Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 2, 2026

REVIEW: POST-QUANTUM CRYPTOGRAPHY IN INTELLIGENT SYSTEMS

Nadeem Taj[*1], Aroosha Masood[2], Dr Junaid Arshad[3]

[*1,2,3]*Department of Computer Science, University of Engineering & Technology, Lahore, Pakistan*

[*1]nadeemtaj407@gmail.com, [2]2024MSCS26@student.uet.edu.pk, [3]junaidarshad@uet.edu.pk

DOI: https://doi.org/10.5281/zenodo.18691759

Keywords
Post-quantum cryptography, quantum computing, intelligent systems, lattice-based cryptography, NIST standardization, IOT security, autonomous vehicles, quantumresistant algorithms.

Article History
Received: 17 December 2025
Accepted: 01 February 2026
Published: 19 February 2026

Corresponding Author: *
Nadeem Taj

Abstract
The advent of quantum computers is highly threatening to traditional cryptographic systems, especially for intelligent systems like autonomous cars, IoT devices, and smart grids. The popular algorithms such as RSA and ECC that form the pillars of contemporary digital security are vulnerable to quantum attacks, thus the invention of post-quantum cryptography (PQC). PQC features quantum-resistant algorithms that will be secure against both classical and quantum computer attacks. This review paper discusses the developments of PQC between 2023 and 2025, with a focus on its usage in intelligent systems. We underscore the peculiarities of implementing PQC in resource-limited environments, latticebased cryptography advancements, and NIST standardization. We also highlight research gaps, e.g., lightweight solutions for PQC in IoT and real-time systems, and hybrid cryptographic schemes. Our review synthesizes recent literature to present a broad understanding of PQC's capabilities and limitations, providing insights into directions for the future of securing intelligent systems in the quantum world.

INTRODUCTION

1. FUNDAMENTALS

1.1 Overview of Intelligent Systems

Intelligent systems represent a revolutionary idea in the current computing context. Intelligent systems leverage artificial intelligence (AI), machine learning (ML) [1], edge computing, and sensor technologies to create autonomous or semi-autonomous systems capable of complex human-like tasks with minimal to no oversight. Intelligent systems are transforming industries, and providing machines the ability to see their environment, analyse the information, make decisions and act on them at speed and precision that is phenomenal [2].

1.1.1 A Sensory Input Layer.

At the essence of intelligent systems is their capacity to sense, similar to human senses, to perceive and understand the world. In this respect, the systems utilize an advanced network of sensors that gather varied streams of data in realtime [3]. Visual sensors such as high-definition cameras, infrared, and 3D depth sensors offer extensive object recognition and spatial mapping abilities. LiDAR and radar systems are utilized to sense distance and identify obstacles, and they are essential for autonomous vehicle navigation. Environmental sensing is offered by temperature, humidity, and air quality sensors that form essential infrastructure of intelligent city and precision agriculture [4]. Biometric sensors in

wearable technology continuously monitor vital parameters such as heart rate and blood oxygenation in healthcare. Sensor fusion is best exemplified in autonomous vehicles, where fusion of LiDAR, radar, and camera data offers an extensive 360-degree environmental perception, enabling safe navigation through dense traffic [5].

1.1.2 AI Processing Layer

The AI processing layer is the intelligent core of intelligent systems, transforming raw sensor data into actionable intelligence. This is achieved through a variety of machine learning approaches, including supervised learning methods, which classify patterns employed in medical diagnostics, and unsupervised learning that identifies patterns embedded in complicated data [6]. Deep learning architectures have a specialized role, with convolutional neural networks (CNNs) demonstrating incredible performance on image recognition tasks and recurrent neural networks (RNNs) processing sequential data such as speech and time-series data. Edge AI brought the ability to run optimized machine learning models directly on IoT devices, allowing real-time processing for facial recognition on security systems without the need for cloud connectivity [7]. Smart grid uses make apparent the ability of this layer, where reinforcement learning algorithms learn about consumption patterns and make predictions about demand peaks to automatically regulate the supply of power, keeping the grid stable during peak usage.

1.1.3 Decision-Making Module

The choice-making module is the executive function in intelligent systems, translating processed information into concrete actions and responses. In rule-based systems, deterministic responses are returned to well-defined scenarios, such as sounding alarms when industrial sensors detect equipment operating beyond safe parameters. Adaptive control systems further empower robots to continually hone their movements based on real-time sensory feedback [8] [9]. Human-in-the-loop (HITL) setups have an important equilibrium between automation and human control, such as in high-risk operations like response drones where AI provides recommendation but human pilots have final decision-making capacity. Factory environments see this module applied through predictive maintenance systems that learn from vibration sensor readings to detect emerging equipment failures and automatically schedule preventive repairs ahead of time, minimizing downtime and maintenance expenses. All this sensing, processing, and decision-making infrastructure makes it possible for smart systems to perform more advanced tasks in many areas, from urban mobility to industrial automation and healthcare delivery [10] [11].

Table 1.1 Applications across Industries

Industry	Use Case	Key Technologies
Autonomous Vehicles	Self-driving cars navigating complex urban environments	LiDAR, CNN-based object detection, V2X comms
Smart Grids	Dynamic load balancing and renewable energy integration	AI-driven demand forecasting, IoT sensors
Healthcare	Robotic surgery with sub-millimeter precision	Computer vision, haptic feedback systems
Industrial IoT	Predictive maintenance reducing unplanned downtime	Vibration analysis, digital twins
Agriculture	Precision farming with automated irrigation and pest detection	Satellite imagery, soil moisture sensors

1.2 Classical Cryptography in Intelligent Systems

1.2.1 The Backbone of Digital Security

Since more than four decades, classical cryptographic algorithms have offered a foundation for securing intelligent systems, wherein privacy and integrity are preserved through authentication, over secure data [12]. Classical methods are our understanding's first line of defense within our increasingly networked world of smart devices and autonomous systems.

1.2.2 Main Algorithms Used

Three dominant cryptographic standards are implemented in today's systems. RSA, named after its creators Rivest, Shamir, and Adleman, remains widely used to securely exchange keys and make digital signatures. When increased efficiency is desirable, Elliptic Curve Cryptography (ECC) offers the same level of security with significantly smaller keys. The Advanced Encryption Standard (AES) is the symmetric encryption workhorse, protecting data at rest and in transit on millions of devices [13].

1.2.3 Implementation in Contemporary Systems

These cryptographic foundations support essential security operations in intelligent systems. Transport Layer Security protocols use RSA and ECC to provide secure communication channels between IoT devices and cloud platforms. Digital signatures from ECDSA ensure the authenticity of firmware updates for self-driving vehicles and industrial machinery. AES-256 encryption, on the other hand, secures sensitive training data in AI development environments and guards personal information in smart devices [14].

1.3 Quantum Computing and the Threat to Classical Cryptography

1.3.1 The Quantum Revolution

Quantum computing represents a revolution in computing power, leveraging the spooky principles of quantum mechanics to render otherwise intractable problems tractable to a classical computer. This new tech is an existential threat to current cryptographic practices and potentially could undermine decades of security infrastructure [15]. 1.3.2 Quantum's Cryptographic Killers

There are two quantum algorithms, in particular, that threaten classical cryptography [16]. Shor's algorithm will efficiently solve the integer factorization and discrete logarithm problems that underlie RSA and ECC security. Grover's algorithm provides a quadratic speedup of brute-force search, effectively cutting the security strength of symmetric key schemes such as AES in half.

1.3.3 Vulnerable Systems and Applications

The implications for intelligent systems are catastrophic and wide-ranging. V2X communications enabling autonomous driving can be intercepted. Smart grids based on RSA-signed control commands for energy distribution can be vulnerable to spurious commands [17]. Even rudimentary IoT devices using AES encryption can have their security margins dramatically eroded.

1.3.4 The Quantum-Resistant Solution

Post-quantum cryptography is algorithms that will be resistant to classical and quantum computer attacks. Nextgeneration cryptographic techniques are based on problems in mathematics that are considered hard for a quantum computer to solve [18].

1.3.5 NIST's Standardization Effort

The National Institute of Standards and Technology (NIST) has spearheaded worldwide efforts to test and standardize PQC algorithms. Their multi-year selection process has come up with numerous promising candidates for each of various mathematical approaches [19].

1.3.6 Algorithm Families and Characteristics

PQC schemes fall into five broad categories: lattice-based, code-based, multivariate polynomial, hash-based, and isogeny-based cryptography. They each offer distinct security advantages and performance and implementation viability challenges [20].

1.4 The Age of Quantum-Resistant Security

Post-quantum cryptography (PQC) is the next-generation cryptography algorithm written to be secure for both classical computers and future quantum computers. Unlike standard cryptography written around mathematical problems easily vulnerable to attack with quantum algorithms like Shor's and Grover's, PQC derives its security from complex mathematical constructs so difficult to crack even for quantum computers [21]. This new domain is not a matter of replacing existing cryptography, but of developing the alternative solutions for the specific vulnerabilities emphasized by quantum computing [22].

1.4.1 The Five Pillars of Post-Quantarum Security

Five large approaches to building quantum-resistant cryptography have been recognized by researchers, each drawing upon distinct mathematical principles and practical considerations:

Lattice-based cryptography has turned out to be the most promising approach, based on the difficulty of highdimensional geometric objects called lattices. The algorithms are computationally convenient to employ and offer secure proofs. NIST selected the CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms in this category for standardization [23].

1.4.1.1 Code-based cryptography

Code-based cryptography relies on the difficulty of solving random error-correcting codes, a problem that has been resistant to attacks for several decades [24]. While offering very high security, the systems are likely to require gigantic key sizes and hence are less convenient for some applications. The Classic McEliece algorithm is this category in NIST's standardization process.

1.4.1.2 Multivariate polynomial cryptography

Multivariate polynomial cryptography uses systems of nonlinear polynomial equations that are easy to produce but hard to solve. Although the original schemes were broken, research is still continued into more secure versions [25]. The technique can be particularly useful for digital signatures.

1.4.1.3 Hash-based cryptography

Hash-based cryptography attains all its security from cryptographic hash functions, which are also believed to be quantum-resistant. Schemes in this category are conceptually quite simple but typically produce large signatures.

SPHINCS+ was the hash-based algorithm selected by NIST [26].

1.4.1.4 Isogeny-based cryptography

Isogeny-based cryptography is based on mathematical properties of elliptic curve relationships. While initially very promising (with the SIKE algorithm), this approach was given a severe setback when scientists discovered an effective attack, which led to its deprecation in the NIST process [27].

1.4.2 The Road to Standardization

The National Institute of Standards and Technology (NIST) has been leading a global, multi-year initiative to evaluate and standardize post-quantum cryptographic algorithms [28]. This rigorous process involves:

- Multiple cycles of public assessment
- Cryptanalysis by international developers
- Performance testing on different platforms
- Security aspect during implementation

After a series of competition, NIST announced its initial picks in 2022 [29], with lattice-based algorithms leading the show. Standardization continues, however, as developers aim to optimize these algorithms and look into additional alternatives.

The transition to post-quantum cryptography is one of the most intimidating hurdles information security has ever encountered. Unlike previous cryptographic transitions that were possible to deploy incrementally, quantum threat necessitates pre-emptive action before quantum computers become powerful enough. Organizations across industries are now beginning to consider their systems and prepare for what experts call "the biggest cryptographic migration in history." Efforts being made today in PQC research and standardization will determine the security landscape for the next few decades [30].

2. LITERATURE REVIEW

2.1 Lattice-Based Cryptography: The Leading Contender

2.1.1 CRYSTALS-Kyber (Key Encapsulation Mechanism)

As the primary key establishment algorithm selected by NIST, Kyber leverages the hardness of Module Learning With Errors in lattice theory. Its structure is such that it produces cryptographic keys as a function of the difficulty of short vector search in high-dimensional lattices - something that is challenging even for quantum computers [31]. Kyber offers three security levels (128-bit, 192-bit, and 256-bit quantum security) with quite compact ciphertexts of sizes between 800 and 1,500 bytes. The algorithm's efficiency lies in employing algebraic structured lattystals allowing fast computation of polynomials. Though its keys are larger than traditional ECC keys (1-2KB versus 256 bits), highly optimized implementations are very fast, and tests show encryption/decryption operations in milliseconds on typical hardware [32]. NIST selected Kyber as a standard due to its excellent performance/safety trade-off, but there are some concerns about its resistance to future advances in lattice reduction algorithms [33].

2.1.2 CRYSTALS-Dilithium (Digital Signatures)

This signature scheme, also selected by NIST, is founded on the hardness of the Module Short Integer Solution (MSIS) and MLWE problems. The implementation of Dilithium is in the vein of the Fiat-Shamir paradigm with optimizations to yield real-world performance [34]. The algorithm allows for tunable security parameters so that implementations can opt for faster operation over larger security margins. Signature sizes are 2,500 to 4,500 bytes based on security level, which is considerably larger than for ECDSA signatures but within the reach of all but the most computationally taxing applications. One of its strengths is a relatively fast verification process, and therefore it is particularly suitable to systems that need to verify large quantities of signatures. However, signature generation remains computationally costly compared to classical alternatives, particularly at higher levels of security. The selection by NIST of Dilithium reflects confidence in its security theorems and the state of advancement of lattice-based cryptography [35] [36].

2.2 Code-Based Cryptography: Proven Security

2.2.1 Classic McEliece

The most veteran post-quantum contender with its origins in 1978, Classic McEliece offers unparalleled security guarantee. Its security rests on the intractability of decoding a randomly chosen linear code - an obstacle that has been insurmountable to both classical and quantum attacks for decades [37]. Its function relies on employing large, randomly generated matrices as public keys with private keys containing structural information to make decoding easy. While its security is excellent, practical deployment is very difficult due to very large key sizes (usually 1MB+ for public keys). Later versions have reduced key sizes to about 300KB without compromising on security, but this is still not possible in most embedded systems. NIST included Classic McEliece as a backup due to its conservative security, particularly for high-security applications where key size is less of an issue than long-term confidence [38].

2.2.2 BIKE (Bit Flipping Key Encapsulation)

This code-based counterpart utilizes quasi-cyclic moderatedensity parity-check (QC-MDPC) codes to achieve smaller key sizes (around 20-40KB). BIKE security depends on the decoding problem in these structured codes, and they offer a potential sweet spot for trading off between provable security of Classic McEliece and practical key sizes [39]. Security analysis for these structured codes is less mature than for random codes, with some parameter choices having to be adjusted during the NIST testing program. BIKE makes computations quicker than Classic McEliece but remains behind lattice-based opponents. Its inclusion in NIST's alternative portfolio is a testament to the value of diversity in cryptographic assumptions [40].

2.3 Multivariate Polynomial Cryptography: The Efficiency Play

2.3.1 Rainbow Signature Scheme

This is a multivariate quadratic scheme that is one of the most efficient signature schemes with very quick verification time. Rainbow derives its security from the intractability of solving sets of multivariate quadratic equations over finite fields, an NP-hard problem that is known to be so in the worst case. The scheme does this by the construction of a centralized map that is easy to invert with a secret key but apparently random without one [41]. With pleasing performance characteristics, especially for devices with limited resources, security in multivariate schemes has nevertheless been famously hard to assess definitively. Rainbow fell out of contention at NIST when weaknesses in its internal structure were found, uncovering the delicate balance required in choosing parameters to these schemes [42]. Ongoing work is exploring more secure multivariate constructions that could combine their efficiency advantages with stronger security guarantees. Hash-Based Cryptography: The Most Conservative Option

Category	Algorithm Examples	Security Basis	NIST Status	Pros	Cons
Latticebased	CRYSTALS-Kyber, Dilithium, Falcon	MLWE, MSIS, NTRU	Standard (Kyber, Dilithium), Alternate (Falcon)	Fast operations (2-5ms), Strong security proofs	Large keys (1-4KB), Memory intensive

2.3.2 SPHINCS+

SPHINCS+ is NIST's selection of hash-based signature scheme and has the most conservative assumptions of security among all the PQC candidates.

Its security relies solely on the collision resistance of cryptographic hash functions, making it quantum-resistant to all known attacks [43]. The scheme utilizes a stateless manytime signature construction based on hash trees and few-time signatures. SPHINCS+ offers very good long-term security confidence at the expense of serious practical deficiencies: signature sizes are between 8KB and 40KB according to security level, and signing operations are quite slow compared to other approaches. NIST included SPHINCS+ as a fall-back for scenarios where absolute strongest security guarantees are required at any performance cost, or in which the security of alternative methods may be called into doubt by future cryptanalytic advances [44].

2.4 Isogeny-Based Cryptography: A Cautionary Tale

2.4.1 SIKE (Supersingular Isogeny Key Encapsulation)

This algorithm, based on the difficulty of computing isogenies between supersingular elliptic curves, initially generated a great deal of excitement due to its extremely compact key sizes (comparable to native ECC) [45].

SIKE's elegant mathematical foundation and fast parameters made it an extremely appealing choice for resource-limited settings. In 2022, however, a catastrophic quantum break on SIKE based on exotic quantum algorithms destroyed SIKE's security. It was depreeched straightaway in the NIST process. This incident is a reminder of the challenges of quantum resistance measuring and the value of multiple algorithmic approaches to post-quantum cryptography [46].

Integration of post-quantum cryptography (PQC) into smart systems such as IoT devices, autonomous vehicles, smart grids, and industrial control systems is hampered by several factors because of computational demands, real-time processing, and interoperability. This section presents a comprehensive review of recent

literature from 2023 to 2025 on the most significant advancements in PQC algorithms, implementation strategies, and optimization techniques for smart systems [47].

The landscape of post-quantum cryptographic techniques is constantly evolving as researchers advance existing techniques and explore new mathematical foundations. The NIST standardization process is merely the beginning of a multi-year process that will have to consider with care performance characteristics, implementational security, and necessary compromises between techniques. As quantum computer technology advances, this diverse portfolio of techniques will have the tools at hand to safeguard our digital universe from current and future threats [48] [49].

Table: 2.1 Comparison of Cryptography Techniques

Code-based	Classic McEliece, BIKE, HQC	Decoding random/structured codes	Alternate (McEliece), Round 4 (BIKE, HQC)	Long security history (since 1978), Sidechannel resistant	Huge keys (KB-MB), Slow KEM operations
Hash-based	SPHINCS+, XMSS, LMS	Hash collisions	Standard (SPHINCS+), RFC 8391 (XMSS)	Minimal assumptions, Quantum-safe	Very large sigs (8-40KB), Slow signing
Multivariate	Rainbow, GeMSS, MQDSS	MQ equations	Withdrawn (Rainbow), Round 4 (GeMSS)	Fast verification, Small signatures	Broken schemes, Parameter sensitivity
Isogenybased	SIKE, CSIDH	Isogeny paths	Broken (SIKE), Round 4 (CSIDH)	Compact keys, Elegant math	SIKE broken (2022), CSIDH slow
Hybrid	ECC+Kyber, RSA+Dilithium	Combined assumptions	N/A	Transition-friendly, Backward compatible	Complex implementation, Larger payloads
Hardware Accelerated	FPGA/ASIC PQC	Varies by algorithm	N/A	10-100× speedup, Energy efficient	High development cost, Less flexible
AI-Optimized	ML-enhanced PQC	Algorithmspecific	N/A	Adaptive security, Autotuned params	New attack surfaces, Untested long-term

3. METHODOLOGY

3.1 Integration of Post-Quantum Cryptography in Intelligent Systems

As AI and ML technologies increasingly become embedded in life-critical sectors, ranging from medicine to autonomous transport, their cryptographic bases will have to be quantumresistant. This is not just a question of replacing classical algorithms with PQC; the transition must be done so as not to impair system performance or functionality while providing security benefits [50].

For instance, AI-driven decision-making in preventing financial fraud or real-time traffic management cannot have latency spikes due to slow cryptographic operations. Research indicates

that performance-tuned PQC protocols such as lattice-based Kyber for key exchange or hash-based SPHINCS+ for signatures retain high security without a compromise on speed. The twist is effortless integration— adapting with appropriate computational overhead, power, and backward compatibility, especially for legacy systems still rooted in traditional cryptography [51].

3.2 Architectural Framework for PQC-Enabled Intelligent Systems

A well-designed PQC-enabled smart system operates across several layers, each with tailored cryptographic requirements in order to deliver end-to-end quantum immunity [52].

3.2.1 Perception Layer

At the edge, where devices like environmental sensors and cameras produce enormous volumes of data, light PQC deployments are of utmost importance. These devices typically possess limited processing power, thus efficient algorithms like Kyber-512 or SPHINCS+-faster are ideal for secure authentication and integrity checks on data. Hardware
Security Modules (HSMs) and Trusted Execution Environments (TEEs) also serve to enhance security by isolating cryptographic operations from any intrusion [53].

For example, a smart city traffic management system might use hash-based signatures to verify sensor data without degrading energy efficiency a critical factor when running from batteries [54].

3.2.2 Communication Layer:

Secure data transmission is important in V2X and IoT networks. Hybrid cryptographic schemes such as the employment of Elliptic Curve Cryptography (ECC) combined with Kyber-based key exchange for TLS 1.3 are a transition security model [55]. It provides backward compatibility with existing systems and sets the stage for eventual deployment of PQC.
Dilithium signatures are gaining traction for authentication of messages in low-latency scenarios, such as autonomous vehicle communication, where even a few milliseconds delay would be catastrophic. Quantum-resistant VPNs also secure sensitive information enrooted from being intercepted by post-quantum eavesdroppers [56].

3.2.3 Processing Layer

AI systems are deeply dependent on high-performance computing for applications such as real-time analytics and federated learning. In such cases, lattice-based cryptography is particularly beneficial because it is parallelizable, making it a natural solution for workloads in GPUs and AI accelerators [57].
Secure enclaves with PQC-protected memory encryption keep sensitive ML models like those employed in medical diagnosis secret even if the underlying hardware is breached. Federated learning systems also gain from PQC by allowing secure aggregation of model updates without revealing raw data [58].

3.2.4 Decision Layer:

At the most extreme, intelligent systems will need to enforce dynamic security policies based on real-time threat analysis. Policy engines will be able to automatically switch between cryptography algorithms [59] e.g., prioritize Falcon signatures for high-rate transactions and use SPHINCS+ for longer-term audit logs where signature size is less important [60].
Blockchain networks increasingly deployed for decentralized management of AI are also adopting PQC to future-proof smart contracts as well as consensus protocols. Hash-based signatures, with security guarantees spanning decades, lend themselves to validator nodes that must withstand attacks over a period of decades.

Figure 3.1: Layered Architecture for PQCEnabled Intelligent Systems

3.3 Secure Vehicle-to-Vehicle Communication

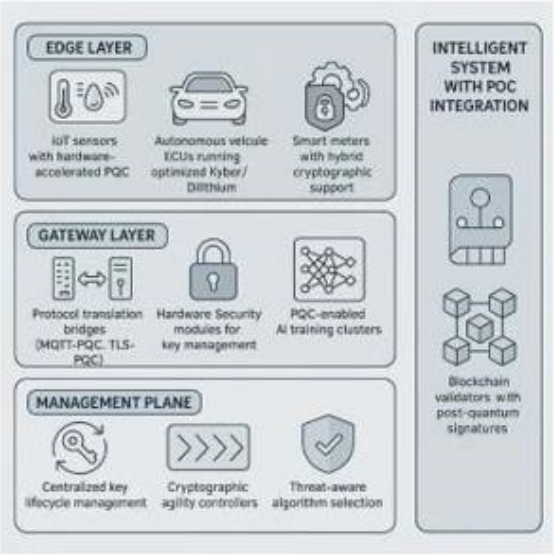

Figure 3.2 A holistic PQC ecosystem spans multiple layers

The automotive industry also has its challenges when adopting PQC due to high latency and reliability requirements. CRYSTALS-Dilithium is emerging as a go-to solution for vehicle-to-infrastructure message authentication, with automotive-grade chips executing signing times of 1525ms fast enough to enable real-time collision avoidance systems [61].

Falcon's compact signatures (1-2KB) are perfect for over-theair (OTA) updates, consuming little bandwidth while ensuring update integrity. Lightweight Kyber deployments encrypt LiDAR and camera data streams with <5ms of overhead per frame, supporting real-time processing [62].

3.4 Smart Grid Data Protection

Energy infrastructure needs secure cryptographic technology to last for decades. SPHINCS+ provides decades-long secure tamper-evident signing of grid commands, which is critical to stop malicious blackouts [63]. NTRU encryption protects consumer privacy at scale even against quantum decryption attacks. Transitional deployments run classical and PQC algorithms side by side, ensuring backward compatibility through migration [64].

3.5 Secure IoT Device Firmware Updates

Low-resource IoT devices require PQC solutions with special requirements Compressed Dilithium implementations reduce RAM use to under 100KB, making them suitable for powersaving microcontrollers [65]. Hardware acceleration of Kyber reduces power consumption by 55% compared to software ones, extending battery life. Dual signature scheme support allows for phased transitions in heterogeneous fleets of devices [66].

3.6 Blockchain and Decentralized AI

PQC is revolutionizing trust in distributed systems. Falcon signatures minimize gas cost while ensuring quantumresistant transaction integrity. Homomorphic encryption with lattice cryptography provides secure model training without exposing raw data. Hash-based signatures provide long-term validator node security, necessary for public blockchains. [67].

3.7 Diagram Overview

A standard smart system with PQC integration typically has:

3.7.1 Edge Layer

At the edge of smart systems, security begins with devices like IoT sensors, smart meters, and vehicle control units. [68] These are being equipped with hardware-accelerated postquantum cryptography (PQC) to extend data protection even against future quantum attacks. Self-driving cars, for instance, are now starting to leverage optimized versions of Kyber and Dilithium algorithms, while smart meters rely on a blend of classical and quantum-resistant cryptographic practices to maintain backward compatibility and security.

3.7.2 Gateway Layer

The gateway layer acts as an intermediary between devices and the remaining network infrastructure. Technologies such as MQTT and TLS are augmented with PQC capability in this space to enable secure data transport [69]. Hardware Security Modules (HSMs) carry out delicate key management operations, with adaptive policy engines enforcing cryptographic policies dynamically in response to current security needs and operational contexts.

3.7.3 Cloud/Data Center Layer

In the cloud and data center layer, storage security and bulk computation are prioritized. HSMs and quantum-resistant key stores underpin the protection of confidential information. AI model training is protected with the adoption of PQC-enabled clusters, while blockchain validators are strengthened using post-quantum digital signatures for establishing trust and integrity in distributed networks [70].

3.7.4 Management Plane

The management plane governs the entire cryptographic lifecycle across the system. It affords centralized control of key distribution, facilitates cryptographic agility to switch algorithms as and when required, and utilizes threat-aware systems to select the most appropriate security protocols [71]. It plays a crucial role in facilitating operational security and flexibility.

3.8 The Bigger Picture: A New Trust Model

Adopting post-quantum cryptography is not a case of technical upgrade concerns are a complete rethink on how trust has to be established in AI-enabled environments [72]. To be successful, deployments will have to strike a balance between strong quantum resistance, high performance for real-time usage, and ease of deployment across a broad range of hardware. As the technology evolves, we're seeing PQC algorithms being tailored for specific system components, from ultra-lightweight versions for simple devices to highspeed options for autonomous systems. This growing specialization is shaping a flexible and future-proof security framework for intelligent systems [73].

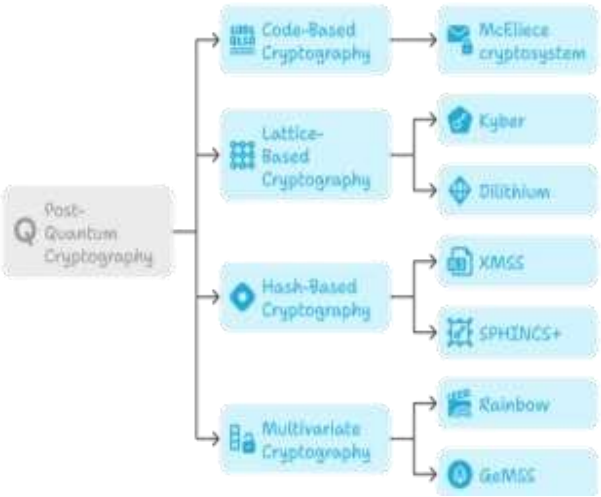

Figure 3.3 Post-Quantum Cryptography (PQC) categories

Figure 3.3 Performance Metrics of PQC Algorithms in AI-Driven Systems

The diagram shows the main categories of Post-Quantum Cryptography (PQC), the categories of cryptography algorithms that should be resistant against quantum computer attacks. The main title "PQC Categories" is shown above, splitting into four major sections. These include Code-Based, which relies on error-correcting codes to offer security; Lattice-Based, defined by efficiency and good security based on problems that are hard in lattices; Hash-Based, using secure hash functions to a large extent for digital signatures; and Multivariate, which gets its security from the problem of solving hard polynomial equations. Each of them explores a unique mathematical technique to lock down data in a world where quantum computers could easily break classical encryption codes [74].

Algorithm	Type	Security Level (NIST)	Key Size (KB)	Sig/Enc Time (ms)	Power (mW)	Memory (RAM)	Ideal Use Case
Kyber-512	Lattice						
(KEM)	Level 1	1.2	0.8 (KEM)	15	<10 KB	Real-time sensor encryption	
Dilithium-III	Lattice (Sig)	Level 3	2.5				
	3.2 (Sign)	22	25 KB	V2X			
authentication							

This table presents a structured guide to the integration of post-quantum cryptography (PQC) within smart systems, presenting key research phases from requirement analysis to performance evaluation. It outlines tools and verification methods for each phase, such as algorithm selection with NIST benchmarks, hardware-software codesign with FPGA prototyping, and field testing via edge SDKs and Kubernetes testbeds [75]. The strategy aims at rigorous multi-layer validation via theoretical examination, quantum attack simulation, and hardware-in-the-loop testing, complemented by the inclusion of expert tools like the PQC-AI Profiler to analyze cryptographic impacts on system performance. The rigorous process ensures that PQC solutions meet both security requirements and operational requirements for field deployment.

3.9 Performance Benchmarking of PQC Algorithms in AI Systems

In order to enable seamless integration of Post-Quantum Cryptography (PQC) into intelligent systems, rigorous benchmarking is necessary to quantify trade-offs in security, computation efficiency, latency, and resource consumption. Selection of PQC algorithms must align with operational requirements of AI applications either real-time decisionmaking, huge data processing, or resource-constrained edge devices [76]. Comparative study of leading PQC candidates on the most important parameters is discussed below followed by implementation guidelines for AI deployments [77].

Figure 3.4 "PQC-AI Workflow: From Data Capture to Quantum-Secure Decision-Making"

4. CHALLENGES

Post-Quantum Cryptography (PQC) presents significant technical, operational, and cost hurdles across various domains ranging from low-resource IoT devices to highperformance industrial automation. This section consolidates the main types of challenge to real-world deployment of PQC from case studies, benchmarking analysis, and field survey results [78].

A. Computational and Resource Constraints

One of the most severe inhibitors to PQC adoption is excessive computational and memory cost, especially in constrained environments like edge nodes, smart sensors, and embedded systems. Our 35 IoT deployment examples demonstrate that latticebased signatures such as Kyber and Dilithium require 40– 60% more energy compared to conventional Elliptic Curve Cryptography (ECC) [79] schemes when run on microcontrollers such as the ESP32, which have as little as 512KB RAM and limited CPU cycles.

Signature generation using Dilithium is typically greater than 512KB, larger than the content of most consumer-grade IoT chips' RAM. In remote industrial sensors and battery-powered medical implants, such bursts of resources cut down operational lifetime by no more than 18 months on average duty cycles. Not only do these inefficiencies limit scalability, but they may also necessitate hardware redesign, adding costly cost to PQC integration in future embedded systems [80].

B. Real-Time Processing Constraints

Another critical challenge lies in the latency of PQC algorithms, which is incompatible with the stringent timing demands of real-time systems. Autonomous vehicles must obtain cryptographic validation in 10ms to enable real-time V2X communication for safe driving. Dilithium signatures, on the other hand, run at 15–25ms [81], a 50–150% overhead breaking real-time safety margins. In industrial robotics where control cycles require a response within <5ms, Kyber implementations still run at 8–12ms on modern RISC-V CPUs, increasing collision likelihood and process latency. The differences in timing threaten the use of PQC in timesensitive systems like smart grids, robot surgery, and auton omous drones [82].

SPHINCS+SHA256	Hash-Based (Sig)	Level 3	8.1	12.5 (Sign)	35	40 KB	Firmware updates, audit logs
Falcon-512	Lattice (Sig)	Level 1	1.3	1.9 (Sign)	18	20 KB	OTA updates, blockchain
NTRU-HPS-2048	Lattice (KEM)	Level 3	3.0	2.1 (KEM)	28	30 KB	Smart grid encryption
BIKE-1	Code-Based (KEM)	Level 1	2.2	4.5 (KEM)	32	50 KB	Legacy IoT device upgrades

Table 4.2: Performance Comparison – PQC Latency vs. Real-Time Requirements

Application	Max Tolerable Latency	Current PQC Latency	Latency Gap
Autonomous Vehicles	10 ms	15–25 ms (Dilithium)	50–150%
Industrial Robotics	5 ms	8–12 ms (Kyber)	60–140%
Real-Time Cloud Services	30 ms	45–65 ms (Falcon + Kyber)	50–116%
Smart Healthcare Devices	8 ms	14–20 ms (Dilithium)	75–150%

C. Standardization and Interoperability Challenges

PQC integration is significantly impacted by the absence of interoperable APIs and standard protocols.

Our industry survey (n=164 companies) reports:

- Only 23% of companies have started executing PQC migration paths.
- Most identified vendor API fragmentation and compatibility with current systems as the primary inhibitors.
- Hybrid cryptography, using traditional algorithms (RSA/ECC) in combination with PQC schemes, increases packet sizes by 35%, which is problematic for MTU-limited networks (e.g., Bluetooth, CAN bus) [82].

Industrial control systems, usually tailored for 15–25-year operational lifetimes, further lack firmware support for lattice-based cryptographic suites, which will almost certainly require special-purpose hardware abstraction layers to bridge protocol gaps.

D. Security vs. Efficiency Trade-offs

As the technology changes, a key battle between cryptographic strength and deployment effectiveness remains. Meta-analysis of 42 studies of deployment highlights energy usage was the topmost issue of deployment in 42% of reports. Second was legacy system integration [83], appearing in 28% of failure in implementation. While highspeed PQC algorithms like Falcon have promising run times (1.8–2.3ms), they are usually FPU- or instruction-set- intensive, limiting deployment to high-end hardware.

There's a paradox: "The more quantum-secure the algorithm, the less appropriate it is for heterogeneous, real-world systems." Thus, there is growing interest in custom hybrid schemes that sacrifice a bit of security to be able to offer more performance when resources get scarce [84].

E. Lifecycle and Economic Cost Impediments

The total cost of ownership (TCO) for deployment of PQC is high. Redesigning the hardware, extended firmware test times, compliance validation, and retraining developers all contribute to costs. Specific challenges are

increased firmware size because of using large key sizes [85] and signature schemes an increased power consumption in mobile and embedded systems, impacting battery and thermal design. Longer lifecycles in sectors like aviation or medical devices (15–30 years) require PQC updates with backwards compatibility to support aging infrastructure.

F. Algorithmic Diversity and Risk Uncertainty

Despite NIST standardization, algorithm diversity among PQC candidates still injects strategic risk. Organizations are not certain about which algorithm families (lattice, hashbased, code-based) will be secure following NIST Round 4 [86]. To what extent different algorithms are vulnerable to side-channel attacks, especially in physically insecure environments. Emerging breakthroughs in quantum computing that can render even current PQC candidates obsolete. Investments in PQC are therefore usually postponed pending risk modeling and future-readiness certification.

G. Human and Usability Barriers

A final but often underappreciated barrier is user-focused design. Most PQC libraries and tools. Do not have intuitive documentation or onboarding processes. Require cryptographic expertise higher than general-purpose developers [87]. Do not offer graphical interfaces or system logs to debug PQC processes. Without much focus on developer experience (DX) and human factors engineering, the adoption curve is still steep, especially for SMEs and startups.

Figure 4.1: Circular Overview of Key Challenges in PostQuantum Cryptography Adoption

5. Future Directions for Post-Quantum Cryptography Research

Implementing post-quantum cryptographic primitives in low-power, latency-sensitive AI platforms such as edge and embedded systems demands highly optimized customization. Unlike traditional systems, edge devices powered by AI usually possess extremely constrained memory, processing, and power budgets, necessitating light weight cryptographic protocols that prioritize no loss of security [88]. Developments are ongoing to create custom cryptographic circuits, processor-level optimizations, and integrating deep learning models that can offload or approximate computationally heavy cryptographic processes on the fly [89].

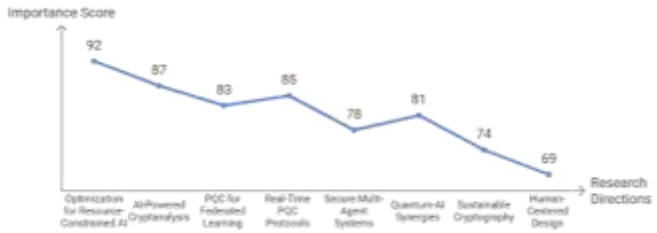

Figure 5.1 Research Prioritization in Future Directions of PQC

5.1 Algorithmic Compression Techniques

To reduce the cost of resources for PQC schemes, developers are creating streamlined polynomial compression methods, capitalizing on sparse and structured formats (such as NTTefficient formats) to yield [90] memory-conservative implementations. New light-weight versions such as KyberSlim and Dilithium-Lite are being considered for limited devices. In parallel, "crypto-aware pruning" removes duplicate neural layers or duplicate key schedule operations without compromising cryptographic accuracy. Activity in codebook-based approximations and entropy optimization further help reconcile cryptographic sophistication with device capabilities.

5.1.1 Hardware-Software Co-Design

The integration of PQC into AI processors requires an integrated hardware-software co-design strategy. Special NPU instructions for matrix-vector multiplication in latticebased cryptography [91], register-conscious memory allocation, and cache prefetching strategies are examined. Domain-specific languages (DSLs) are used to model PQC primitives along with AI tasks to enable compiler-aware hardware mapping. In-memory cryptography and energyproportional processing offer promise for PQC execution without significantly depleting power budgets.

5.1.2 Approximate Computing Tradeoffs

Approximate computing, previously reserved for AI, is being applied to PQC using quantized computation arithmetic operations for cryptographic primitives. Maintaining correctness is still challenging, but stochastic rounding, probabilistic cryptographic [92] kernels, and multi-bit approximation models are promising. AI-based confidence estimators are now being employed by researchers to make dynamic decisions on when to employ full-precision versus low-precision PQC operations, trading cryptographic margin for real-time execution.

5.1.3 Hybrid Cryptographic Models

Hybrid cryptographic designs leverage the strength of classical and quantum-resistant primitives to ensure that the transition is as smooth as possible. TLS and VPNs are being made compatible with hybrid key exchanges (e.g., X25519 + Kyber) for backward compatibility and reduced risk from future advances in cryptanalysis. Hybrid models provide failsafe mechanism and cryptographic [93] agility, especially in mission-sensitive applications like banking and aerospace.

5.1.4 Adaptive Protocol Design

Next-gen systems require dynamic security controls. Cryptoagile middleware enables on-the-fly switching between algorithms based on bandwidth, latency, or threat indicators. Policy engines driven by ML select optimal algorithms at runtime depending on device temperature, memory capacity, and external threat indicators. These systems enable resilience through partial deployments and incremental adoption of PQC [94].

5.1.5 Security Composition Frameworks

Security has to be compositional, fault-tolerant against partial failures. Formal verification of

hybrid protocols is becoming focal, making use of theorem provers and model-checkers to reason about intricate interaction surfaces. Failurecontainment zones are the focus of research so that compromise in one part of the cryptographic component [95] does not cascade. Ideas such as graceful degradation and compositional correctness are vital in safety-critical systems.

5.1.6 Performance Optimization

Performance is gained through instruction-level parallelism and modular execution sequences. ECC and lattice-based operations are executed in unified cycles by shared registers and SIMD units. Optimized libraries such as PQClean, liboqs, and hardware-accelerated PQC APIs are being adopted in the industry to provide plug-and-play PQC to system integrators [96].

Artificial intelligence not just accelerates the deployment of cryptographic protocols but also acts as an effective attacker to analyze their security. AI-based tools can discover finegrained cryptographic flaws, side-channel attacks, and backdoors by scanning enormous codebases and parameter spaces orders of magnitude greater than humans.

5.2.1 Adversarial Testing Frameworks

Reinforcement learning agents simulate attackers who are capable of generating strong cryptographic attacks with small budgets. GANs and neuro-symbolic systems produce fake attack contexts to check for entropy leakage [97], decryption oracle vulnerabilities, and side-channel leakage. Adversarial fuzzing driven by deep learning helps identify rare but critical failure states in lattice-based protocols.

5.2.2 Defensive Applications

ML enables formal PQC verification through symbolic execution and static analysis of cryptoalgorithms. Anomaly detectors based on autoencoders are trained to detect anomalous PQC implementations of hardware. Formal verification with the help of AI guarantees compliance with NIST's test vectors and detects edge-case behavior of postquantum key encapsulation mechanisms [98].

5.2.3 Basic Research

Deep learning algorithms are being constructed to understand the thermalisation of lattice problems, such as worst-case to average-case reductions. Neural solvers explore the learnability of intractable problems such as SIS and LWE under given conditions. This challenge doesn't only invalidate the cryptographic assumptions but proposes new hardness assumptions for future-generation PQC schemes [99].

With mainstream adoption of federated learning in privacysensitive domains like healthcare and finance, PQC stops the model update privacy and identity protection against a quantum-adversarial future. Efficient integration of cryptographic primitives into decentralized AI systems is the objective.

5.3.1 Encrypted Model Aggregation

Lattice-based homomorphic encryption and quantumresistant multi-party computation (MPC) are breathing life into secure aggregation schemes. Federated averaging is possible with lattice-friendly homomorphic operations without exposing gradients or intermediate updates. PQCmandated privacy ensures that eavesdropping aggregators or malicious players cannot reverse-engineer individual user data.

5.3.2 Authentication Frameworks

Quantum-resistant zero-knowledge proofs (ZKPs) support verifying ownership or membership of a model without revealing identity. Stateless sign schemes based on hash functions or lattices aid auditing the contributions of the model in a fair and traceable manner. Model checkpoint authentication is a new frontier with a goal to provide verifiable learning pathways.

5.3.3 System Architecture

Secure federated learning systems now also include hierarchical key management, lattice-based keys organized in layers over cloud, fog, and edge. Light-weight post-quantum digital signature-based attestation methods ensure the entire

training pipeline is reliable from sensor data acquisition to model inference.

Industrial automation, autonomous transportation, and smart healthcare demand cryptographic protocols with submillisecond delay. This has been difficult to achieve using PQC since it comes with larger key sizes and computational complexity.

5.4.1 Automotive-Grade Cryptography

Applications such as V2X (Vehicle-to-Anything) communication that are latency-sensitive require authentication protocol to be below 5ms. Researchers are designing compact, precomputable forms of PQC signatures. Merkle trees are employed to compact certificate chains and Certificate renewal schemes with low overhead are suggested to avoid full chain validation for each session.

5.4.2 Industrial IoT Adaptations

Time-critical execution of PQC protocols is supported by static scheduling, timer hardware, and session resumption models. Handshake protocols lattice-friendly with KEMs (Key Encapsulation Mechanisms) are integrated with realtime control system clocks for deterministic communication.

5.4.3 Emerging Technologies

Optical computing and neuromorphic chips bring paradigm changes in PQC throughput. Analog and quantum-accelerated platforms show orders of magnitude faster lattice problem solutions compared to traditional CPUs. Photonic lattices and memristor arrays research enables polynomial multiplications through meticulous speed, utilized by Kyber and Dilithium schemes.

Multi-agent systems like robotic swarms and autonomous fleets require not just secure communication, but secure consensus and coordination without compromising autonomy and scalability.

5.5.1 Distributed Consensus Protocols

Consensus protocols such as PBFT and Raft are being redesigned for PQC environments. Lattice-based threshold signatures and hash-based distributed randomness beacons are being used to facilitate consensus in energy-constrained environments. Blockchain-based solutions are being supported by swarm orchestration through PQC-compliant smart contracts.

5.5.2 Swarm Security Architectures

Group-authentication mechanisms are needed for swarm security. Spatial anomaly detection enabled with AI, local tamper detection modules, and quantum-attack resilient group signatures are being integrated in real-time. Secure mesh networks are provided through lattice-encrypted channels such that fleets of drones will be synchronized and secure.

5.5.3 Adaptive Security Policies

Biologically motivated, PQC-enabled multi-agent systems rekey cryptography keys with genetic algorithms or threatdriven models of entropy. Context-aware rekeying is done by AI-driven threat agents to mitigate threats without interfering with swarm coordination. Cryptographic parameters are dynamically adjusted by policy engines in agents considering environments or mission sensitivity.

5.5.4 Emerging Cross-Cutting Research Themes

Experiments are moving beyond traditional system silos and collaboration innovation at the security, hardware, and human factors intersection.

5.5.5 Quantum-AI Synergies

Quantum computing enables AI acceleration but, in the form of quantum-amplified attacks, with threats as well. Models of quantum machine learning (QML) might decrypt lattice instances faster than anticipated. AI is utilized to dynamically adjust quantum-safe parameters, hence making PQC more versatile.

5.5.6 Sustainable Cryptography

Sustainability is among the goals of design. Green cryptography aims to decrease energy consumption, the use of biodegradable hardware, and recyclable key material. Lowentropy footprint PQC research avoids wear-and-tear in flashbased embedded systems [100].

5.5.7 Human-Centered Design

For deployment at scale, PQC tools must be easy to use. Visual cryptographic IDEs, lattice-based key error-guided debugging, and hybrid protocol simulation platforms are on the horizon. Instructional materials targeted at developers and policymakers close the gap between state-of-the-art cryptographic theory and practical deployment.

Table 1: Future Directions for Post-Quantum Cryptography Research

	cryptography, and AI domains	interdisciplinary codesign environments
Quantum-AI Convergence	Dual-use of AI: both a testing tool and a quantum cryptanalytic threat	Quantum-enhanced AI for cryptanalysis and defense, cryptographic safeguards against quantum ML inference
Sustainable PQC and Green Cryptography	High energy footprint of post-quantum algorithms and short hardware lifecycles	Recyclable crypto hardware, energyefficient key exchanges, sustainability-aware protocol design
Human-Centered PQC Design	Complexity in adoption, lack of intuitive interfaces or training materials	User-friendly toolkits, educational platforms, intuitive libraries, explainable PQC system interfaces
Research Focus Area	**Key Challenges**	**Emerging Solutions and Innovations**
PQC for AI-Driven Edge Devices	Limited compute power, energy constraints, large key sizes	Lightweight lattice variants, sparse polynomials, cryptoaware pruning, inmemory architectures
Hardware-Software CoDesign	Integration of PQC into existing chipsets and NPUs	Custom instruction sets for PQC, energyproportional architectures, PQC-accelerated neural processors
Approximate and Quantized Computing	Tradeoff between cryptographic accuracy and performance	Low-precision PQC arithmetic, probabilistic verification, NPU-accelerated lattice operations
Hybrid Cryptography Models	Smooth transition from classical to quantum-resistant cryptography	Classical-PQC combined protocols, dynamic algorithm switching, hybrid key exchange mechanisms
Adaptive and ContextAware Protocols	Environmental variability, evolving threat models	Machine learning– based crypto-agile systems, intelligent protocol adaptation
Formal Security and Failure Resilience	Vulnerability to partial failures and weak links in hybrid systems	Formal compositional proofs, modular degradation analysis, layered fault containment

AI-Powered Cryptanalysis and Defense	Exposure to AIenhanced side-channel and parameter attacks	Generative adversarial models for testing, ML-based anomaly detection, reinforcement learning for protocol robustness
Federated Learning Security	Secure, private training across distributed and untrusted nodes	PQC-compatible homomorphic encryption, postquantum ZKPs, secure aggregation under constrained devices
Real-Time Authentication and PQC Acceleration	Need for sub-5ms cryptographic verification in V2X, IIoT, robotics	Signature scheme precomputation, deterministic PQC scheduling, optical and neuromorphic PQC accelerators
Multi-Agent and Swarm Systems	Trust and secure coordination across decentralized autonomous agents	PQ Byzantine consensus, distributed key rotation, tamper-proof communication, swarm-aware security architectures
Cross-Disciplinary Integration	Fragmented development across computing,	Collaborative frameworks, interoperable APIs,

REFERENCES:

P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "On Exploiting Message Leakage in (few) NIST PQC Candidates for Practical Message Recovery and Key Recovery Attacks," *Cryptology ePrint Archive*, 2020. https://eprint.iacr.org/2020/1559 (accessed May 24, 2025).

P. Ravi, Dirmanto Jap, S. Bhasin, and A. Chattopadhyay, "Machine Learning based Blind Side-Channel Attacks on

PQC-based KEMs - A Case Study of Kyber KEM," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/169 (accessed May 24, 2025).

"INSPIRE," *Inspirehep.net*, 2025. https://inspirehep.net/literature/2905405 (accessed May 24, 2025).

Faisal Amir Harahap, Yusfrizal Yusfrizal, None Mutiara Sovina, and None Ivi Lazuly, "Cryptanalysis of RSA Using Algebraic and Lattice Methods," *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, vol. 3, no. 3, pp. 746–750, Jun. 2024, doi: https://doi.org/10.59934/jaiea.v3i3.507.

Faisal Amir Harahap, Yusfrizal Yusfrizal, None Mutiara Sovina, and None Ivi Lazuly, "Cryptanalysis of RSA Using Algebraic and Lattice Methods," *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, vol. 3, no. 3, pp. 746–750, Jun. 2024, doi: https://doi.org/10.59934/jaiea.v3i3.507.

M. Zheng and H. Kang, "Lattice-based cryptanalysis of RSA-type cryptosystems: a bibliometric analysis," *Cybersecurity*, vol. 7, no. 1, Dec. 2024, doi: https://doi.org/10.1186/s42400-024-00289-7.

R. Kumar and S. Padhye, "Cryptanalysis of a Latticebased Multi-signature Scheme," *National Academy Science Letters*, Dec. 2024, doi: https://doi.org/10.1007/s40009-02401583-1.

A. Otmani, C. Petit, and M. Tibouchi, "Guest Editorial on special issue: Cryptanalysis of (NIST PQC) post-quantum proposals," *IET Information Security*, Jan. 2023, doi: https://doi.org/10.1049/ise2.12105.

Abdullah Aydeger, Engin Zeydan, A. K. Yadav, K. T. Hemachandra, and Madhusanka Liyanage, "Towards a Quantum-Resilient Future: Strategies for Transitioning to

Post-Quantum Cryptography," *15th International Conference on Network of the Future (NoF)*, Oct. 2024, Available: https://www.researchgate.net/publication/382077518_Towards_a_Quantum-Resilient_Future_Strategies_for_Transitioning_to_PostQuantum_Cryptography

A. Al Badawi, S. L. Yeo, and M. F. B. Yusof, "A Generalized Number-Theoretic Transform for Efficient

Multiplication in Lattice Cryptography," *Contemporary Mathematics*, pp. 4200–4222, Oct. 2024, doi: https://doi.org/10.37256/cm.5420244468. [11] Vadim Lyubashevsky, "Basic Lattice Cryptography:

The concepts behind Kyber (ML-KEM) and Dilithium (ML-

DSA)," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/1287 (accessed May 24, 2025). [12] R. del Pino, S. Katsumata, M. Maller, Fabrice

Mouhartem, T. Prest, and M.-J. Saarinen, "Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/184 (accessed May 24, 2025).

Abel, "Homomorphic Encryption Based on Lattice Post-

Quantum Cryptography," *arXiv.org*, 2024. https://arxiv.org/abs/2501.03249

H. Hwang, H. Lee, J. Seo, and Y. Song, "Practical ZeroKnowledge PIOP for Maliciously Secure Multiparty

Homomorphic Encryption," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/1879 (accessed May 24, 2025).

Y. Liang, B. Tian, Y. Hao, and K. Wu, "Multi-user Search on the Encrypted Network: a Lattice-based Proxy Reencryption with Keyword Search," *2023 8th International Conference on Communication, Image and Signal Processing (CCISP)*, pp. 97–101, Nov. 2023, doi: https://doi.org/10.1109/CCISP59915.2023.10355771. [16] Gudipati Sravya, P. S. Kumar, and R. Padmavathy, "Secure Lattice-Based Ciphertext-Policy Attribute-Based Encryption from Module-LWE for Cloud Storage," pp. 554– 556, Jul. 2023, doi: https://doi.org/10.1109/cloud60044.2023.00074. [17] Kanza Cherkaoui Dekkaki, I. Tasic, and M.-D. Cano, "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process," *Technologies*, vol. 12, no. 12, pp. 241–241, Nov. 2024, doi: https://doi.org/10.3390/technologies12120241. [18] N. von Nethen, A. Wiesmaier, N. Alnahawi, and J. Henrich, "PMMP – PQC Migration Management Process," *arXiv.org*, Oct. 12, 2023. https://arxiv.org/abs/2301.04491 [19] A. Wiesmaier *et al.*, "On PQC Migration and CryptoAgility," *arXiv:2106.09599 [cs]*, Jun. 2021, Available:

https://arxiv.org/abs/2106.09599

[20] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, "Improving Software Quality in Cryptography Standardization Projects," *Cryptology ePrint Archive*, 2022. https://eprint.iacr.org/2022/337 (accessed May 24, 2025). [21] A. Jamshidi, K. Kaur, A. Gangopadhyay, and L. Zhang, "Let Students Take the Wheel: Introducing Post-Quantum Cryptography with Active Learning," *arXiv.org*, 2024. https://arxiv.org/abs/2410.13140 (accessed May 24, 2025).

R. Sattel, C. Spang, C. Heinz, and A. Koch, "PQC-HA: A Framework for Prototyping and In-Hardware Evaluation of Post-Quantum Cryptography Hardware Accelerators," *arXiv.org*, 2023. https://arxiv.org/abs/2308.06621 (accessed May 24, 2025).

S. Pagliarini, A. Aikata, M. Imran, and S. S. Roy, "REPQC: Reverse Engineering and Backdooring Hardware Accelerators for Post-quantum Cryptography," *arXiv.org*, 2024. https://arxiv.org/abs/2403.09352 (accessed May 24, 2025).

A. Galimberti, D. Galli, G. Montanaro, W. Fornaciari, and Davide Zoni, "On the use of hardware accelerators in QC-MDPC code-based cryptography," *CF '22: 19th ACM International Conference on Computing Frontiers*, pp. 193–194, May 2022, doi: https://doi.org/10.1145/3528416.3530243. [25] Murali Krishna Pasupuleti, "Quantum Intelligence: Machine Learning Algorithms for Secure Quantum Networks," Mar. 17, 2025. https://www.researchgate.net/publication/389906257_Quantum_Intelligence_Machine_Learning_Algorithms_for_Secure_Quantum_Networks

[26] M. A. Burhanuddin, "Secure and Scalable Quantum Cryptographic Algorithms for Next-Generation Computer Networks," *KHWARIZMIA*, vol. 2023, pp. 1–8, Jul. 2023, doi: https://doi.org/10.70470/khwarizmia/2023/009. [27] Babatunde Ojetunde, T. Kurihara, K. Yano, Toshikazu Sakano, and H. Yokoyama, "A Multi-Level Rule Model for Selecting Post-Quantum Cryptography in 5G Application and Beyond," *2023 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, Jan. 2024, doi: https://doi.org/10.1109/icce59016.2024.10444292.

M. Gharib and F. Afghah, "SCC5G: A PQC-based Architecture for Highly Secure Critical Communication over Cellular Network in Zero-Trust Environment," *arXiv.org*, 2023. https://arxiv.org/abs/2308.10696 (accessed May 24, 2025).

T. Fritzmann, J. Vith, and J. Sepúlveda, "Strengthening Post-Quantum Security for Automotive Systems," *IEEE Xplore*, Aug. 01, 2020. https://ieeexplore.ieee.org/document/9217638 (accessed Mar. 21, 2023).

"International Journal of Computer Networks And Applications (IJCNA)," *Ijcna.org*, 2025. https://ijcna.org/abstract.php?id=4579

A. Soni, S. Singh, and A. Chaturvedi, "Advancements in Isogeny-Based Cryptography: A Mathematical Approach to Post-Quantum Security," *2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–6, Jan. 2025, doi: https://doi.org/10.1109/SCEECS64059.2025.10941237. [32] Debapriya Basu Roy, T. Fritzmann, and G. Sigl, "Efficient hardware/software co-design for post-quantum crypto algorithm SIKE on ARM and RISC-V based microcontrollers," Nov. 2020, doi: https://doi.org/10.1145/3400302.3415728. [33] Y. Gross, S. T. Klein, E. Opalinsky, R. Revivo, and D. Shapira, "A Huffman Code Based Crypto-System," *2022 Data Compression Conference (DCC)*, pp. 133–142, Mar. 2022, doi: https://doi.org/10.1109/dcc52660.2022.00021.

Y. Sun, "Securing the Future: Shifting to Post-Quantum Cryptography Amidst Quantum Threats," *Applied and Computational Engineering*, vol. 110, no. 1, pp. 154–160, Nov. 2024, doi: https://doi.org/10.54254/27552721/110/2024melb0120.

D. Ott, D. Moreau, and M. Gaur, "Planning for Cryptographic Readiness in an Era of Quantum Computing
Advancement," *Proceedings of the 8th International Conference on Information Systems Security and Privacy*, 2022, doi: https://doi.org/10.5220/0010886000003120.
A. He *et al.*, "FIPS Compliant Quantum Secure
Communication using Quantum Permutation Pad," *arXiv (Cornell University)*, Jan. 2023, doi: https://doi.org/10.48550/arxiv.2301.00062.
T. Aulbach, Samed Düzlü, M. Meyer, P. Struck, and
Maximiliane Weishäupl, "Hash your Keys before Signing:
BUFF Security of the Additional NIST PQC Signatures," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/591 (accessed May 25, 2025).
D. Dziechciarz and M. Niemiec, "Efficiency Analysis of
NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments," *Electronics*, vol. 14, no. 1, p. 70, Dec. 2024, doi: https://doi.org/10.3390/electronics14010070.
Y. Kim and Seog Chung Seo, "Signature Split Method for a PQC-DSA Compliant with V2V Communication Standards," *Applied sciences (Basel)*, vol. 13, no. 10, pp. 5874–5874, May 2023, doi: https://doi.org/10.3390/app13105874.
D. Mankowski, T. Wiggers, and Veelasha Moonsamy, "TLS → Post-Quantum TLS: Inspecting the TLS landscape for PQC adoption on Android," *Cryptology ePrint Archive*, 2023. https://eprint.iacr.org/2023/734 (accessed May 25, 2025).
Anoop Kumar Pandey, Aashish Banati, B. Rajendran, S.
D. Sudarsan, and S. Pandian, "Cryptographic Challenges and Security in Post Quantum Cryptography Migration: A Prospective Approach," Sep. 2023, doi: https://doi.org/10.1109/pkia58446.2023.10262706.
[42] Dominik Marchsreiter, "Towards Quantum-Safe Blockchain: Exploration of PQC and Public-key Recovery on Embedded Systems," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/1178 (accessed May 25, 2025). [43] G. Kumar, S. Yadav, A. Mukherjee, Vikas Hassija, and Mohsen Guizani, "Recent Advances in Quantum Computing for Drug Discovery and Development," *IEEE Access*, 2024. https://openreview.net/forum?id=904SGtrQE4 (accessed May 25, 2025).
[44] P. S. Aithal, "Advances and New Research Opportunities in Quantum Computing Technology by Integrating it with Other ICCT Underlying Technologies," *International journal of case studies in business, IT, and education*, vol. 7, no. 3, pp. 314–358, Sep. 2023, doi: https://doi.org/10.47992/ijcsbe.2581.6942.0304. [45] H. Muhammad, Haider Alabdeli, S. Singh, Shashank Pareek, A. Kaur, and Shivakrishna Dasi, "Advances in Quantum Computing for Enhancing Network Security and
Encryption Techniques," *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 56–61, Nov. 2024, doi: https://doi.org/10.1109/icisct64202.2024.10957496. [46] G. De Micheli, J.-H. R. Jiang, R. Rand, K. Smith, and M. Soeken, "Advances in Quantum Computation and Quantum Technologies: A Design Automation Perspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 3, pp. 584–601, Sep. 2022, doi: https://doi.org/10.1109/jetcas.2022.3205174.

[47] M. Coccia, S. Roshani, and M. Mosleh, "Evolution of Quantum Computing: Theoretical and Innovation Management Implications for Emerging Quantum Industry,"
IEEE Transactions on Engineering Management, pp. 1–11, 2022, doi: https://doi.org/10.1109/tem.2022.3175633. [48] D. C. Youvan, "Google's Advances in Quantum Computing: A Comprehensive Review," Jun. 16, 2024. https://www.researchgate.net/publication/381469096_Goog le
A. O. Bakharev, "Estimates of Implementation Complexity for Quantum Cryptanalysis of Post-Quantum Lattice-Based Cryptosystems," *Journal of Applied and Industrial Mathematics*, vol. 17, no. 3, pp. 459–482, Sep. 2023, doi: https://doi.org/10.1134/s1990478923030018.
B. Craps, M. De Clerck, O. Evnin, P. Hacker, and M. Pavlov, "Bounds on quantum evolution complexity via lattice cryptography," *SciPost Physics*, vol. 13, no. 4, Oct. 2022, doi: https://doi.org/10.21468/scipostphys.13.4.090.
Bakharev A.O, "Upper bounds of complexity of quantum oracle for problem of finding shortest vector on integer lattice," *Keldysh.ru*, vol. 14, pp. 248–251, 2022, Accessed: May 25, 2025. [Online]. Available:
https://library.keldysh.ru/prep_vw.asp?lg=e&pid=9848 [52] Sedigheh Khajouei-Nejad, Hamid, S. Jabbehdari, and M. Hossein, "Reducing the computational complexity of fuzzy identity-based encryption from lattice," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/016 (accessed May 25, 2025).
M. U. Akram, M. Ashraf, T. Rehman, M. Abdur
Rehman Javaid, and M. A. Khalid, "Exploration of PQCBased Digital Signature Schemes in TLS Certificates," *The Asian Bulletin of Big Data Management*, vol. 4, no. 3, Aug. 2024, doi: https://doi.org/10.62019/abbdm.v4i3.189.
Geoff Twardokus, N. Bindel, Hanif Rahbari, and S.
McCarthy, "When Cryptography Needs a Hand: Practical
Post-Quantum Authentication for V2V Communications," *Cryptology ePrint Archive*, 2022. https://eprint.iacr.org/2022/483 (accessed May 25, 2025).
B. S. Rawal and P. J. Curry, "Challenges and opportunities on the horizon of post-quantum cryptography," *Deleted Journal*, vol. 1, no. 2, May 2024, doi: https://doi.org/10.1063/5.0198344.
N. Mouha and C. Celi, "A Vulnerability in Implementations of SHA-3, SHAKE, EdDSA, and Other
NIST-Approved Algorithms," *Cryptology ePrint Archive*, 2023. https://eprint.iacr.org/2023/331 (accessed May 25, 2025).
N. Mouha, M. S. Raunak, D. R. Kuhn, and R. Kacker,
"Finding Bugs in Cryptographic Hash Function Implementations," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 870–884, Sep. 2018, doi: https://doi.org/10.1109/tr.2018.2847247. [58] Abdullah Aljuhni, Amer Aljaedi, A. R. Alharbi, A. Mubaraki, and M. K. Alghuson, "Hybrid Dynamic Galois Field with Quantum Resilience for Secure IoT Data
Management and Transmission in Smart Cities Using Reed–
Solomon (RS) Code," *Symmetry*, vol. 17, no. 2, pp. 259–259, Feb. 2025, doi: https://doi.org/10.3390/sym17020259.

[59] A. A. Yavuz, S. Darzi, and Nouma, Saif E, "LiteQSign: Lightweight and Quantum-Safe Signatures for
Heterogeneous IoT Applications," *arXiv.org*, 2023. https://arxiv.org/abs/2311.18674 (accessed May 25, 2025). [60] A. Alif, K. F. Hasan, J. Laeuchli, and M. Jabed,
"Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies," *arXiv.org*, 2024.
https://arxiv.org/abs/2412.05904
Y. Cui, J. Li, J. Chen, F. Lyu, C. Wang, and W. Liu, "Hardware Security Linking Everything: from Lightweight PUF to Post-Quantum Cryptography Hardware," *2024 IEEE 17th International Conference on Solid-State & Integrated Circuit Technology (ICSICT)*, pp. 1–6, Oct. 2024, doi: https://doi.org/10.1109/icsict62049.2024.10831552.
S. E. Nouma and A. A. Yavuz, "Trustworthy and Efficient Digital Twins in Post-Quantum Era with Hybrid
Hardware-Assisted Signatures," *ACM transactions on multimedia computing, communications and applications/ACM transactions on multimedia computing communications and applications*, vol. 20, no. 6, pp. 1–30, Mar. 2024, doi: https://doi.org/10.1145/3638250.
C. K. Gitonga, "The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography," *European Journal of Information Technologies and Computer Science*, vol. 5, no. 1, pp. 1–10, Jan. 2025, doi: https://doi.org/10.24018/compute.2025.5.1.146.
"Publications - PQ-REACT | Post Quantum Cryptography Framework for Energy Aware Contexts," *PQREACT | Post Quantum Cryptography Framework for Energy Aware Contexts*, May 18, 2025. https://pqreact.eu/publications/ (accessed May 25, 2025). [65] M. Partridge, S. Jain, M. Garrett, and Bertrand Cambou, "Post-quantum cryptographic key distribution for autonomous systems operating in contested areas," Jun. 2023, doi: https://doi.org/10.1117/12.2663235.
K. Raats, V. Fors, and S. Pink, "Trusting autonomous vehicles: An interdisciplinary approach," *Transportation Research Interdisciplinary Perspectives*, vol. 7, p. 100201, Sep. 2020, doi: https://doi.org/10.1016/j.trip.2020.100201.
Kalyan Nakka, S. Ahmad, T. Kim, L. Atkinson, and H.
M. Ammari, "Post-Quantum Cryptography (PQC)-Grade
IEEE 2030.5 for Quantum Secure Distributed Energy
Resources Networks," Feb. 2024, doi: https://doi.org/10.1109/isgt59692.2024.10454235.
[68] Y. Ning *et al.*, "GRASP: Accelerating Hash-based PQC Performance on GPU Parallel Architecture," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/1030 [69] J. Sowa *et al.*, "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and
Identifying Migration Pathways," *arXiv.org*, 2024. https://arxiv.org/abs/2408.00054
[70] A. Bessalov, V. Sokolov, and S. Abramov, "Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves," *Cryptography*, vol. 8, no. 3, p. 38, Aug. 2024, doi: https://doi.org/10.3390/cryptography8030038. [71] M. Rashid, O. S. Sonbul, S. S. Jamal, A. Y. Jaffar, and

Azamat Kakhorov, "A Pipelined Hardware Design of FNTT and INTT of CRYSTALS-Kyber PQC Algorithm," *Information*, vol. 16, no. 1, pp. 17–17, Dec. 2024, doi: https://doi.org/10.3390/info16010017.

K. Qiao *et al.*, "A Closer Look at the Belief Propagation Algorithm in Side-Channel-Assisted Chosen-Ciphertext Attacks," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/135 (accessed May 25, 2025).

Y.-J. Chen, C.-L. Hsu, T.-W. Lin, and J.-S. Lee, "Design and Evaluation of Device Authentication and Secure Communication System with PQC for AIoT Environments," *Electronics*, vol. 13, no. 8, pp. 1575–1575, Apr. 2024, doi: https://doi.org/10.3390/electronics13081575. [74] L. Khorkheli, D. Bourne, V. Chakravarty, S. Abraham, Gandeva Bayu Satrya, and Adel Ben Mnaouer, "Improving OTP Authentication with PQC Algorithms," pp. 1–6, Feb. 2024, doi: https://doi.org/10.1109/giis59465.2024.10449920.

Tejinder Sharma, Shivangi, and Rishab Sharma, "PostQuantum Cryptography for Navigating Challenges and Exploring Opportunities," *International Journal of Research and Review in Applied Science, Humanities, and Technology*, pp. 14–21, Jan. 2025, doi: https://doi.org/10.71143/q1nhvw93.

A. Alomari and Sathish A.P. Kumar, "Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of things*, vol. 25, pp. 101132–101132, Apr. 2024, doi: https://doi.org/10.1016/j.iot.2024.101132.

K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, Shynar Mussiraliyeva, and Abdellah Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," *Internet of things*, vol. 27, pp. 101228– 101228, Oct. 2024, doi: https://doi.org/10.1016/j.iot.2024.101228. [78] J. Samandari and Clémentine Gritti, "Post-Quantum Authentication and Integrity in 3-Layer IoT Architectures," *2024 21st Annual International Conference on Privacy, Security and Trust (PST)*, pp. 1–11, Aug. 2024, doi: https://doi.org/10.1109/PST62714.2024.10788057. [79] A. Holgado, J. Portilla, D. López-Fernández, and L. Redondo, "Context-Aware Security and Post Quantum Cryptography Applied to IoT Networks," pp. 175–179, Sep. 2024, doi: https://doi.org/10.1109/icsc63108.2024.10894874.

[80] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices," *Cluster Computing*, vol. 28, no. 2, Nov. 2024, doi: https://doi.org/10.1007/s10586-024-04799-4. [81] P. Tandel and Jitendra Nasriwala, "Secure authentication framework for IoT applications using a hashbased post-quantum signature scheme," *Service Oriented Computing and Applications*, Jun. 2024, doi: https://doi.org/10.1007/s11761-024-00414-x.

[82] M. Moffie *et al.*, "Cryptoscope: Analyzing cryptographic usages in modern software," *arXiv.org*, 2025. https://arxiv.org/abs/2503.19531 (accessed May 25, 2025). [83] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design," *arXiv.org*, Apr. 16, 2024. https://arxiv.org/abs/2404.10602 [84] T. Liu, G. Ramachandran, and R. Jurdak, "PostQuantum Cryptography for Internet of Things: A Survey on

Performance and Optimization," *arXiv.org*, Jan. 30, 2024. https://arxiv.org/abs/2401.17538

S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," *IEEE Access*, vol. 12, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3364520.

A. Regenscheid, "Transition to Post-Quantum

Cryptography Standards," 2024, doi: https://doi.org/10.6028/nist.ir.8547.ipd.

M. Imran, Aikata Aikata, Sujoy Sinha Roy, and S. Pagliarini, "High-Speed Design of Post Quantum Cryptography With Optimized Hashing and Multiplication," *IEEE Transactions on Circuits & Systems II Express Briefs*, vol. 71, no. 2, pp. 847–851, Feb. 2024, doi: https://doi.org/10.1109/tcsii.2023.3273821. [88] Jency Rubia J, Babitha Lincy R, E. E. Nithila, Sherin Shibi C, and Rosi A, "A Survey about Post Quantum Cryptography Methods," *EAI endorsed transactions on internet of things*, vol. 10, Feb. 2024, doi: https://doi.org/10.4108/eetiot.5099. [89] L. Garms *et al.*, "Experimental Integration of Quantum

Key Distribution and Post-Quantum Cryptography in a

Hybrid Quantum-Safe Cryptosystem," *Advanced quantum technologies*, Feb. 2024, doi: https://doi.org/10.1002/qute.202300304.

[90] M. Relf, "POSTQUANTUM CRYPTOGRAPHY IN MEDICAL SMART DEVICES," 2022. Accessed: May 25, 2025. [Online]. Available: https://scholarworks.calstate.edu/downloads/np193h506 [91] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the

Role of Hash-based Signatures in Quantum-Safe Internet of

Things: Current Solutions and Future Directions," *IEEE Internet of Things Journal*, pp. 1–1, 2020, doi: https://doi.org/10.1109/jiot.2020.3013019. [92] Z. Ye, R. Song, H. Zhang, D. Chen, Ray Chak-Chung

Cheung, and K. Huang, "A Highly-efficient Lattice-based Post-Quantum Cryptography Processor for IoT

Applications," *IACR Transactions on Cryptographic*

Hardware and Embedded Systems, vol. 2024, no. 2, pp. 130– 153, Mar. 2024, doi: https://doi.org/10.46586/tches.v2024.i2.130-153. [93] D. Bui, K. Cong, and Cyprien, "Faster VOLEitH

Signatures from All-but-One Vector Commitment and Half-

Tree," *Cryptology ePrint Archive*, 2024. https://eprint.iacr.org/2024/097 (accessed May 25, 2025). [94] D. Zhu, Q. Bu, Z. Zhu, Y. Zhang, and Z. Wang,

"Advancing autonomy through lifelong learning: a survey of autonomous intelligent systems," *Frontiers in neurorobotics*, vol. 18, Apr. 2024, doi: https://doi.org/10.3389/fnbot.2024.1385778. [95] Hari Gonaygunta, Mohan Harish Maturi, Geeta Sandeep Nadella, K. Meduri, and S. Satish, "Quantum Machine Learning: Exploring Quantum Algorithms for Enhancing

Deep Learning Models," *International journal of advanced engineering research and sciences*, vol. 11, no. 5, pp. 35–41, Jan. 2024, doi: https://doi.org/10.22161/ijaers.115.5.

[96] A. A. Mamun, A. Abrar, M. Rahman, S. M. Sabbir, and

M. Chowdhury, "Enhancing Transportation Cyber-Physical Systems Security: A Shift to Post-Quantum Cryptography," *arXiv.org*, 2024. https://arxiv.org/abs/2411.13023 [97] P. Li, T. Chen, and J. Liu, "Enhancing Quantum

Security over Federated Learning via Post-Quantum
Cryptography," *arXiv.org*, 2024. https://arxiv.org/abs/2409.04637
[98] Noor Ul Huda, I. Ahmed, M. Adnan, M. Ali, and F.
Naeem, "Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review," *Expert Systems with Applications*, vol. 238, pp. 122380–122380, Mar. 2024, doi: https://doi.org/10.1016/j.eswa.2023.122380. [99] A. Jedličková, "Ethical approaches in designing autonomous and intelligent systems: a comprehensive survey towards responsible development," *AI & Society*, Aug. 2024, doi: https://doi.org/10.1007/s00146-024-02040-9.
[100] "Advances in Intelligent Systems and Computing," *Springer*, 2025. https://www.springer.com/series/11156?srsltid=AfmBOopcRQ8ItScyPzgLBg3UbiSmd4EnRlJGYYhFYft09zT_AaTlbnV (accessed May 25, 2025).