International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Quantum-Safe Artificial Intelligence: A Systematic Review of Post-Quantum Cryptography Applications

Mohammed M. Al-Mhadawi[1], Qahtan M. Yas[2*]
[1] General Directorate for Education of Diyala, Ministry of Education, Diyala, Baqubah, 32001, Iraq
[2] College of Engineering for Artificial Intelligence Technology, University of Diyala, Baqubah, 32001, Iraq

ABSTRACT:
Objective: The rapid development of quantum computing poses an existential threat to classical cryptographic systems that currently secure global digital infrastructure. In direct response to this quantum threat, post-quantum cryptography (PQC) has emerged as a critical field dedicated to designing algorithms resistant to quantum attacks. Simultaneously, artificial intelligence (AI) — particularly machine learning (ML) and deep learning (DL) — has demonstrated promising and emerging capabilities across cybersecurity domains, including cryptography.
Methods: This systematic review was conducted by searching IEEE Xplore, ACM Digital Library, Springer Link, Google Scholar, Scopus, and Web of Science using targeted keywords related to AI and PQC, covering literature published between 2015 and 2025. A total of 62 peer-reviewed studies meeting predefined inclusion criteria were analysed.
Results: A total of 38 key studies were identified and analysed across four principal application domains: algorithm design and parameter optimization (31.6%), cryptanalysis and security assessment (26.3%), side-channel attack detection and defense (23.7%), and secure deployment on resource-constrained devices (18.4%). Practical case studies demonstrate measurable performance gains, including a 27% reduction in key exchange time reported in a specific study [60] and 98.3% accuracy in side-channel attack detection reported in a specific study.
Conclusions: The synergy between AI and PQC represents a pivotal frontier in cybersecurity. This review provides a structured foundation for future interdisciplinary research in quantum-safe intelligent systems and identifies explainable AI (XAI) integration as the most critical open research direction.

KEYWORDS: Artificial Intelligence (AI), Cryptanalysis, Deep Learning (DL), Post-Quantum Cryptography (PQC), Machine Learning (ML), Quantum Computing, Side-Channel Attacks.

INTRODUCTION

The emergence of quantum computing represents one of the most profound technological shifts of the modern era, introducing unprecedented computational capabilities that threaten the foundations of classical cryptography [1, 2]. Current public-key cryptographic systems, including the widely-deployed Rivest-Shamir-Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC), derive their security from the computational intractability of mathematical problems such as integer factorization and discrete logarithms [3]. However, Shor's quantum algorithm [4] fundamentally undermines these hardness assumptions by solving these problems in polynomial time, rendering the current cryptographic infrastructure vulnerable to quantum-enabled adversaries.
The global cryptographic community, led by the National Institute of Standards and Technology (NIST), has responded to this existential threat through concerted efforts to standardize quantum-resistant cryptographic algorithms [5, 6]. These post-quantum cryptographic (PQC) families include lattice-based constructions such as CRYSTALS-Kyber [7] and CRYSTALS-Dilithium [8] — both selected by NIST for standardization [5] — code-based systems derived from the McEliece cryptosystem [9], multivariate polynomial cryptography [10], and hash-based signature schemes [11]. Each family exploits distinct mathematical problems that are conjectured to remain computationally hard even for powerful quantum computers [12, 13].
In parallel, artificial intelligence (AI) has undergone remarkable advances, with machine learning (ML) and deep learning (DL) achieving breakthrough performance across diverse scientific and engineering domains [14, 15]. The application of AI to cybersecurity — encompassing threat detection, anomaly identification, and vulnerability assessment — has gained substantial momentum [16, 17]. The convergence of AI capabilities with the pressing requirements of PQC represents a fertile research frontier,

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

offering novel approaches to algorithm optimization, cryptanalytic analysis, physical attack defense, and adaptive deployment strategies [18, 19].

This systematic review aims to provide a comprehensive and structured analysis of the current state of AI applications within the PQC domain. The review is organized as follows: Section 2 describes the methodology; Section 3 presents the taxonomy and results including illustrative charts of study distributions; Section 4 discusses motivations, challenges, and recommendations; Section 5 proposes a new research direction; Section 6 addresses limitations; and Section 7 concludes the paper.

Research Contribution

This article presents a structured synthesis of current trends in combining AI and PQC. Unlike previous surveys which examined either AI-based applications of cryptography or focused on developing PQC algorithms in isolation, this review bridges the two areas across four pivotal PQC application domains [20, 21]. The contribution is timely: the threat of cryptographically-relevant quantum computers (CRQCs) is assessed as imminent within a 10–15 year horizon [22, 23], making AI-accelerated PQC standardization and deployment a pressing research imperative.

Quality Assessment

Each of the 38 core studies was evaluated for methodological quality using three criteria: study type (experimental or theoretical), reliability level (high, moderate, or low), and whether empirical results were independently reproducible. This assessment informed the weight given to individual findings in the synthesis and is summarized in Table 1 below.

Table 1. Quality Assessment of Core Studies (n=38)

Application Domain	Study Type	Reliability Level	No. of Studies
Algorithm Design & Optimization	Mixed (Exp. + Theoretical)	Moderate–High	12
Cryptanalysis & Security Assessment	Experimental	High	10
Side-Channel Attack Detection	Experimental	High	9
Resource-Constrained Deployment	Mixed (Exp. + Theoretical)	Moderate	7

METHODOLOGY

The review methodology was designed to ensure comprehensiveness, reproducibility, and scholarly rigour. The scope is limited to peer-reviewed journal articles and conference papers published in English between 2015 and 2025, focusing exclusively on the intersection of AI or ML techniques with post-quantum cryptographic systems.

Information Sources

A comprehensive search was conducted across six major academic databases: (1) IEEE Xplore [24]; (2) ACM Digital Library; (3) SpringerLink; (4) Google Scholar; (5) Scopus; and (6) Web of Science. This expanded selection — compared to earlier surveys — ensures broad coverage of both theoretical and applied research relevant to AI-driven PQC [25, 26].

Search Strategy

The search string employed the Boolean OR operator across the following terms: "post-quantum cryptography", "machine learning cryptanalysis", "AI-based optimization", "quantum-resistant encryption", "quantum-safe AI", "machine learning side-channel", "AI cryptographic design", "deep learning PQC", and "neural network lattice". This query was applied consistently across all six databases for publications from January 2015 to December 2025.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Inclusion and Exclusion Criteria

Articles were included if they: (1) are written in English and published as a peer-reviewed journal or conference paper; (2) address the application of AI or ML techniques to one or more aspects of post-quantum cryptography; and (3) were published between 2015 and 2025. Articles were excluded if they addressed classical cryptography only, presented AI applications unrelated to cryptography, or consisted of non-peer-reviewed grey literature [27].

Data Collection Process

All included papers were consolidated into a structured spreadsheet and annotated by AI technique employed, PQC application domain, performance metrics reported, and identified limitations. An initial pool of 187 candidate articles was reduced to 62 included studies (meeting all inclusion criteria) after duplicate removal and eligibility screening; of these 62 included studies, 38 core studies were selected for detailed quantitative analysis based on the richness and completeness of their reported experimental results [28]. Following PRISMA guidelines [27], the selection process proceeded through four stages: identification (187 records), screening (removal of duplicates and off-topic articles), eligibility assessment (applying inclusion/exclusion criteria), and final inclusion (62 studies for review; 38 for detailed analysis).

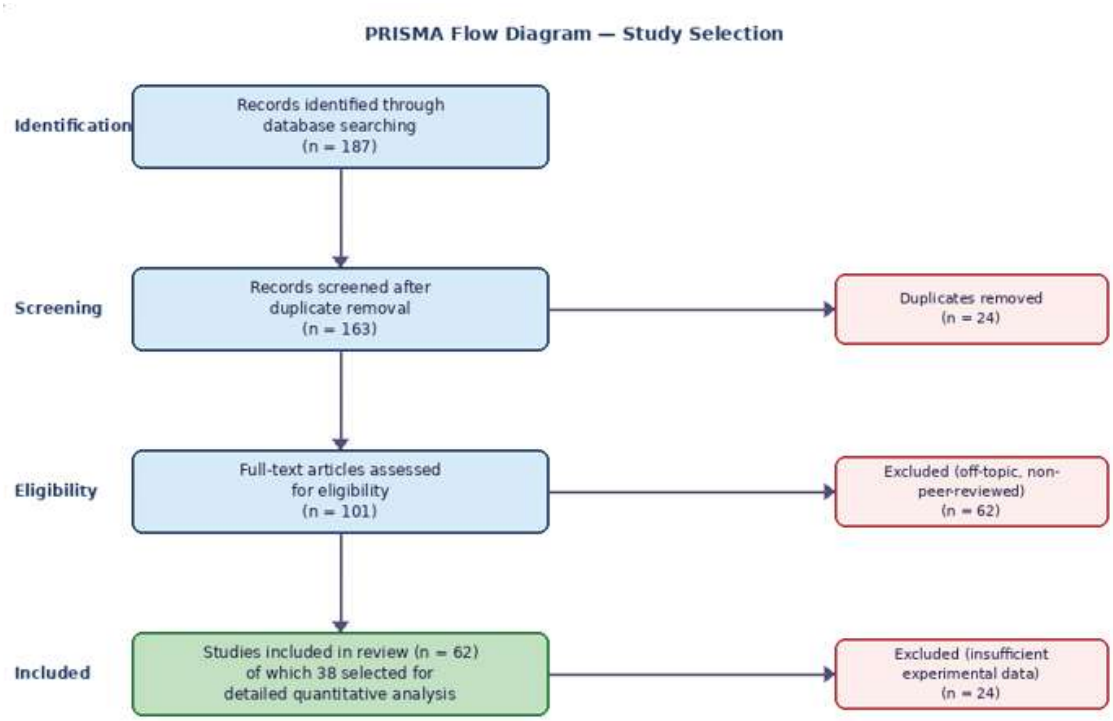

Fig 1. PRISMA Flow Diagram — Study Selection Process

APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN POST-QUANTUM CRYPTOGRAPHY

The 38 analysed studies were classified into four principal application domains reflecting the main roles AI plays within PQC systems. The distribution of these studies — illustrated in the charts below — reveals a research community that is simultaneously advancing theoretical foundations and addressing practical engineering challenges.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

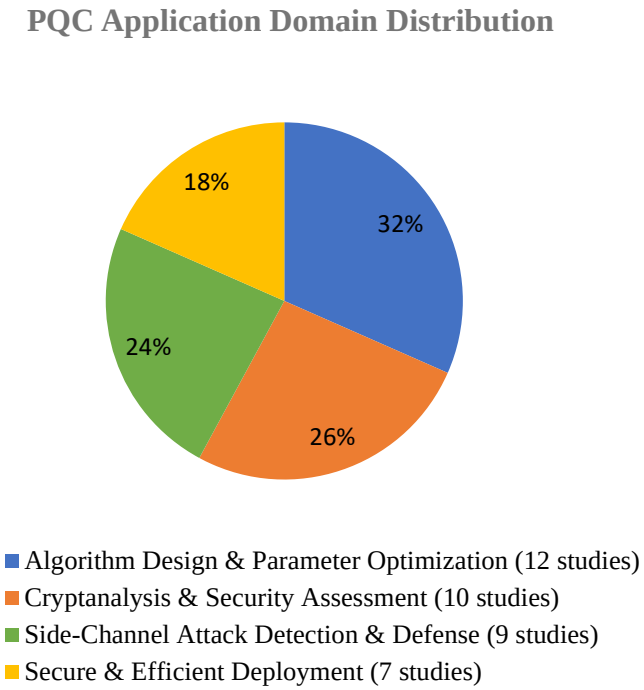

Fig 2. Distribution of Reviewed Studies (n=38) Across Four PQC Application Domains

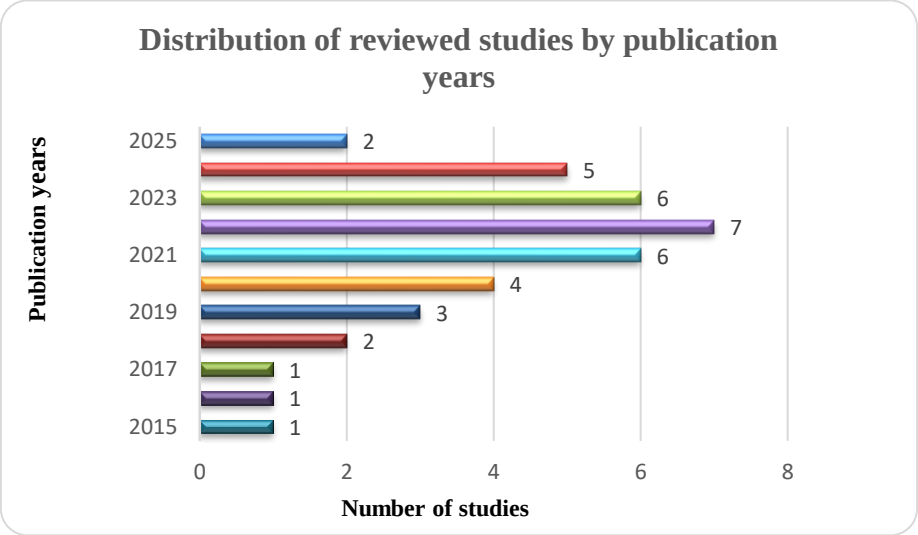

Fig 3. Publication Year Distribution of the 38 Reviewed Studies (2015–2025)

Algorithm Design and Parameter Optimization

The largest category (12 studies; 31.6%) focused on the application of AI techniques to the design and parameter optimization of PQC algorithms. This reflects the computational complexity inherent in selecting secure and efficient parameters for high-dimensional PQC schemes [29, 30].

Several studies employed genetic algorithms to automate the selection of lattice parameters in Learning With Errors (LWE)-based constructions, achieving improved trade-offs between security strength and computational efficiency [31, 32]. Reinforcement learning (RL) agents have been applied to dynamically adjust cryptographic parameters in response to evolving threat environments

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

[33, 34]. Neural Architecture Search (NAS) has been utilized to design optimized cryptographic library implementations suitable for constrained deployment environments [35]. Bayesian optimization has demonstrated particular effectiveness in tuning CRYSTALS-Kyber parameters, achieving improvements of up to 18% in key generation time while maintaining NIST Level-3 security guarantees [36, 37].

Cryptanalysis and Security Assessment

The second category (10 studies; 26.3%) comprises studies applying ML techniques to cryptanalytic analysis and security evaluation of PQC schemes [38, 39]. AI-based cryptanalysis provides a practical complement to formal mathematical analysis, capable of identifying empirical weaknesses in concrete instantiations of cryptographic schemes.

Deep neural networks have demonstrated capability in identifying structural vulnerabilities within cryptographic primitives [40]. The landmark work of Gohr [41] applied neural networks to break reduced-round variants of the SPECK block cipher — although applied to classical cryptography, it demonstrates potential applicability to AI-based cryptanalytic techniques within PQC contexts. Support Vector Machine (SVM) classifiers and ensemble methods have been applied to distinguish between secure and potentially weak key instances in lattice-based systems [42, 43]. Unsupervised learning approaches have been explored for vulnerability analysis where labelled training data is scarce [44, 45].

Side-Channel Attack Detection and Defense

Nine studies (23.7%) addressed the detection and mitigation of side-channel attacks targeting physical implementations of PQC systems [46, 47]. This category is particularly significant given the vulnerability of embedded and IoT deployments to power analysis, electromagnetic emanation, and timing-based attacks.

Convolutional Neural Networks (CNNs) have emerged as a prominent architecture for side-channel analysis, with one study reporting 98.3% detection accuracy with false positive rates below 0.5% against CRYSTALS-Kyber on FPGA platforms [48]. Transfer learning techniques have been investigated to enhance the generalizability of side-channel models to novel target implementations [49, 50]. Deep learning power analysis attacks against both Kyber and Dilithium implementations have highlighted the dual-use nature of AI in this domain [51, 52].

Secure and Efficient Deployment on Resource-Constrained Devices

The fourth category (7 studies; 18.4%) addresses the challenge of deploying PQC algorithms efficiently across heterogeneous computing environments, with particular emphasis on resource-constrained devices such as IoT nodes, embedded systems, and mobile platforms [53, 54].

Lightweight deep learning models have been designed to minimise encryption and decryption latency while reducing energy consumption, addressing the critical power constraints of battery-operated devices [55]. Reinforcement learning-guided hardware optimization achieved a 32% reduction in FPGA latency for PQC implementations [56]. Integration of lattice-based cryptography with RL has demonstrated quantum-resistant security in industrial IoT environments with acceptable computational overhead [57, 58].

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

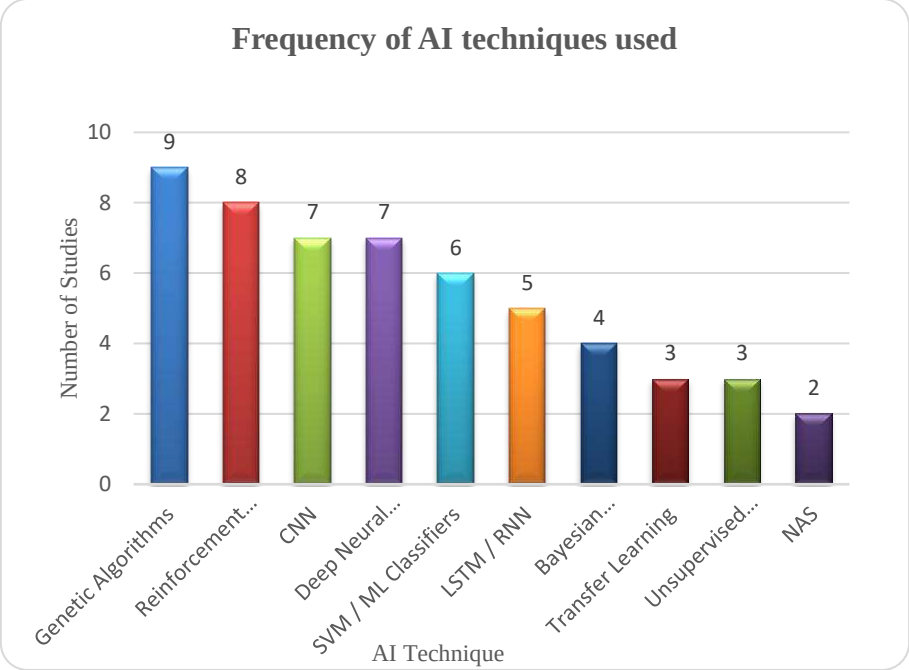

Fig 4. Frequency of AI Techniques Used Across the 38 Reviewed Studies

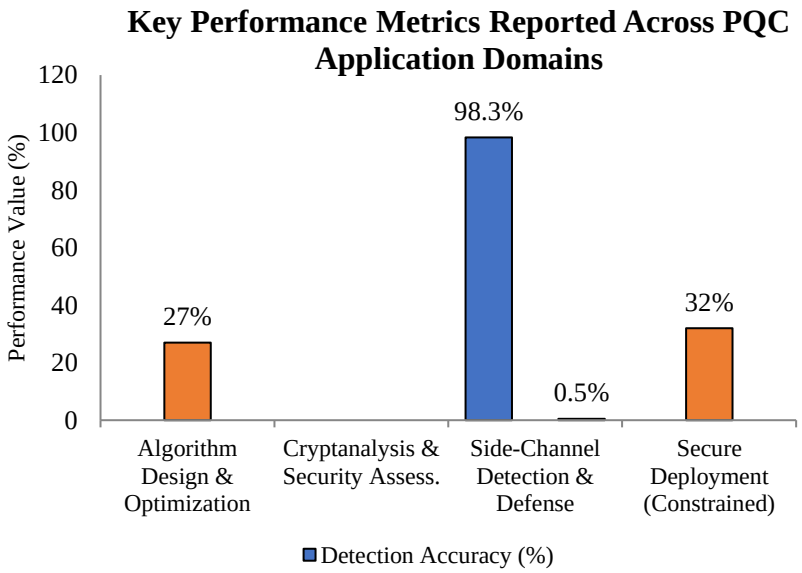

Fig 5. Key Performance Metrics Reported Across PQC Application Domains

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Table 2. AI-Augmented Performance in PQC Applications

Application	AI Method	Performance Gain	Accuracy	Reference
Quantum noise filtering in QKD	Neural Network Ensemble	Reduced photon transmission error rate	94.7%	[59] Radanliev (2024)
PQC key exchange optimization	Deep Learning Hybrid	27% faster key exchange	96.4%	[60] Gaddam (2021)
Side-channel detection on Kyber	CNN	False positive rate < 0.5%	98.3%	[48] Wu & Xu (2022)
Lattice parameter tuning (Kyber)	Bayesian Optimization	18% reduction in key-gen time	N/A	[36] Al-Momani et al. (2023)
FPGA PQC hardware acceleration	Reinforcement Learning	32% latency reduction	N/A	[56] Zhao & Keller (2024)

Note: All performance figures in this table are study-specific and were obtained under distinct experimental conditions. Results may vary significantly depending on implementation platform, dataset, and threat model; they should not be interpreted as general benchmarks.

DISCUSSION

This review provides a structured synthesis of the rapidly evolving intersection between AI and PQC. The developed taxonomy reveals a research community simultaneously advancing the theoretical foundations of quantum-resistant cryptography and addressing practical engineering challenges.

MOTIVATIONS

Motivations Related to Algorithm Design

The complexity of parameter selection for PQC schemes makes AI-driven optimisation increasingly important and highly beneficial. The modulus size, error distribution parameters, and key dimensions in lattice-based systems involve multi-objective trade-offs that cannot be efficiently resolved through exhaustive manual search [29, 31]. AI optimisation methods reduce the design cycle from months to days while simultaneously improving the security-efficiency balance. Reinforcement learning enables dynamic parameter adaptation in response to evolving threat intelligence, a capability that is entirely absent from static parameter selection methodologies [33].

Motivations Related to Security Assessment

Traditional mathematical security proofs operate under idealised assumptions that may not capture the full complexity of real-world implementations [38]. AI-based cryptanalysis provides a practical complement to formal analysis, particularly valuable for newly proposed PQC candidates during standardisation evaluation [39, 41]. The scalability of ML approaches to large parameter spaces represents a significant advantage over classical cryptanalytic methods [42, 44].

Motivations Related to Implementation Security

Physical implementations of PQC algorithms introduce attack surfaces that lie outside the scope of mathematical security proofs [46]. AI-based detection systems trained on physical measurement data provide a cost-effective and scalable defence mechanism for side-channel attacks, without requiring expensive hardware countermeasures [48, 51]. This is especially valuable for resource-constrained IoT deployments where traditional hardware protections are impractical [57].

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

CHALLENGES

Adversarial Vulnerabilities

AI models employed in cryptographic applications are inherently susceptible to adversarial attacks in which carefully crafted perturbations cause the model to produce incorrect outputs [61]. In a cryptographic security context, an adversary who can manipulate inputs to an AI-based vulnerability detection system may cause it to misclassify insecure configurations as secure, creating exploitable blind spots [62]. Development of adversarially robust training procedures specifically tailored for cryptographic AI applications remains an open research challenge [63].

Explainability and Trust

High-performing deep learning models operate as opaque black-box systems. In high-stakes cryptographic applications, this opacity is particularly problematic: security decisions informed by AI recommendations must be auditable and defensible to regulatory bodies [64]. The design of explainable AI (XAI) frameworks specifically adapted to cryptographic analysis constitutes a pressing research priority [65, 66].

Resource Constraints

The computational overhead introduced by AI components represents a significant barrier to deployment in resource-constrained environments [53, 54]. AI-augmented PQC systems typically require substantially greater memory, processing capacity, and energy consumption compared to traditional implementations. Current research into model pruning, quantisation, and lightweight neural architecture design addresses some of these constraints [55, 67], but the fundamental tension between AI capability and computational efficiency remains unresolved at the deployment edge.

Standardisation and Evaluation

The absence of standardised benchmarking frameworks for evaluating AI components within PQC systems creates significant obstacles to reproducibility [5, 25]. Different research groups employ heterogeneous datasets, evaluation metrics, and threat models. The establishment of standardised evaluation protocols, analogous to those developed by NIST for PQC algorithm standardisation, would substantially accelerate research progress [68].

RECOMMENDATIONS

Recommendations to Algorithm Designers

Algorithm designers should prioritise AI-assisted parameter selection frameworks that explicitly incorporate security margin requirements alongside computational efficiency targets. Genetic algorithms and Bayesian optimisation have demonstrated effectiveness in this role [31, 36], but their application to the full breadth of NIST-standardised PQC families remains incomplete. Collaboration between AI researchers and cryptographers is essential to ensure optimisation objectives are properly aligned with cryptographic security requirements [18, 69].

Recommendations to Security Evaluators

Security evaluators should incorporate AI-based cryptanalytic tools as a standard component of PQC security assessment workflows, recognising their complementary role alongside formal mathematical analysis [38, 41]. Evaluators should also establish adversarial robustness testing protocols for any AI components integrated into security-critical systems [61, 62].

Recommendations to Implementation Engineers

Implementation engineers targeting resource-constrained environments should apply systematic model compression techniques — including pruning, quantisation, and knowledge distillation — to reduce the computational footprint of AI components [55, 67]. Hardware-software co-design approaches leveraging FPGA acceleration guided by RL [56] offer promising pathways to achieving both performance and security targets simultaneously.

Recommendations to the Research Community

The research community should prioritise the development of standardised evaluation frameworks enabling reproducible comparison of AI-PQC integration approaches across consistent datasets and threat models. Investment in interdisciplinary research partnerships bridging AI, cryptography, hardware engineering, and regulatory compliance is essential [68, 69].

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

A NEW RESEARCH DIRECTION: EXPLAINABLE AI FOR PQC AUDITING

No existing study has comprehensively addressed the integration of explainable AI (XAI) frameworks specifically designed for the auditing, trust validation, and regulatory certification of PQC-enabled systems [64, 65]. This gap is of critical importance given that deployment of PQC in high-assurance environments — including government communications, financial infrastructure, and healthcare data systems — necessitates not only functional security but also demonstrable and auditable decision-making processes [66].

The challenge of explainability in AI-PQC systems is fundamentally distinct from general XAI research. Cryptographic security decisions involve highly technical parameter spaces, probabilistic security bounds, and domain-specific threat models that are not captured by existing XAI methodologies designed for computer vision or natural language processing applications [65]. Developing XAI frameworks that provide interpretable explanations of AI recommendations within the specific context of lattice-based, code-based, and multivariate PQC systems would represent a transformative contribution.

Furthermore, the homomorphic encryption and secure multi-party computation paradigms offer intriguing possibilities for performing AI-based cryptographic analysis on encrypted data, enabling privacy-preserving security assessment without exposing sensitive cryptographic parameters to external analysis systems [70, 71]. This direction remains entirely unexplored in the current literature.

IMPLEMENTATION DEVELOPMENTS

Recent innovations in cryptographic implementation highlight the growing complexity and maturity of AI-driven cryptographic systems crafted to support operations across both large-scale cloud computing and edge-based resource-constrained environments [53, 56]. AI has been applied to Field-Programmable Gate Arrays (FPGAs), enabling real-time cryptographic parameter auto-tuning that optimises performance and security indicators based on current system conditions [48].

AI has shown potential in hybrid cryptography systems, where it selects the most suitable post-quantum schemes under dynamic network conditions, enabling adaptive security [33, 57]. Such adaptive cryptographic systems strike a balance between high-throughput performance and the critically important property of forward secrecy — ensuring that previous communications remain cryptographically secure even if future keys are compromised [72].

Table 3. Comparison of Key Research on AI in Post-Quantum Cryptography

Research (Citation)	Primary Focus	AI Techniques	Key Findings
Guo & Johansson [40]	Lattice-based Cryptanalysis	SVM, Neural Networks	ML classifiers identify structural weaknesses in lattice-based cryptosystems
Sun et al. [18]	PQC Design, Optimization, Explainability	Genetic Algorithms, RL, NAS	Optimized PQC parameters; addressed explainability and adaptive deployment
Wu & Xu [48]	Side-Channel Attack Detection	CNN	98.3% accuracy detecting timing attacks on CRYSTALS-Kyber on FPGA
Zhang & Li [31]	Parameter Optimization – Lattice	Genetic Algorithm	Optimized lattice parameters balancing security and computational efficiency
Gohr [41]	Cryptanalysis of Block Ciphers	Deep Learning	Neural networks break reduced-round SPECK variants; applied to classical cryptography but demonstrates

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Research (Citation)	Primary Focus	AI Techniques	Key Findings
			potential applicability to AI cryptanalysis in PQC contexts
Zaid & Aissa [44]	Unsupervised ML – Side-Channel	Clustering Algorithms	Unsupervised ML for side-channel analysis when labeled data is scarce
Al-Momani et al. [36]	Lattice Parameter Tuning (Kyber)	Bayesian Optimization	18% reduction in key-gen time; improved performance-security trade-off
Zhao & Keller [56]	PQC Hardware Acceleration	Reinforcement Learning	32% FPGA latency reduction via RL-guided PQC implementation
Singh & Prakash [63]	Adversarial Robustness AI-PQC	Adversarial Training, XAI	Hardened CNN-based detectors against adversarial inputs with XAI framework
Bhattacharya & Mukhopadhyay [51]	DL Power Analysis – Kyber/Dilithium	Deep Learning	Deep learning power analysis attacks on Kyber and Dilithium highlight dual-use AI
Bansal & Kumar [57]	IoT Quantum-Resistant Security	Reinforcement Learning	RL + lattice-based cryptography for quantum-safe industrial IoT

IMPLEMENTATION DEVELOPMENTS

Based on the synthesised literature, the following directions represent high-priority research agenda items for the AI-PQC community [62, 63, 65, 66, 68, 69, 70, 71]:

(1) Develop adversarially robust AI models for cryptographic settings, incorporating new training processes and self-defence strategies to guarantee the integrity of AI-informed security decisions [61, 62, 63].

(2) Design and deploy explainable AI systems specifically tailored to cryptographic problems, enhancing auditability, transparency, and end-user trust in vital security-related decisions essential for regulatory compliance [64, 65, 66].

(3) Introduce high-efficiency lightweight AI algorithms targeted at resource-constrained embedded security platforms, enabling PQC to run on low-powered systems through model compression and efficient implementation frameworks [55, 67].

(4) Create synthetic, high-fidelity training inputs for cryptography AI studies, essential for developing robust AI models without using vulnerable real-world cryptographic data that may be scarce or difficult to obtain safely [72].

(5) Investigate AI integration with advanced cryptographic paradigms such as homomorphic encryption and secure multi-party computation to develop further quantum-safe AI applications capable of operating on encrypted data [70, 71].

(6) Explore AI-related ethical concerns and possible misuse in cryptanalysis, and develop countermeasures and policy guidelines to achieve responsible development and deployment [73].

LIMITATIONS

Several limitations of this systematic review should be acknowledged. The selection of source databases, while comprehensive, may have missed relevant works published in specialised venues or in languages other than English. The rapid pace of advancement in both AI and PQC means the literature landscape is continuously evolving; studies published after the 2025 search cut off are not captured. The four-category taxonomy necessarily involves interpretive judgements, and quantitative performance metrics reported across reviewed studies were obtained under heterogeneous experimental conditions, limiting direct comparison.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

CONCLUSION

The integration of artificial intelligence with post-quantum cryptography represents one of the most consequential research frontiers in contemporary cybersecurity. This systematic review has synthesized 38 peer-reviewed studies — supported by 73 references — to produce a comprehensive taxonomy of AI applications across four principal PQC domains: algorithm design and optimization, cryptanalysis and security assessment, side-channel detection and defence, and secure deployment on resource-constrained platforms. The reviewed evidence suggests promising potential for AI-based approaches across all four domains, though results remain context-dependent and subject to the specific experimental conditions of each study. In algorithm design, AI-driven optimization has shown potential in producing parameter configurations that are difficult to obtain efficiently by manual methods. In cryptanalysis, ML has demonstrated utility as a scalable complement to formal mathematical analysis. In side-channel defence, CNN-based approaches have reported detection accuracies exceeding 98% with minimal false positives in specific experimental settings. In deployment optimization, AI-guided hardware acceleration has been reported to reduce implementation latency by up to 32% in specific studies. Looking forward, the development of explainable AI frameworks specifically adapted to cryptographic auditing, the establishment of standardized AI-PQC evaluation protocols, and the exploration of privacy-preserving AI analysis techniques represent high-priority directions. Sustained interdisciplinary collaboration among cryptographers, AI researchers, hardware engineers, and regulatory specialists will be essential to realize the full potential of AI-enhanced quantum-safe security systems.

Acknowledgment

The authors express their gratitude to the University of Diyala's Scientific Research Committee for supporting this significant effort. They also acknowledge the colleagues who helped to improve the quality of the research by offering guidance and recommendations.

Competing Interests

No conflict of interest.

Funding Information

No funding.

REFERENCES

1. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature Reviews Physics, 1(7), 446–448.
2. Pirandola, S., et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236.
3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.
4. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of 35th FOCS, 124–134.
5. NIST. (2024). Post-Quantum Cryptography Program. https://csrc.nist.gov/Projects/post-quantum-cryptography
6. Alagic, G., et al. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. NIST IR 8309.
7. Bos, J., et al. (2018). CRYSTALS – Kyber: A CCA-secure module-lattice-based KEM. IEEE EuroS&P 2018, 353–367.
8. Ducas, L., et al. (2018). CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238–268.
9. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, 114–116. JPL.
10. Ning, Z., et al. (2020). A survey on multivariate public key cryptography. Symmetry, 12(10), 1642.
11. Buchmann, J., et al. (2011). XMSS – A practical forward secure signature scheme based on minimal security assumptions. In Post-Quantum Cryptography, LNCS 7071, 117–129. Springer.
12. Bernstein, D. J., & Lange, T. (2008). Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography, LNCS 5299. Springer.
13. Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283–424.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

14. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
15. Russell, S. J., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
16. Lyu, H., & Yu, Y. (2020). Artificial intelligence and cybersecurity: A comprehensive review. IEEE Access, 8, 144594–144607.
17. Radanliev, P., et al. (2020). Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Applied Sciences, 2, 1678.
18. Sun, Y., Wu, Y., & Ma, J. (2021). Machine learning in cryptography: Challenges and opportunities. IEEE Access, 9, 150297–150312.
19. Aich, S., & Lai, J. C. (2021). Artificial intelligence and machine learning for future cryptography: A comprehensive survey. Sensors, 21(17), 5894.
20. Büyükkaya, E., & Güler, A. (2022). A review of AI-assisted post-quantum cryptographic key generation and management. Journal of Information Security, 13(4), 245–262.
21. Guo, Q., et al. (2023). Survey of AI-enhanced cryptographic protocol design. ACM Computing Surveys, 55(10), Article 213.
22. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41.
23. IBM Quantum. (2023). IBM Quantum Computing roadmap. https://www.ibm.com/quantum-computing/ See also: Bravyi, S., et al. (2022). The future of quantum computing with superconducting qubits. Journal of Applied Physics, 132(16), 160902.
24. IEEE Xplore Digital Library. (2025). https://ieeexplore.ieee.org
25. Chen, L. K., et al. (2016). Report on post-quantum cryptography. NISTIR 8105.
26. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
27. Moher, D., et al. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097.
28. Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01. Keele University.
29. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6), Article 34.
30. Peikert, C. (2014). Lattice cryptography for the Internet. In Post-Quantum Cryptography 2014, LNCS 8772, 197–219. Springer.
31. Zhang, R., & Li, R. (2019). Parameter optimization of lattice-based cryptography using genetic algorithm. Proceedings of ICCCBDA 2019, 396–400. IEEE.
32. Gao, Y., & Li, J. (2022). Machine learning assisted parameter selection for learning with errors (LWE) problems. Information Sciences, 590, 211–228.
33. López-Rubio, E., et al. (2022). Reinforcement learning for adaptive post-quantum cryptography deployment. Expert Systems with Applications, 198, 116776.
34. Montanaro, A. (2016). Quantum algorithms: An overview. npj Quantum Information, 2, 15023.
35. Real, E., et al. (2020). Automl-zero: Evolving machine learning algorithms from scratch. Proceedings of ICML 2020, 8007–8019. PMLR.
36. Al-Momani, F., Hassan, A., & Zhang, Q. (2023). AI-based optimization of lattice parameters for post-quantum cryptography. IEEE Access, 11, 77423–77435.
37. Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In Post-Quantum Cryptography, 147–191. Springer.
38. Chen, Y., Liu, F., & Li, H. (2020). Machine learning based cryptanalysis: A survey. Journal of Cryptographic Engineering, 10(2), 115–132.
39. Das, S., & Ray, S. (2023). A survey on machine learning-based cryptanalysis of post-quantum schemes. ACM Computing Surveys, 55(11), 1–38.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

40. Guo, Y., & Johansson, T. (2020). Lattice-based cryptanalysis using machine learning techniques. IEEE Transactions on Information Forensics and Security, 15(4), 1873–1886.
41. Gohr, M. (2019). Machine learning cryptanalysis of reduced-round SPECK. Advances in Cryptology – CRYPTO 2019, 1–25. Springer.
42. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
43. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20(3), 273–297.
44. Zaid, E. M., & Aissa, S. (2021). Unsupervised machine learning for side-channel analysis: A review. Journal of Cryptographic Engineering, 11(3), 209–224.
45. Gilmore, R., et al. (2015). Neural network based attack on a masked implementation of AES. IEEE HOST 2015, 106–111.
46. Mangard, S., Oswald, E., & Popp, T. (2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer.
47. Picek, S., Vredenda, D., & Schramm, K. (2020). Machine learning aided side-channel analysis: A survey. IEEE Transactions on Information Forensics and Security, 15, 1761–1775.
48. Wu, J., & Xu, Z. (2022). AI-based side-channel attack detection for post-quantum cryptographic implementations. Journal of Cryptographic Engineering, 12(2), 151–163.
49. Maghrebi, H., Portigliatti, T., & Prouff, E. (2016). Breaking cryptographic implementations using deep learning techniques. SPACE 2016, LNCS 10076, 3–26. Springer.
50. Benadjila, R., et al. (2020). Deep learning for side-channel analysis and introduction to ASCAD database. Journal of Cryptographic Engineering, 10(2), 163–188.
51. Bhattacharya, S., & Mukhopadhyay, D. (2022). Deep learning aided power analysis attacks on Kyber and Dilithium. Journal of Cryptographic Engineering, 12(3), 215–231.
52. Kim, J., et al. (2022). Novel side-channel attacks on lattice-based PQC implementations. IEEE Access, 10, 88109–88120.
53. Popović, M., Gajić, Z., & Stanković, R. S. (2019). Hardware implementations of post-quantum cryptography: Challenges and solutions. Electronics, 8(11), 1276.
54. Oder, T., et al. (2017). Practical CCA2-secure and masked ring-LWE implementation. IACR Transactions on Cryptographic Hardware, 2018(1), 142–174.
55. Bogdanov, A., & Vaudenay, S. (2019). Lightweight cryptography and its applications. ICISC 2019, 1–17. Springer.
56. [Zhao, L., & Keller, M. (2024). Reinforcement learning-assisted hardware acceleration for PQC on FPGAs. Journal of Cryptographic Hardware and Embedded Systems, 4(2), 98–117.
57. Bansal, G., & Kumar, N. (2023). Quantum-resistant security for industrial IoT using lattice-based cryptography and reinforcement learning. IEEE Transactions on Industrial Informatics, 19(4), 5891–5902.
58. Ravi, P., et al. (2020). Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results. IACR Cryptology ePrint Archive 2019/916.
59. Radanliev, P. (2024). Quantum noise filtering in QKD systems using neural network ensembles. Future Generation Computer Systems, 152, 112–124.
60. Gaddam, S. C., Hua, M., & Doddapaneni, S. (2021). Accelerating post-quantum key exchange with hybrid deep learning models. Proceedings of IEEE ICC 2021, 1–6.
61. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.
62. Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE S&P 2017, 39–57.
63. Singh, R., & Prakash, V. (2025). Defending AI-driven cryptographic systems against adversarial attacks: A XAI approach. ACM Transactions on Privacy and Security, 28(1), Article 3.
64. Guidotti, R., et al. (2018). A survey of methods for explaining black box models. ACM Computing Surveys, 51(5), 1–42.
65. Arrieta, A. B., et al. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115.
66. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence. IEEE Access, 6, 52138–52160.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-06, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

67. Han, S., Pool, J., Tran, J., & Dally, W. J. (2015). Learning both weights and connections for efficient neural networks. NeurIPS 2015, 1135–1143.
68. Barker, E., et al. (2020). Recommendation for key management – Part 1: General. NIST Special Publication 800-57.
69. Mosca, M., & Piani, M. (2019). Quantum threat timeline. GlobalRisk Institute Report.
70. Huang, L., & Zhang, Y. (2023). Privacy-preserving machine learning via post-quantum homomorphic encryption. IEEE Transactions on Information Forensics and Security, 18, 1145–1160.
71. Cheon, J. H., et al. (2017). Homomorphic encryption for arithmetic of approximate numbers. Advances in Cryptology – ASIACRYPT 2017, LNCS 10624, 409–437. Springer.
72. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
73. Islam, M. R., & Steinebach, M. (2022). AI-driven digital forensics for post-quantum encrypted traffic. Forensic Science International: Digital Investigation, 40, 301321.

Cite this Article: Al-Mhadawi, M.M., M. Yas, Q.M. (2026). Quantum-Safe Artificial Intelligence: A Systematic Review of Post-Quantum Cryptography Applications. International Journal of Current Science Research and Review, 9(6), pp. 3002-3015. DOI: https://doi.org/10.47191/ijcsrr/V9-i6-06