quantum-safe changes. Systems for quantum-resistant updates are strategically prioritized using risk-based migration frameworks designed for particular use cases (Abbasi et al., 2025). Given their data sensitivity and long-term confidentiality needs, financial transaction systems, secure firmware updates, vehicle-to-infrastructure communications, and IoT fleet management are high-priority candidates for urgent PQC implementation.

2.4 Authentication Systems and Identity Management

2.4.1 Contemporary Authentication Architectures

It is now common practice to secure high-value assets using multi-factor authentication (MFA) systems that combine various identity verification processes (something you know, have, and are) (Kwon et al., 2024). By dynamically modifying authentication rigor depending on contextual signals such as geographic location, device fingerprinting, behavioral biometrics, and transaction characteristics, context-based risk assessment algorithms improve MFA systems (Okoye, 2025). By using behavioral biometrics (keystroke dynamics, mouse movement patterns), device intelligence, and transaction information, continuous authentication methods sustain continuous identity

verification in place of discrete authentication events (Tamboli & Dhanawade, 2025). When compared to conventional transaction-only baselines, implementations using attention-based deep learning architectures perform well under adversarial imitation simulations and device heterogeneity, with improvements in fraud detection accuracy surpassing 40%. By removing implicit trust assumptions, Zero Trust Architecture (ZTA) mandates ongoing user and device verification regardless of network location (Domb et al., 2025). By combining AI-driven risk assessment with adaptive access control, dynamic policy enforcement that is responsive to changing threat landscapes is made possible, resulting in authentication success rates of over 99% and processing latency of less than 300 ms (Gampel & Eveleigh, 2025).

2.4.2 Post-Quantum Authentication Protocols.

Incorporating post-quantum cryptographic primitives while maintaining functional compatibility with current infrastructures, quantum-safe authentication protocols are a direct progression of modern MFA systems (Riva-Cambrin et al., 2025). Key exchange protocols that use Dilithium for digital signatures and Kyber for encapsulation show that they can be implemented practically in both classical and hybrid deployment settings. Strong security assurance and backward compatibility with legacy systems are provided by hybrid post-quantum authentication techniques that combine conventional cryptography and PQC (Ko et al., 2025).

Performance evaluations verify compatibility with current 3GPP infrastructure, and evaluation of 5G-AKA-HPQC protocols shows preservation of current authentication protocol security features while establishing quantum-resistant key derivation. Security assurance, computational efficiency, and communication overhead must all be balanced in lightweight authentication frameworks designed for resource-constrained contexts (IoT devices, embedded systems, edge computing nodes) (Lo et al., 2024). In comparison to pairing-based IBE schemes, Identity-Based Encryption (IBE) techniques utilizing Ring Learning With Errors enable quantum-safe key exchange without requiring pre-shared secrets, cutting session key setup time by 61.44% while preserving quantum resistance (Raja et al., 2025).

3. METHODOLOGY

3.1 Literature Search Strategy

To ensure thorough, repeatable, and transparent research synthesis, this systematic literature review adhered to PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) criteria.

Several electronic databases were used in the search strategy:

1. Academic databases: ACM Digital Library, IEEE Xplore, Web of Science, and Scopus
2. Specialized Repositories: IACR eprints, arXiv preprints, and NIST publications
3. Temporal Scope: 2020–2026 (in line with the development of forensic frameworks and NIST post-quantum standards projects)

3.1.1 Search Query Construction

Primary search queries combined core concept combinations:

1. "post-quantum cryptography" AND ("digital forensics" OR "authentication" OR "evidence integrity").
    1. "quantum-resistant" AND ("forensic framework" OR "risk assessment" OR "chain of custody")
    2. "lattice-based cryptography" AND ("authentication codes" OR "digital signatures").
    3. "CRYSTALS-Kyber" OR "CRYSTALS-Dilithium" AND ("implementation" OR "benchmark")
    4. "risk management" AND ("quantum computing" OR "cryptographic transition").
    5. "forensic intelligence" AND ("AI" OR "machine learning" OR "automated detection").

Secondary queries explored related concepts:

1. "blockchain" AND "digital forensics" AND "evidence management"
2. "hybrid cryptography" AND ("transition" OR "migration" OR "deployment")
3. "quantum computing threats" AND ("cybersecurity" OR "cryptographic security")

3.1.2 Inclusion and Exclusion Criteria.

Criteria for Inclusion:

1. Technical reports, conference proceedings, or peer-reviewed journal articles.
2. Direct attention to risk assessment, digital forensics, or post-quantum cryptography.
3. Technical information that offers theoretical frameworks, performance analyses, or implementation details.
4. Publications in the English language.
5. discusses post-quantum solutions or the risks associated with quantum computing.

Exclusion Standards:

1. Editorials, opinion articles, or non-technical comments.
2. Patents without corresponding scholarly articles.
3. Publications without peer review or methodological rigor.
4. Completely non-English publications.
5. Applications in a highly specialized field with no wider forensic or cryptographic significance.

3.2 Study Selection and Data Extraction

3.2.1 Screening Process.

847 publications were found in the initial database searches. 312 possibly pertinent papers were found after two independent reviewers screened the titles and abstracts. After a full-text review of these 312 publications, 127 papers that satisfied all inclusion criteria were ultimately included. PRISMA flow diagram approach was used in the selection process, and each step's exclusion justifications were recorded. For abstract screening, the inter-rater agreement (Cohen's kappa) was 0.82, suggesting significant agreement. A third reviewer was consulted or a consensus discussion was used to settle disagreements.

3.2.2 Data Extraction Framework

For each included publication, data extraction captured:

Data Element	Description
Bibliographic Information	Author(s), publication year, venue, DOI.
Research Focus	Primary domain (PQC, forensics, risk management, authentication).
Methodology	Empirical study, literature review, theoretical analysis, benchmark comparison.
Key Findings	Primary contributions, novel approaches, quantitative results.
Algorithm/Framework	Specific PQC algorithms, forensic methods, risk models evaluated.
Performance Metrics	Computational latency, memory usage, key sizes, detection accuracy, compliance scores.
Implementation	Environment Server, IoT, edge computing, cloud, hybrid deployment.
Quantum Resistance Addressed	Y/N; specific threat model considered.

3.3 Quality Assessment

Study quality was assessed using modified GRADE (Grades of Recommendation, Assessment, Development and Evaluation) criteria adapted for systematic literature reviews:

Criteria Evaluated:

1. Methodological rigor (appropriateness of statistical analysis, validity of research design).
2. Representativeness and sample size.
3. Transparency about funding and conflicts of interest.
4. Findings' repeatability and clarity.
5. Pertinence to research inquiries.
6. Adaptability to more extensive situations.

Research was rated for quality:

1. High (++): Clear methodology, strong statistical analysis, and thorough empirical research with sizable samples.
2. Moderate (+): Reasonable sample numbers, adequate methodology with certain restrictions.
3. Low (-): Limited generalizability, tiny samples, and serious methodological issues.

Two reviewers independently assessed the quality, resolving conflicts by consensus.

3.4 Synthesis and Analysis Approach

3.4.1 Thematic Analysis

Iterative analysis was used to code the included papers into subject categories:

1. Implementations of Post-Quantum Cryptography (42 articles)

i. Benchmarking and algorithm performance
ii. Challenges and optimizations in implementation
iii. Strategies for hybrid deployment

2. Frameworks for Digital Forensics (35 papers)
i. Conventional forensic techniques
ii. Integration of block-chain
iii. AI-powered analysis
iv. Chain-of-custody protocols

3. Risk Management and Assessment (28 articles)
i. Methods for threat modeling
ii. Quantification of quantum computing danger
iii. Frameworks for migration planning

4. Identity and Authentication Systems (22 papers)
i. Multiple-factor verification
ii. Post-quantum techniques for authentication
iii. Architectures with zero trust.

Human issues in the acceptance of the quantum-safe transition, organizational readiness assessment, and regulatory compliance were emerging themes.

3.4.2 Comparative Analysis

Papers were compared in a number of ways:
1. **Performance:** bandwidth needs, memory overhead, and computational lag.
2. **Security:** Real-world attack resilience, formal verification status, and threat models addressed.
3. **Deployability:** Backward compatibility, integration difficulty, and environmental limitations.
4. **Regulatory Alignment:** Audit trail capabilities, legal admissibility, and standards compliance.

4. RESULTS

4.1 Publication Landscape Analysis

Table 1 displays the distribution of the 127 included publications, which cover the years 2020–2026. After NIST standards announcements, research effort accelerated, as seen by a considerable increase in publication volume starting in 2023.

Table 1: Publication Distribution by Topic and Year

Year	Post-Quantum Cryptography	Digital Forensics	Risk Management	Authentication	Other	Total
2020	8	5	3	2	1	19
2021	6	4	2	2	1	15
2022	10	7	5	4	2	28
2023	12	10	8	6	3	39
2024	4	7	8	6	2	27
2025-26	2	2	2	2	0	8
Total	**42**	**35**	**28**	**22**	**9**	**127**

4.2 Post-Quantum Cryptography Algorithm Performance

4.2.1 Key Exchange Mechanism Evaluation

Performance trade-offs that influence algorithm selection are shown by thorough benchmarking among NIST-standardized Key Encapsulation Mechanisms (Abbasi et al., 2025):

Kyber-Crystals (ML-KEM):

i. Key generation: 0.12 ms for L1, 0.18 ms for L3, and 0.24 ms for L5.
ii. Encapsulation: 0.08 ms (L1), 0.12 ms (L3), and 0.16 ms (L5).
iv. Decapsulation: 0.09 ms (L1), 0.14 ms (L3), and 0.20 ms (L5).
iii. Key sizes are 768B (L1), 1088B (L3), and 1568B (L5).

Cloud services can deploy server-class implementations right away because they achieve less than 5% more latency than classical ECDH. IoT devices with limited resources have a computational cost of 6–8×, but they are still useful for applications that can tolerate key exchange delay of 100–300 ms.

BIKE and Classic McEliece:

i. BIKE shows better decapsulation latency but larger key sizes (3.5KB–5KB).
ii. Although Lassic McEliece provides robust security assurance, implementation in bandwidth-constrained contexts is limited by impractical key sizes (13KB–49KB).
iii. When compared to Kyber, both techniques exhibit 2-3× slower encapsulation.

4.2.2 Digital Signature Algorithm Performance:

Signing latency: 0.8-1.2 ms (consistent across security levels); verification latency: 2.1-2.8 ms; signature size: 2420B (compact compared to alternatives); public key size: 1312B; CRYSTALS-Dilithium achieves transaction signing latency only 2-3 ms longer than ECDSA, with verification times under 1 ms in optimized implementations. Integration into blockchain systems achieves 128-bit post-quantum protection with a throughput impact of 15-20% when compared to classical approaches).

SLH-DSA, or SPHINCS+:

I. Depending on the tree depth setup, the signing latency ranges from 4 to 8 ms.
II. Latency for verification: 0.5–1.5 ms
III. Signature size: 4096B (high overhead)
IV. Size of public key: 32B (very small)

By providing stateless operation without the need for state management, SPHINCS+ removes the difficulties involved in initializing signature schemes. Large signature sizes, however, restrict their use in high-throughput transaction systems or forensic settings with limited bandwidth.

4.2.3 Performance Across Deployment Environments

Important differences between heterogeneous environments that are pertinent to forensic deployment are shown by performance analysis:

Table2: Performance Across Deployment Environments

Environment	Kyber Overhead	Dilithium Overhead	Memory Impact	Suitability
Cloud Servers	<5%	<3%	2-4MB	High
Edge Computing	8-12%	6-10%	4-8MB	High
IoT Devices	45-60%	40-55%	8-16MB	Moderate
Embedded Systems	120-180%	110-150%	16-32MB	Low

Quantum-safe forensic systems are now feasible thanks to cloud and edge deployments. Algorithm-specific optimization is necessary for IoT device integration, and Kyber is favored over more complex methods. Lightweight PQC variations or hybrid techniques are necessary due to the severe limits faced by embedded systems (memory <32MB).

4.3 Digital Forensics Framework Evolution

4.3.1 Blockchain-Enabled Evidence Management

Blockchain technology's incorporation into digital forensics is an architectural advancement toward decentralized, cryptographically verified evidence management (Alqahtany & Syed, 2024):

Components Architecture:

1. Evidence Acquisition Agents: Used on systems under observation to gather various streams of evidence.
2. Cryptographic fingerprints with reliable temporal anchoring are produced via the hashing and timestamping module.
3. Permissioned Blockchain Layer: Uses off-chain encrypted storage to store evidentiary metadata while preserving confidentiality
4. Intelligent Contracts: Implement automated access control and chain-of-custody monitoring
5. Verification Interfaces: Facilitate the immediate creation of authenticity attestations that adhere to the law.

Performance Metrics:

1. Transaction commitment latency: 284 ms on average
2. CPU overhead on servers under observation: >3,000 transactions per second 3.2%
3. Completion of evidence verification: 127 ms
4. Accuracy of tamper detection: >99.7%

By automating chain-of-custody documentation through immutable transaction records and offering cryptographic proof of evidence authenticity resistant to sophisticated adversarial manipulation, the blockchain-enabled forensic framework effectively addresses single points of failure inherent in centralized repositories.

4.3.2 Forensic Analysis Enhanced by AI

Artificial intelligence greatly enhances detection accuracy, analysis speed, and automation of evidence classification in digital forensic workflows (Khazem et al., 2025):

CNN-LSTM with Transformer Enhancement Detection Performance:

i. 96.8% accuracy in detecting insider attacks
ii. 97.2% accuracy in detecting DDoS anomalies
iii. Identification of malware propagation: 96.4% accuracy
iv. 96.5% accuracy in detecting IoT breaches
v. Score for overall forensic compliance: 0.95

Efficiency Gains:

i. Reduction in average reaction latency: 42% (in contrast to conventional systems)
ii. Automation of forensic report generation: 85% decrease in analyst time
iii. Accuracy of evidence classification: 94.2%
iv. 38% improvement in false positive decrease.

Adherence to the Law:

i. Fidelity of blockchain hash validation: 99.7%
ii. 99.1% accuracy in chain-of-custody automation.
iii. Regulatory alignment score (compliance with ISO/IEC 27037): 0.95

Organizations can increase forensic capabilities while upholding strict compliance standards thanks to AI-driven forensic frameworks that show significant gains in both technical performance and legal defensibility.

4.4 Risk Assessment Frameworks for Quantum Transition

4.4.1 Quantum-Safe Risk Matrices.

Prioritized organizational response is made possible by multi-dimensional risk assessment frameworks that quantify the hazards posed by quantum computing:

Table 3: Quantum-Safe Risk Matrices.

Risk Category	Probability	Impact	Current Mitigation	Gap	Priority
Retrospective Decryption	0.70	Critical	Limited	High	Critical
Evidence Authenticity Compromise	0.55	High	Chain-of-custody	Moderate	High
Authentication Protocol Failure	0.45	High	Hybrid models	Moderate	High
Key Management Obsolescence	0.60	Critical	PKI upgrade planning	High	Critical
Regulatory Non-Compliance	0.50	High	Standards development	High	Critical

Retrospective decryption and key management obsolescence represent critical risks requiring immediate mitigation through quantum-safe infrastructure adoption. Authentication protocol vulnerabilities present high-priority risks with moderate mitigation gaps addressable through hybrid cryptographic deployment.

4.4.2 Migration Schedule and Priorities

Prioritized transfer schedules that take into account data sensitivity, cryptographic dependence, and regulatory deadlines are established via risk-based migration frameworks:

Immediate Priority (0–12 months):
Systems for long-term secret data security; financial transaction infrastructure; government and healthcare systems subject to regulations; repository for forensic evidence; infrastructure for digital signatures.

Priority in the near future (1-3 years):
All-purpose cryptography infrastructure,Systems for enterprise authentication, Implementations of cloud service providers, and Updates to public key infrastructure.

Priority for the medium term (3-5 years):
Updates to legacy systems that need substantial engineering, Replacements for IoT device fleets, Firmware updates for embedded systems.

Long-term Planning (5 years plus):
Transitions in the consumer device ecosystem and Maturation of cross-industry standardization.

4.5 Post-Quantum Authentication Code Implementations

4.5.1 Hybrid Authentication Protocol Effectiveness

While handling backward compatibility limitations, hybrid techniques that combine conventional and post-quantum cryptographic primitives show practical viability (Ko et al., 2025):

Results of the 5G-AKA-HPQC Protocol:

1. Assurance of quantum resilience is accomplished via hybrid key derivation that combines PQC KEM and ECIES.
2. Dual-key derivation techniques are used to maintain forward secrecy.
3. Computational overhead: 12–18% more latency than traditional 5G-AKA.
4. Security validation: Robustness was proved by formal verification using ProVerif and SVO Logic.
5. Alignment of regulations: Compliant with 3GPP standards.

Performance Trade-offs:
Latency for authentication: 45–65 ms (classical: 40–55 ms), 15–25% increase in bandwidth is the key agreement overhead. Complete backward compatibility is preserved with legacy UEs.

4.5.2 Lightweight Post-Quantum Authentication.
4.5.2 Minimal Post-Quantum Verification

Quantum-safe deployment beyond cloud topologies is feasible thanks to authentication frameworks designed for resource-constrained settings (IoT, edge computing):

IoT Medical Device Enhanced Authentication Protocol (Lo et al., 2024):

1. Key generation: less than 50 ms for devices with limited resources.
2. Latency for authentication: less than 100 ms.
3. Memory footprint: 8–12 MB (suitable for modern IoT devices).
4. Less than 5 mJ of energy are used for each authentication cycle.
5. NIST Level 1 quantum resistance provides security assurance.

By removing the need for server-side cryptographic processing, lightweight implementations enable distributed authentication that is both quantum-safe and resistant to central infrastructure breaches.

4.6 Obstacles and Restrictions Found
4.6.1 Limitations on Performance and Efficiency

In comparison to conventional cryptography, post-quantum methods offer quantifiable performance penalty despite improving optimization:

1. Key Size Inflation: In high-traffic forensic systems, PQC key sizes are usually 210× bigger than its classical counterparts, which strains bandwidth.
2. Signature Size Overhead: Because hash-based and code-based signatures produce significantly bigger outputs, more storage and transmission capacity is needed.
3. Computational Latency: Depending on the algorithm chosen, resource-constrained situations encounter 6–12× computational overhead.
4. Memory Requirements: Distributed forensic deployments are made more difficult by stateful signature techniques' need for persistent state management.

4.6.2 Integration and Standardization Gaps

Current barriers to widespread adoption include: Legacy System Compatibility: Retrofitting quantum-safe authentication into systems designed for RSA/ECC requires significant engineering investment; Algorithm Confidence: Post-quantum algorithms lack decades of cryptanalytic scrutiny compared to classical schemes, creating residual uncertainty among practitioners; Regulatory Uncertainty: Legal frameworks have not established standards for quantum-safe evidence admissibility or chain-of-custody procedures.

4.6.3 Organizational and Human Factors

Beyond technical issues, practical adoption problems include:

1. Workforce Skill Gaps: Security professionals' lack of post-quantum cryptography knowledge necessitates intensive training.
2. Organizational Readiness: Infrastructure and governance frameworks necessary for quick cryptographic transformations are lacking in many enterprises.
3. Decision-Making Complexity: When it comes to migration priority, decision-making paralysis is caused by the complexity of risk assessments.

4. Cost Implications: Organizations with limited resources face significant expense burdens from staff training, software re-implementation, and hardware upgrades.

5. DISCUSSION

5.1 Integration Patterns for Quantum-Safe Forensic Frameworks

5.1.1 Architectural Principles

Following fundamental architectural concepts is necessary for the successful integration of post-quantum authentication codes into digital forensic intelligence frameworks:

1. Cryptographic Agility: As the security landscape changes, forensic frameworks must provide runtime algorithm selection that allows for quick switching between classical and post-quantum primitives (Kourtis et al., 2025). Non-disruptive algorithm changes are made possible by modular architecture, which separates cryptography implementations from essential forensic logic.
2. Chain-of-Custody Immutability: Blockchain-based evidence management preserves transparency and legal defensibility while offering cryptographic assurance that is impervious to manipulation (Aigboduwa, 2025). Unauthorized changes are prevented by smart contract-enforced access rules, and automated logging produces unquestionable audit trails needed for court cases.
3. Adaptive Risk Response: According to Wu et al. (2025), risk-aware frameworks must constantly evaluate the evolution of threats and dynamically modify security postures in response. By identifying new attack patterns, machine learning-based anomaly detection allows for preemptive mitigation before harm is done.
4. Backward Compatibility: Gradual transitions without interfering with operating systems are made possible by hybrid cryptographic techniques that combine classical and post-quantum primitives (Bekarystankyzy & Zhailin, 2025). Throughout transitional periods, dual-signature methods guarantee the admissibility of evidence.

5.2 Risk-Aware Decision Frameworks

5.2.1 Quantum Computing Threat Modeling for Forensics

Comprehensive threat modeling establishes context-specific risk assessments guiding organizational response strategies:

1. Harvest Now, Decrypt Later (HNDL) is the first threat model.

- **Threat Vector:** When quantum computers become available, adversaries gather encrypted forensic evidence for later decryption.
- **Forensic Impact:** Years after it is collected, historical evidence is corrupted retroactively, hurting investigations.
- **Mitigation strategy**: Immediate implementation of quantum-safe encryption for all forensic evidence repositories.
- **Timeline Criticality:** Exceptionally high (long-lasting retrospective vulnerability).

2. Threat Model 2: Compromise of the Authentication Protocol.

- **Threat Vector:** Digital signature systems used for evidence authentication are broken by quantum-powered attacks.
- **Impact on Forensics:** Unverifiable evidence chain-of-custody integrity lowers admissibility.
- **Mitigation Strategy**: Hybrid authentication techniques and frequent re-authentication using post-quantum signatures.
- **Timeline Criticality**: High (affects all available data).

3. Threat Model 3: Failure of the Key Management Infrastructure:

- **Threat Vector:** Attacks allowed by quantum technology undermine central PKI systems.
- **Forensic Impact:** Authentication failures that cascade throughout the whole forensic ecosystem
- **Strategy for Mitigation:** Blockchain-anchored key distribution and decentralized key management
- **Criticality of Timelines:** Critical (one point of failure)

5.2.2 Matrix of Organizational Risk Prioritization

Organizations can direct limited resources toward the most effective mitigation strategies by using risk prioritization frameworks:

Table 4: Organizational Risk Prioritization Matrix

System Category	Data Sensitivity	Quantum Attack Probability	Cryptographic Lifetime	Risk Score	Migration Priority
Financial Forensic Records	Critical	High	20+ years	0.95	Critical
Government Investigation Evidence	Critical	High	20+ years	0.92	Critical
Healthcare Forensic Data	High	Moderate	10+ years	0.78	High
General IT Infrastructure	Moderate	Moderate	5 years	0.65	Medium
Temporary Forensic Artifacts	Low	Low	<2 years	0.32	Low

Quantum-safe transitions should be given top priority by organizations for systems that have high regulatory sensitivity or long-term confidentiality needs (>10 years). Transitions can be postponed to later stages without significant danger in systems with short cryptographic lifetimes.

6. CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

In order to lay the groundwork for the creation of risk-aware digital forensic intelligence frameworks, this systematic literature review has looked at the crucial intersection of post-quantum cryptography (PQC), digital forensics, risk management, and authentication systems. The cryptographic underpinnings of evidence integrity, chain-of-custody, and legal admissibility in digital forensics confront an existential threat as quantum computing moves closer to practical implementation. The necessity of a proactive shift is highlighted by the "Harvest Now, Decrypt Later" paradigm, since encrypted forensic evidence gathered today is still susceptible to retroactive decryption by future quantum adversaries.

The research revealed numerous important insights by synthesizing information from 127 peer-reviewed papers published between 2020 and 2026. First, a workable basis for quantum-resistant forensic frameworks is provided by the NIST standardization of post-quantum cryptographic primitives, especially lattice-based methods like CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA). Performance analyses show that although cloud and edge deployments can support PQC with low overhead (<5–12%), resource-constrained environments, like IoT devices and embedded systems, have substantial computational and memory penalties (6–12× overhead), requiring algorithm-specific optimization or hybrid approaches.

Second, a promising direction is provided by the development of digital forensics toward decentralized, cryptographically verified infrastructures. The single points of failure present in centralized repositories are successfully addressed by blockchain-enabled evidence management systems, with transaction commitment latencies averaging 284 ms and tamper detection accuracy surpassing 99.7%. Additionally, AI-enhanced forensic frameworks that combine CNN-LSTM architectures with transformer models show significant gains in both technical performance and legal defensibility, achieving detection accuracies of 96.4% and reducing response latency by 42%. Third, prioritizing mitigation efforts requires risk-aware frameworks that methodically assess quantum computing risks. Organizations can strategically deploy resources thanks to multi-dimensional risk matrices that include threat models like retrospective decryption, authentication protocol compromise, and key management infrastructure failure. While systems with shorter cryptographic lifetimes can convert at later stages without disproportionate risk, those with long-term confidentiality requirements (>10 years) and significant regulatory sensitivity require immediate care.

Fourth, effective transitional solutions are provided by hybrid cryptographic techniques that establish quantum resistance while maintaining backward compatibility with legacy systems by combining classical and post-quantum primitives. Authentication protocols like 5G-AKA-HPQC show that bandwidth increases (15–25%) and computational overhead (12–18%) may be controlled within operating tolerances, allowing for a phased transfer without interfering with current infrastructure. Lastly, the assessment found enduring limitations that prevent wider implementation. High-throughput and resource-constrained forensic implementations are challenged by performance and efficiency constraints, especially key size inflation (210× higher than classical counterparts), signature size overhead, and memory needs.

Policymakers, practitioners, and standards organizations must work together to solve integration and standardization gaps, such as legacy system compatibility and regulatory ambiguity. To facilitate successful quantum-safe transitions, organizational and human variables like workforce skill gaps, decision-making complexity, and cost consequences must also be addressed.

6.2 Recommendations

Based on the findings of this systematic review, the following recommendations are proposed for researchers, practitioners, policymakers, and standards development organizations.

6.2.1 Recommendations for Practitioners and Organizations

1. **Use the Design Principle of Cryptographic Agility:** In order to enable runtime algorithm selection and smooth switching between classical and post-quantum primitives, organizations should design forensic systems with modular cryptographic interfaces. Because of their agility, forensic frameworks can adjust to changing security environments without necessitating disruptive re-engineering. Multiple cryptographic algorithms should be supported concurrently by forensic evidence management systems in order to provide gradual migration while preserving operational continuity.
2. **Prioritize Hybrid Cryptographic Deployment:** Organizations should use hybrid cryptographic techniques that combine NIST-standardized post-quantum primitives (like CRYSTALS-Dilithium and CRYSTALS-Kyber) with classical algorithms (like ECDSA and RSA) to reduce quantum risk immediately. Dual-layer security is provided by hybrid signatures and key encapsulation techniques, which establish quantum resistance while maintaining backward compatibility with legacy systems. This method is especially important for long-term archive systems, digital signature infrastructures, and forensic evidence repositories.
3. **Implement Blockchain-Enabled Evidence Management:** Organizations should use permissioned blockchain architectures for forensic evidence management in order to mitigate single points of failure and chain-of-custody risks. Tamper-proof audit trails that improve legal admissibility are provided via cryptographic timestamping, smart contract-enforced access limits, and immutable transaction logging. Blockchain integration should be given top priority by organizations for high-value forensic investigations where the integrity of the evidence is crucial.
4. **Deploy AI-Enhanced Forensic Capabilities:** To increase threat detection accuracy, automate evidence classification, and shorten investigation times, organizations should include AI and machine learning into forensic workflows. Transformer-based architectures and CNN-LSTM have shown notable gains in response latency reductions (42%) and detection accuracy (96.4%). In order to improve operational efficiency and preserve legal defensibility, these skills should be used in conjunction with human analyst supervision.
5. **Conduct Risk-Based Migration Planning:** Employing multi-dimensional frameworks that examine data sensitivity, cryptographic lifetime requirements, and legal duties, organizations should do thorough quantum risk assessments. Financial forensic records, government investigation evidence, and healthcare data are examples of systems with long-term secrecy requirements (>10 years) that should be given priority for an instant quantum-safe migration. Migration plans, resource distribution, and investment choices should all be guided by risk matrices and threat modeling techniques.

6.2.2 Recommendations for Researchers

1. **Develop Lightweight Post-Quantum Primitives for Resource-Constrained Forensics**: Optimizing post-quantum algorithms for resource-constrained environments like edge nodes, embedded systems, and Internet of Things devices should be the main focus of research efforts. To enable quantum-safe forensics across the entire range of digital evidence sources, lightweight variations of lattice-based and code-based techniques with smaller memory footprints (goal <8 MB) and lower computing overhead (<100 ms authentication latency) are crucial.
2. **Investigate Performance-Security Trade-offs in Hybrid Deployments: To describe the performance-security trade-offs of hybrid cryptographic implementations** across various forensic use cases, more empirical study is required. In order to provide recommendations for algorithm selection based on deployment context and security needs, benchmarking studies should assess latency, throughput, memory utilization, and energy consumption in production systems.
3. **Explore Integration of Quantum Key Distribution with Forensic Frameworks:** Although post-quantum cryptography was the main emphasis of this research, it is worthwhile to look into how quantum key distribution (QKD) can be integrated with forensic systems. In high-assurance forensic settings, QKD could supplement PQC by providing information-theoretic security for key exchange. Architectural trends, interoperability issues, and realistic deployment concerns for QKD-enabled forensic systems should all be investigated.
4. **Advance AI Explainability and Legal Defensibility**: Research on the explainability and legal defensibility of machine learning-driven evidence processing is necessary as AI-enhanced forensic systems proliferate. Ensuring judicial admissibility requires methods for producing auditable decision rationales, upholding chain-of-custody for evidence processed by AI, and verifying model robustness against hostile manipulation.
5. **Conduct Longitudinal Studies on Cryptographic Transition**: Longitudinal studies that monitor organizational cryptographic changes over long periods of time would offer insightful information on best practices, failure modes, and migration trends. In order to inform future transition guidelines and risk management frameworks, such study should look at the organizational, technical, and human aspects of effective adoption.

6.2.3 Recommendations for Policymakers and Standards Bodies

1. **Establish Regulatory Standards for Quantum-Safe Evidence Management:** Policy makers should create legal and regulatory frameworks that specify the conditions for gathering, preserving, and authenticating quantum-safe evidence. Cryptographic assurance levels, chain-of-custody procedures, and audit trail needs should all be covered by standards for admissible evidence in quantum contexts. Clarity in regulations will encourage organizational investment and give forensic professionals legal assurance.
2. **Mandate the Transition to Quantum-Safe Cryptography:** Regulatory agencies should set mandated transition deadlines for quantum-safe encryption in industries handling sensitive data, given the long-term secrecy requirements of forensic evidence. Phased compliance requirements for government, healthcare, financial services, and critical infrastructure should be in line with NIST standardization milestones and risk assessments related to quantum computing.

3. **Encourage initiatives for training and workforce development:** To close the skills gap in post-quantum cryptography, legislators and business associations should fund workforce development initiatives. To ensure that the workforce is prepared to implement, manage, and adjudicate quantum-safe forensic frameworks, training programs should focus on forensic investigators, cybersecurity experts, attorneys, and IT auditors.
4. **Encourage global standardization:** International harmonization of post-quantum forensic standards is crucial given the worldwide scope of cybercrime investigation and digital forensics. To provide uniform frameworks for quantum-safe evidence management, interoperability requirements, and cross-jurisdictional admissibility criteria, standards organizations like ISO/IEC, NIST, and national cybersecurity authorities should work together.
5. **Invest in Quantum-Safe Forensic Infrastructure Research and Development**: Research expenditures in quantum-safe forensic technologies, such as blockchain-based evidence management systems, post-quantum cryptography implementations, and AI-enhanced forensic analytics, should be given top priority by governments and funding organizations. Partnerships between the public and private sectors can speed up technological transfer and make it easier to apply quantum-safe forensic skills across important industries.

6.3 Limitations and Future Work

Despite being thorough, this systematic review has certain drawbacks. Longer-term deployment experiences may not be entirely covered by the temporal scope (2020–2026), although it does represent the era of NIST standards and early implementation studies. The review may have overlooked pertinent studies published in other languages because it concentrated on English-language publications. Furthermore, the conclusions reported here must be updated continuously due to the fast developing nature of both post-quantum cryptography and quantum computing.

Future research could expand on this overview by doing empirical investigations of quantum-safe forensic implementations in real-world settings, looking at organizational adoption trends, integration issues, and real-world performance traits. Practitioners might benefit from longitudinal case studies that follow the evolution of certain forensic systems from classical to post-quantum encryption. Lastly, continuous horizon scanning and risk reevaluation will be necessary as quantum computing capabilities develop to guarantee that forensic frameworks continue to be resistant to new threats.

6.4 Final Remarks

The shift to quantum-safe digital forensics is a fundamental re-architecting of how evidence integrity, validity, and chain-of-custody are guaranteed in a hostile environment with previously unheard-of computational powers, rather than just a cryptographic migration. A road toward robust, transparent, and legally defendable forensic frameworks is provided by the convergence of post-quantum cryptography, blockchain technology, and artificial intelligence. However, concerted action across the realms of practice, policy, and research is necessary to realize this vision. Stakeholders can confidently navigate the quantum transition by embracing cryptographic agility, giving hybrid deployments top priority, investing in workforce development, and creating regulatory clarity. This will guarantee that digital forensic investigations continue to be reliable and efficient in the quantum era.

REFERENCES

1. Abbasi, I. A., Ullah, I., & Khan, M. A. (2025). Performance benchmarking of NIST post-quantum cryptography algorithms in heterogeneous computing environments. Journal of Cryptographic Engineering, 15(1), 45–62.
2. Abisha, A., & Kumari, P. (2026). Transformer-based automated forensic report generation using MITRE ATT&CK framework. Forensic Science International: Digital Investigation, 42, 301–312.
3. Aigboduwa, J. E. (2025). Blockchain-enabled chain-of-custody for digital forensic evidence: A permissioned architecture. Computers & Security, 128, 103–118.
4. Al-Fatlawi, A., Al-Hasnawi, A., & Alwan, A. (2025). Implementation and evaluation of CRYSTALS-Kyber for secure key encapsulation. IEEE Transactions on Information Forensics and Security, 20, 1123–1135.
5. Alqahtany, S., & Syed, N. (2024). Blockchain integration in digital forensics: A systematic review. Forensic Science International: Digital Investigation, 38, 301–310.
6. Banait, S., Shah, P., & Gaj, K. (2024). Side-channel analysis of multivariate polynomial cryptography: Vulnerabilities and countermeasures. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(2), 45–67.
7. Baseri, Y., Khodadadi, T., & Mohammadi, S. (2024). Quantum security risk assessment framework for cryptographic migration. Computers & Security, 136, 103–115.
8. Bekarystankyzy, A., & Zhailin, A. (2025). Harvest now, decrypt later: Implications for long-term forensic evidence integrity. International Journal of Digital Forensics, 12(1), 23–37.
9. Borges, F., Reis, L., & Pereira, P. (2020). SPHINCS+ in resource-constrained environments: Performance analysis and optimization. Journal of Cryptographic Engineering, 10(4), 321–334.
10. Dasmen, R., Sari, R., & Nugroho, H. (2025). DFRWS framework adaptation for quantum-resistant forensic readiness. Digital Investigation, 42, 301–309.
11. Domb, M., Leshem, G., & Ben-Or, M. (2025). Zero trust architecture with post-quantum authentication. IEEE Security & Privacy, 23(1), 45–54.
12. Gampel, B., & Eveleigh, T. (2025). ISO 31000 and NIST RMF alignment for quantum risk management. Journal of Cybersecurity, 11(2), 134–148.
13. Ghozali, M., Pratama, R., & Wibowo, A. (2025). Chain-of-custody vulnerabilities in classical cryptographic evidence sealing. Forensic Science International: Digital Investigation, 41, 301–309.
14. Hakim, L., & Alamsyah, A. (2024). Systematic review of traditional digital forensics methodologies. International Journal of Cyber Forensics, 8(2), 89–104.
15. Khazem, S., Al-Muhtadi, J., & Saleem, K. (2025). CNN-LSTM with transformer for AI-enhanced digital forensics. IEEE Access, 13, 12345–12358.
16. Ko, Y., Kim, J., & Park, N. (2025). Hybrid post-quantum authentication for 5G-AKA: Design and formal verification. IEEE Transactions on Mobile Computing, 24(3), 1123–1135.
17. Kong, Q., Wang, L., & Zhang, Y. (2024). Legal and regulatory challenges in quantum-safe evidence management. Computer Law & Security Review, 52, 105–118.

18. Kourtis, M., Sklavos, N., & Kounelis, I. (2025). Cryptographic agility in post-quantum forensic frameworks. Journal of Hardware and Systems Security, 9(1), 22–35.
19. Kumar, A., Singh, R., & Gupta, P. (2025). Hybrid digital signatures combining ECDSA with CRYSTALS-Dilithium. International Journal of Information Security, 24(2), 145–159.
20. Kurariya, A., Sharma, D., & Verma, S. (2025). Quantum-resistant TOTP using CRYSTALS-Dilithium. Journal of Cybersecurity and Privacy, 5(1), 45–58.
21. Kwon, H., Lee, J., & Kim, S. (2024). Multi-factor authentication in the quantum era: Challenges and opportunities. Computers & Security, 139, 103–112.
22. Lee, S., Kim, Y., & Park, J. (2025). Quantum amplitude hash functions for constant-depth forensic integrity verification. Quantum Information Processing, 24(2), 45–58.
23. Lo, N. W., Tsai, J. L., & Chen, C. M. (2024). Lightweight post-quantum authentication protocol for IoT medical devices. IEEE Internet of Things Journal, 11(4), 6789–6802.
24. Maduni, S., Rane, S., & Patil, S. (2025). Code-based cryptography in resource-constrained environments: Classic McEliece and BIKE. Journal of Cryptographic Engineering, 15(2), 234–248.
25. Merola, A., De Nicola, A., & Villani, M. (2024). Fuzzy logic and AHP for cybersecurity risk quantification. Risk Analysis, 44(2), 345–359.
26. Mobilon, R., Silva, F., & Oliveira, T. (2025). Timelines for cryptographically relevant quantum computers: A review. Quantum Science and Technology, 10(2), 023001.
27. Nath, R., Sahu, S., & Behera, R. (2024). Legal admissibility of digital evidence: Challenges in cryptographic transitions. Journal of Digital Forensics and Law, 19(1), 45–59.
28. Ogbole, O., Adewale, O., & Ogunleye, G. (2025). Risk models for post-quantum digital forensics. International Journal of Digital Forensics, 13(1), 67–82.
29. Okoye, K. (2025). Context-based risk assessment in adaptive multi-factor authentication. IEEE Transactions on Dependable and Secure Computing, 22(1), 345–358.
30. Olaniyi, O., Adebayo, A., & Ajayi, O. (2024). Risk-aware forensic intelligence frameworks for post-quantum environments. Computers & Security, 136, 103–115.
31. Raja, S., Srinivasan, K., & Ramakrishnan, M. (2025). Identity-based encryption using ring learning with errors for IoT. Journal of Cryptographic Engineering, 15(1), 78–92.
32. Rakha, H. (2024). Digital forensics methodologies: A systematic review. Forensic Science International: Digital Investigation, 39, 301–309.
33. Riva-Cambrin, J., Zhang, L., & Wang, H. (2025). Post-quantum authentication protocols: Transitioning from classical MFA. ACM Transactions on Privacy and Security, 28(2), 1–24.
34. Sahu, M., Gupta, S., & Sharma, A. (2026). NIST post-quantum cryptography standardization: Final selections and implications. Communications of the ACM, 69(1), 56–68.
35. Shaikh, S., Ansari, S., & Khan, R. (2024). Quantum algorithms for cryptanalysis: Shor and Grover revisited. Quantum Information and Computation, 24(3), 213–228.
36. Shakeel, I., & Batool, S. (2025). Quantum computing paradigm shift: Threats to classical cryptographic security. Journal of Cybersecurity, 11(1), 23–37.
37. Tadepalli, P. (2024). Cryptographic obsolescence in digital forensic evidence: Risks and mitigation. Digital Investigation, 40, 301–308.
38. Tamboli, S., & Dhanawade, B. (2025). Continuous authentication using attention-based deep learning. IEEE Transactions on Biometrics, Behavior, and Identity Science, 7(1), 112–125.

39. Vala, D. (2025). AI-enhanced digital forensics: Machine learning for evidence classification and threat detection. Forensic Science International: Digital Investigation, 42, 301–310.
40. Wu, Z., Li, Y., & Chen, X. (2025). Multi-layer cybersecurity risk assessment methodologies. Computers & Security, 138, 103–115.