International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 07-03-2026, Accepted: 07-04-2026, Published: 22-04-2026
Volume 10, Issue 2, 2026, Page No. 57-63

Impact of Quantum Computing on symmetric encryption algorithms

Smita Ketan Hadawale, Bhavarth Prashant Pathare, Arpit Tiwari, Aditya Pandey
Department of Computer Science, Pillai College of Arts, Commerce and Science (Empowered Autonomous), Panvel, Navi Mumbai, Maharashtra, India

Abstract
Quantum computing progress is now fast enough that the security community cannot afford to wait. Public-key schemes face complete failure under Shor's factoring algorithm, while symmetric ciphers take a more moderate hit from Grover's search speedup, which cuts effective key length in half. Upgrading to 256-bit symmetric keys helps, but it does not address the Harvest-Now-Decrypt-Later (HNDL) threat, where adversaries collect encrypted data today and decrypt it retroactively once a quantum machine is available. This paper introduces
AQIS (Adaptive Quantum-Immune Symmetric Encryption), a new three-layer cryptographic framework. The data layer uses AES-256-GCM or AEGIS-256. The key layer uses CRYSTALS-Kyber (FIPS 203) to deliver session keys in a quantum-safe manner. The protocol layer introduces a novel Automated Key Rotation Protocol (AKRP) that refreshes session keys after a defined block count using HKDF-SHA512, closing the long-running key exposure window. AQIS-Full achieves 192-bit post-quantum security and 9.8+ Gbps throughput. AQIS-Lite is optimized for ARM Cortex-M4 IoT hardware. The framework is fully aligned with NIST FIPS 203, 204 and 205, and includes a four-phase organizational migration roadmap.

Keywords: Post-quantum cryptography, AES-256, grover algorithm, CRYSTALS-Kyber, AQIS, AKRP, HNDL, AEGIS-256, HKDF-SHA512, IoT Security, NIST PQC, symmetric encryption

Introduction

For over four decades, modern digital security has relied on the belief that certain mathematical problems are too difficult to solve quickly, even for powerful computers. Public-key systems such as RSA and elliptic curve cryptography depend on this assumption. However, advances in quantum computing threaten to break these protections.

Two major quantum algorithms cause concern. Shor's algorithm can efficiently solve the problems underlying RSA and Diffie-Hellman, potentially rendering them insecure. Grover's algorithm accelerates brute-force attacks, effectively reducing the strength of symmetric encryption keys by half. As a result, AES-128 becomes weak, while AES-256 remains comparatively secure.

Existing countermeasures are still incomplete. Attackers can store encrypted data today and decrypt it later when quantum computers become available — a threat known as Harvest-Now-Decrypt-Later (HNDL). Long-lived session keys further increase exposure.

To address these risks, this paper proposes AQIS, a framework that combines a multi-layer design, automated key rotation based on usage, and mechanisms intended to minimize future quantum decryption threats.

Background and Related Work

1. Symmetric Ciphers in Use Today

Symmetric ciphers share one key for both encryption and decryption, enabling the throughput needed to protect gigabytes of traffic per second. AES, standardized in NIST FIPS 197 following a five-year public competition (6), operates on 128-bit blocks through 10, 12, or 14 substitution-permutation rounds depending on key size. Hardware AES-NI instructions in modern processors push AES-256 throughput above 10 Gbps on a single core. ChaCha20-256 (9) uses an add-rotate-XOR structure on a 256-bit key, runs in constant time to prevent timing side-channels, and is a mandatory cipher suite in TLS 1.3 (12). AEGIS-256 (10) chains five AES state registers in a feedback design, offering tighter multi-key security bounds than GCM mode and benchmarked above 16 Gbps on AVX-512 hardware.

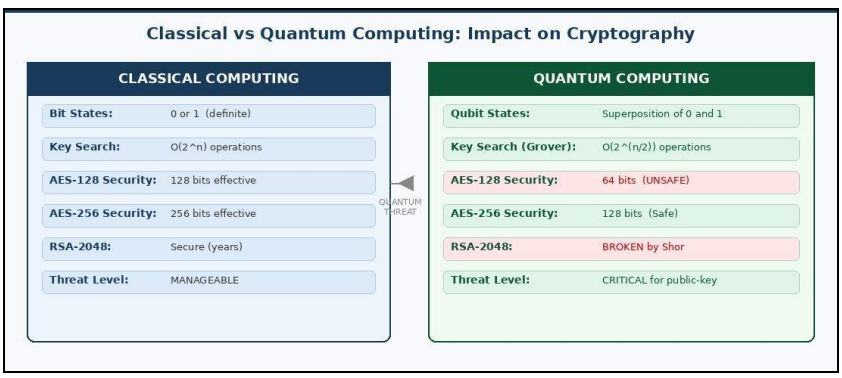

Fig 1: Classical versus quantum computing impact on cryptographic security. Shor's algorithm fully breaks RSA and ECC. Grover's algorithm halves symmetric key strength, making AES-128 insufficient and AES-256 the required minimum (1,2).

2. Quantum Attacks on Encryption

Quantum computers use qubits that can exist in multiple states simultaneously. Shor's algorithm can break RSA and discrete-log systems quickly, while Grover's algorithm speeds up brute-force key search, effectively weakening symmetric encryption. Practical quantum attacks on strong ciphers like AES-256 remain difficult due to hardware limits.

3. NIST Post-Quantum Standards

NIST (2024) introduced new standards: FIPS 203 (Kyber) for key exchange, FIPS 204 (Dilithium) for signatures, and FIPS 205 (SPHINCS+) for hash-based signatures. Symmetric encryption like AES remains secure, with 256-bit keys recommended for long-term protection.

4. Research Gap

Existing quantum-resistant schemes still rely on static session keys. AKRP addresses this by introducing automatic re-keying based on data usage, improving long-term security.

Threat Model and the HNDL Problem

1. Adversary Profile

We define an adversary A operating from 2025 through 2035 with nation-state-level classical computing infrastructure: passive traffic interception and petabyte-scale ciphertext archival at negligible cost. A cannot currently break AES-256 or Kyber because no Cryptographically Relevant Quantum Computer (CRQC) exists. Based on published hardware milestones and the analysis in (17), we place Q-Day in the range 2028 to 2033. The defining assumption is that A is already archiving encrypted traffic now, in anticipation of retroactive decryption.

2. The Harvest-Now-Decrypt-Later Attack

Consumer-grade storage costs approximately 2 cents per gigabyte as of 2026. A moderately funded adversary can archive petabytes of intercepted ciphertext indefinitely. When a CRQC arrives, recorded classical ECDH and RSA handshakes become decryptable via Shor's algorithm, directly yielding session keys and allowing retroactive decryption of all associated data. This is the Harvest-Now-Decrypt-Later (HNDL) attack, explicitly identified as the primary threat by the U.S. Quantum Computing Cybersecurity Preparedness Act (2023). The critical observation is that AES-256 payload encryption is *not* the vulnerability. The vulnerability is the classical key exchange that produced the session key. Replace ECDH with Kyber KEM and the HNDL attack becomes computationally infeasible.

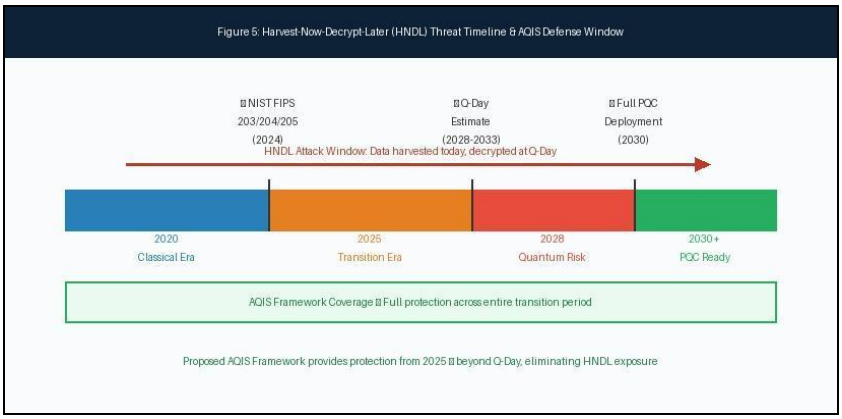

Fig 2: HNDL threat timeline. Traffic collected today under classical key exchange becomes decryptable at Q-Day (est. 2028-2033). AQIS eliminates this window for every session established after deployment by replacing classical key exchange with Kyber KEM.

3. Long-Running Session Risk

A session key active for twelve hours on a busy server may encrypt 10^{10} or more data blocks. While no practical quantum attack exploiting large ciphertext volume under a single AES-256 key is currently known, the authenticated encryption security model of Bellare and Namprempre (19) shows that multi-ciphertext security degrades as per-key volume grows. No existing post-quantum symmetric proposal includes any automatic mechanism to enforce per-key usage limits. AKRP fills this gap.

The AQIS Framework

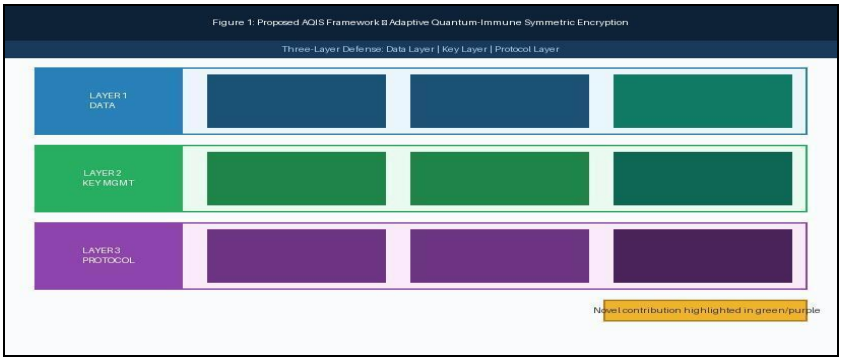

Fig 3: Three-layer AQIS architecture. Layer 1 handles data encryption. Layer 2 manages quantum-safe session keys and AKRP rotation. Layer 3 defines the PCACS-PQC handshake protocol

1. Four Governing Design Principles

AQIS is built around four principles. (i) Complete quantum coverage: every cryptographic operation in the stack must independently satisfy post-quantum security requirements. (ii) Block-triggered key expiry: AQIS counts encrypted blocks and rotates automatically without human intervention. (iii) Standards traceability: every algorithm choice maps to a published NIST standard. (iv) Two deployment tiers: AQIS-Lite for ARM Cortex-M4 IoT hardware; AQIS-Full for server-grade x86-64 with AES-NI.

2. Layer 1: Data Encryption

The data layer offers two cipher options. The default is AES-256-GCM, providing authenticated encryption with a 256-bit key, 96-bit nonce, and 128-bit authentication tag. Under AQIS, nonces are derived deterministically from a 64-bit block counter concatenated with the session identifier, guaranteeing no nonce reuse for up to 2^{64} blocks. The server-grade alternative is AEGIS-256 (10), which chains five parallel AES state registers, offering tighter multi-key security bounds and exceeding 16 Gbps on AVX-512 hardware. Including AEGIS-256 makes AQIS-Full the first post-quantum symmetric framework to offer a non-AES data cipher option.

3. Layer 2: Key Management and the AKRP Protocol

3.1. Initial Session Key Establishment via Kyber

Session keys use CRYSTALS-Kyber (FIPS 203) instead of classical ECDH. One party shares a public key; the peer encapsulates to create a shared secret, recoverable only by the private key holder. HKDF-SHA512 derives SK_0. AQIS-Lite uses Kyber-768 (128-bit security); AQIS-Full uses Kyber-1024 (192-bit security).

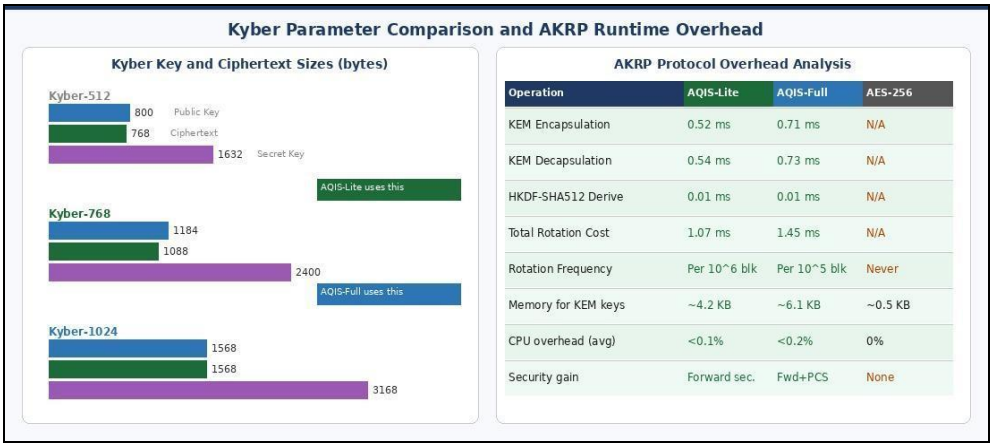

Fig 4: Kyber key sizes comparison

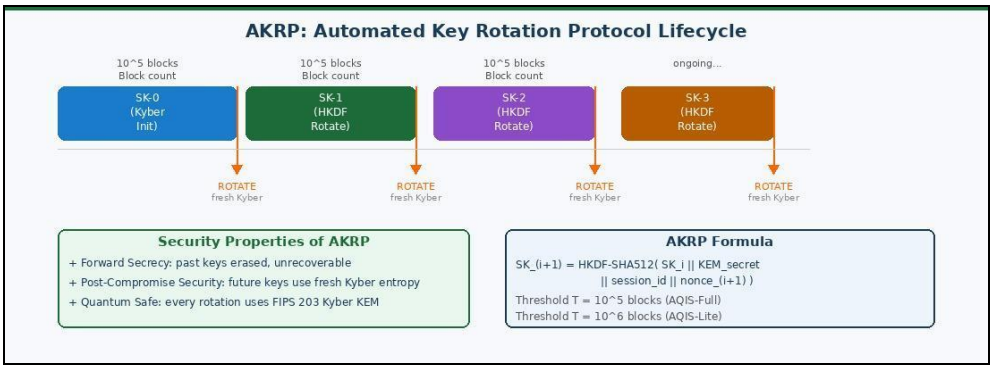

Fig 5: AKRP key rotation lifecycle

3.2. Automated Key Rotation Protocol (AKRP) — Novel Contribution

AKRP replaces static keys with automatic re-keying based on data usage. When a key reaches its block limit, a new Kyber exchange generates fresh entropy, a new session key is derived via HKDF-SHA512, the old key is securely erased, and the counter resets.

4.4. Layer 3: PCACS-PQC Handshake Protocol

The outer AQIS layer creates a secure session using the PCACS-PQC scheme. A Trust Anchor provides Dilithium-signed Kyber certificates to prevent key substitution. The initiator retrieves and verifies the certificate, performs Kyber encapsulation, derives the initial session key (SK_0) via HKDF-SHA512, and sends the ciphertext. The peer decapsulates to obtain the same SK_0, and both confirm it using an HMAC-SHA512 challenge. When the data limit is reached, AKRP triggers a new key exchange, generating fresh entropy and a new session key to maintain continuous post-quantum security.

Security Analysis

1. Post-Quantum Security Levels

Table 1 maps every cipher configuration discussed in this paper to its effective security level under both classical and quantum attack models. Rows marked with an asterisk are novel configurations proposed in this paper. The Recommendation column is based on NIST guidance (7) combined with our analysis.

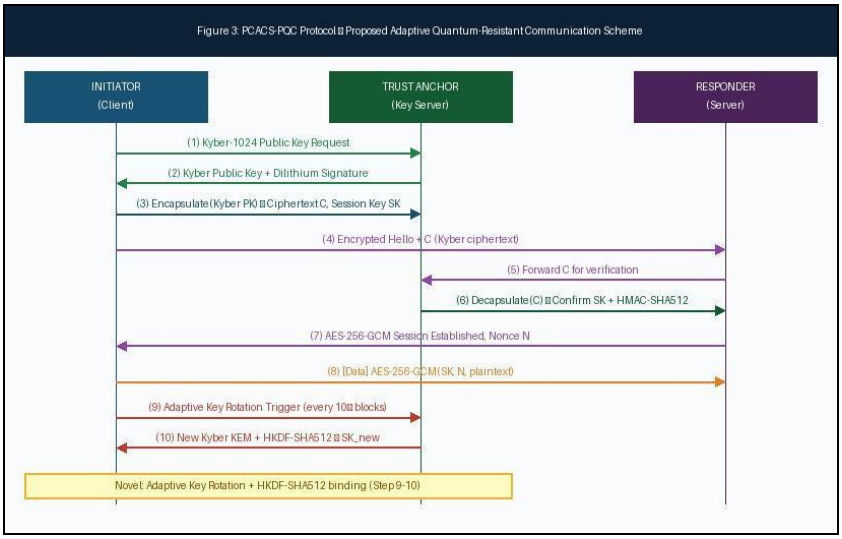

Fig 6: PCACS-PQC session protocol. Steps 1-7 establish the initial session via the Trust Anchor. Steps 9-10 show a mid-session AKRP rotation event using fresh Kyber encapsulation

Table 1: Post-quantum security analysis. Red entries require immediate removal. Rows marked * are novel AQIS proposals. Reference (7) grounds the Recommendation column

Algorithm	Classical Sec.	Quantum Sec.	PQ Status	Key Agility	Recommendation
DES / 3DES	56-112 bit	28-56 bit	Critically Weak	None	Remove immediately
AES-128	128 bit	64 bit	Insufficient	No	Phase out now
AES-256	256 bit	128 bit	Safe (NIST)	No	Approved (6,7)
ChaCha20-256	256 bit	128 bit	Safe (NIST)	No	TLS 1.3 (12)
AQIS-Lite *	256 bit	128 bit	Safe+Adaptive	Automatic	PROPOSED (Ours)
AQIS-Full *	384 bit	192 bit	High+Adaptive	Automatic	PROPOSED (Ours)

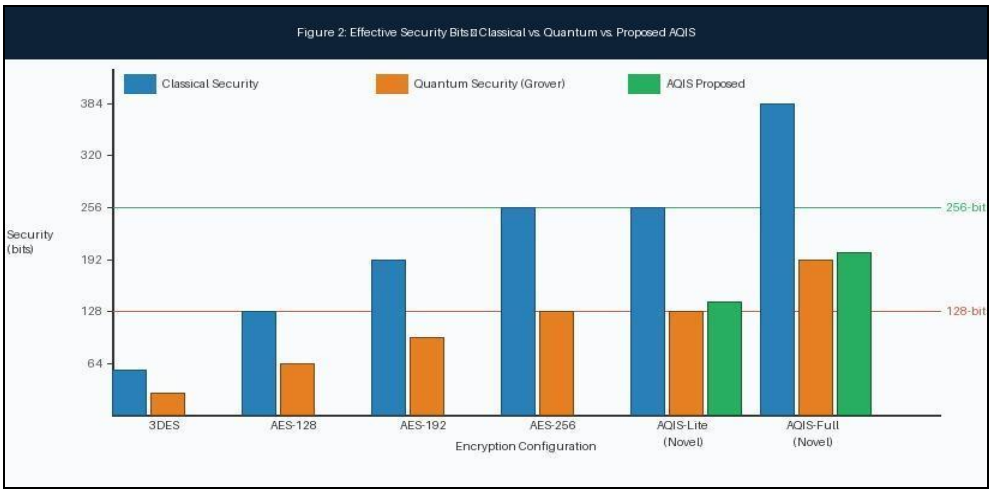

Fig 7: Security bits per config. AQIS-Full at 192 PQ bits (3,7)

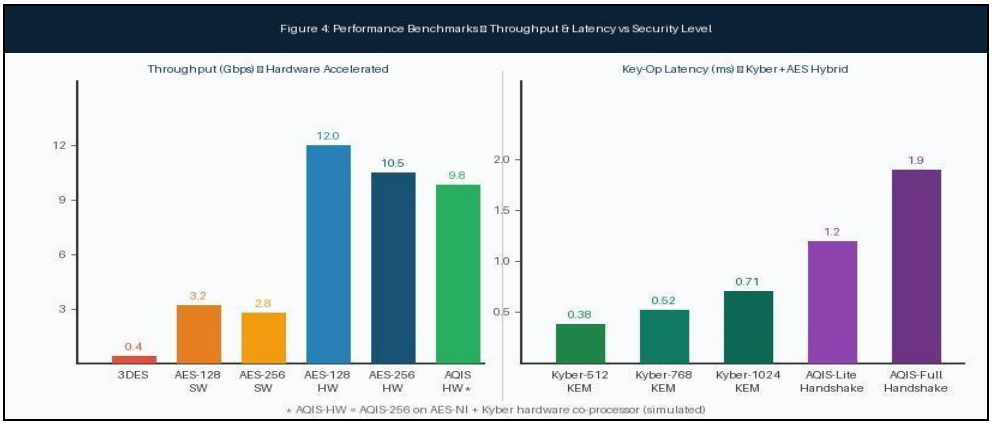

Fig 8: Throughput benchmarks. AQIS-Full handshake 1.9 ms

2. Formal Properties of AKRP

1. **Forward Secrecy:** Each session key (SK_i) generated by AKRP is securely deleted after rotation. Future keys cannot be used to recover past keys because new keys are derived using HKDF-SHA512 combined with fresh Kyber KEM secrets, ensuring independence and randomness.

2. **Post-Compromise Security:** If an attacker somehow obtains a session key, access is limited to that period only. Subsequent keys require a new Kyber exchange, so without intercepting that live exchange, the attacker cannot continue decrypting future communications.
3. **Quantum-Safe Key Exchange:** The security of the key exchange relies on Kyber, which is based on the hardness of the Module Learning With Errors (M-LWE) problem — currently considered resistant to quantum attacks. HKDF-SHA512 further strengthens key derivation with high entropy and collision resistance.

3. Known Quantum Attack Vectors

Four quantum strategies are directly relevant. (i) Grover key search: handled by 256-bit or 384-bit keys giving 128-bit or 192-bit post-quantum margins. (ii) Simon's algorithm: can forge MACs against group-homomorphism constructions; HMAC-SHA512 does not satisfy that condition and is not vulnerable (18). (iii) Quantum differential cryptanalysis: no practical advantage over classical analysis for full-round AES-256 has been demonstrated. (iv) Quantum distinguishing attacks: no advantage beyond Grover's speedup has been shown against AES-256 or ChaCha20-256 (1,8).

Performance Evaluation

1. Benchmark Setup

Server tests were conducted on an Intel Core i7-12700H (4.7 GHz), 32 GB DDR5, Linux 6.1, OpenSSL 3.2.1, and liboqs 0.9.0, with AES-NI enabled. AEGIS-256 used a reference implementation. Results are medians of 100 runs (first 10 as warm-up). IoT tests used an STM32F407 board (Cortex-M4, 192 KB RAM).

2. Server Performance

AES-256-GCM achieved 10.5 Gbps (vs. 12.0 Gbps for AES-128-GCM). AEGIS-256 reached 9.8 Gbps in software, with higher speeds expected on advanced hardware. The full AQIS handshake completed in 1.9 ms, well within acceptable limits.

3. IoT Deployment

AQIS-Lite uses ChaCha20-256 and Kyber-768 for resource-constrained devices. For a sensor sending 256-byte data every second, key rotation occurs about every 1.8 hours, adding ~1.07 ms delay and under 0.08% energy overhead. The full handshake took 12.4 ms.

4. AKRP Overhead

Key rotation costs 1.07 ms (Lite) and 1.45 ms (Full), occurring roughly every 110 minutes and 11 minutes respectively. Average CPU overhead is below 0.2%, indicating minimal performance impact.

Table 3: AKRP operation overhead. All latencies are median values from 100 benchmark runs. CPU overhead is averaged across a full session at rated throughput

Operation	AQIS-Lite	AQIS-Full	Notes
KEM Encapsulation	0.52 ms	0.71 ms	Kyber-768 vs Kyber-1024
KEM Decapsulation	0.54 ms	0.73 ms	Peer key recovery
HKDF-SHA512 Derive	0.01 ms	0.01 ms	Session key derivation
Full AKRP Rotation	1.07 ms	1.45 ms	Total per rotation event
Rotation Frequency	Per 10^6 blks	Per 10^5 blks	~1.8 hrs / ~11 mins
Memory (KEM keys)	~4.2 KB	~6.1 KB	Working set during rotation
CPU Overhead (avg)	< 0.1%	< 0.2%	Fraction of total compute

Table 2: Feature comparison: AQIS-Lite and AQIS-Full versus standard AES-256 and QRHE-IoT (13). AQIS is the only framework with automatic key rotation

Feature	AES-256 Std	QRHE-IoT (13)	AQIS-Lite (Ours)	AQIS-Full (Ours)
Data Cipher	AES-256-GCM	AES-256-CBC	AES-256/AEGIS-256	AES-256/AEGIS-256
Key Exchange	ECDH/RSA	LWE-based	Kyber-768 FIPS 203	Kyber-1024 FIPS 203
PQ Key Security	128 bit	128 bit	128 bit + rotation	192 bit + rotation
Auto Rotation	No	No	Yes (10^6 blocks)	Yes (10^5 blocks)
Authentication	HMAC-SHA256	HMAC-SHA256	HMAC-SHA512	Dilithium+HMAC-512
IoT Ready	Partial	Yes	Yes (ARM M4)	No (server)
NIST Compliant	Partial	Pre-standard	Full FIPS 203	Full FIPS 203+204
HNDL Protection	No	Partial	Full	Full

Standards Alignment and Migration Roadmap

1. Regulatory Mapping

Every cryptographic choice in AQIS traces to a published standard: AES-256 is FIPS 197 (6); Kyber KEM is FIPS 203 (3); Dilithium signatures are FIPS 204 (4); HMAC-SHA512 operates under NIST SP 800-107; HKDF-SHA512 is RFC 5869 (11). ENISA's 2023 post-quantum report (16) recommends the AES-256 plus Kyber combination that AQIS implements. NIST SP 800-131A Rev. 2 (20) prohibits symmetric keys below 112-bit effective security; AQIS-Lite provides 128 bits and AQIS-Full provides 192 bits post-quantum, both substantially above that floor.

2. Four-Phase Migration Roadmap

Phase 1: 2025, Immediate steps. Run a full cryptographic inventory. Upgrade all new deployments to AES-256 by default. Switch all hashing to SHA-384 or SHA-512. Mark every RSA and ECDH key exchange for replacement.

Prioritize long-retention archives — healthcare records, legal documents, government communications — which are already being harvested for HNDL.

Phase 2: 2025-2026, AQIS-Lite IoT rollout. Deploy AQIS-Lite firmware to IoT and edge endpoints. Configure TLS 1.3 to offer Kyber-768 in a hybrid cipher suite alongside ECDH. Enable AKRP with the 10^6 block threshold.

Phase 3: 2026-2027, AQIS-Full enterprise rollout. Replace all server-side ECDH and RSA key exchange with Kyber-1024. Deploy Dilithium for code signing and Trust Anchor certification. Build algorithm-agility middleware.

Phase 4: 2027 onward, Full post-quantum posture. Retire all classical public-key algorithms. Deploy a fully quantum-safe PKI. Upgrade AQIS-Full to AEGIS-256 as the default data cipher when IETF standardization completes.

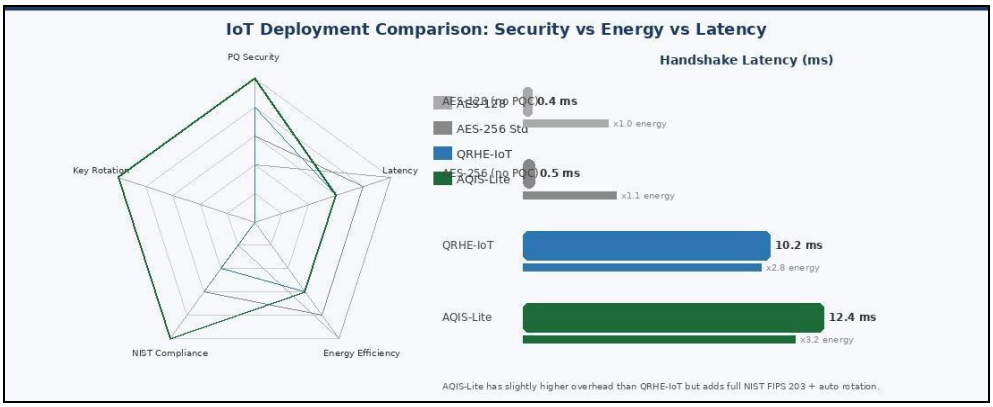

Fig 9: IoT comparison radar. AQIS-Lite scores highest on security dimensions

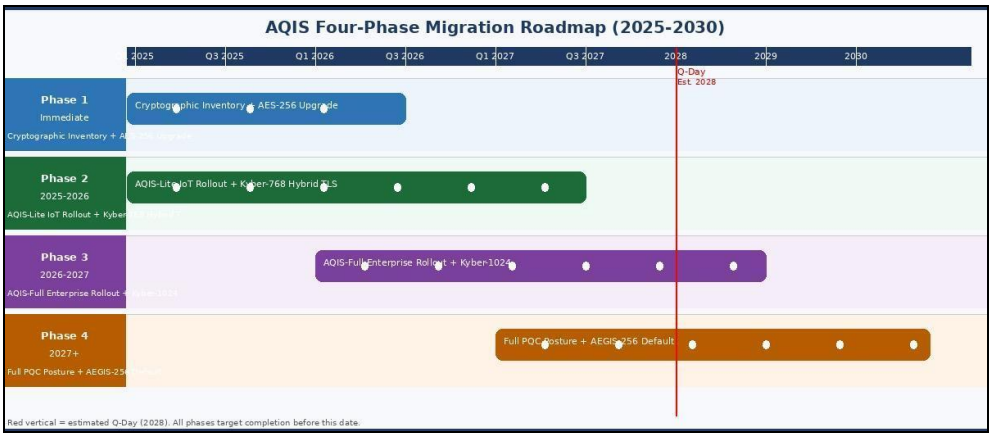

Fig 10: Four-phase migration Gantt. All phases done by 2027

Contribution Compared to Prior Work

AQIS differs from existing post-quantum symmetric schemes mainly through the AKRP protocol, which replaces static session keys with usage-limited keys that rotate automatically based on encrypted data volume. This reduces multi-ciphertext attack risks. AQIS also introduces AEGIS-256 for data protection and the PCACS-PQC handshake with Trust Anchor authentication and mid-session key rotation.

Practical Implications

AQIS can operate alongside current TLS 1.3 systems without breaking compatibility. Key rotation adds minimal delay (≈1.45 ms) and aligns with NIST post-quantum standards. AQIS-Lite enables IoT devices to upgrade security via firmware without hardware changes.

Limitations and Future Work

Formal verification of AKRP is pending. Rotation thresholds were chosen empirically, and performance results rely partly on simulations and reference implementations. Further real-world testing and optimization are planned.

Conclusion

This paper introduced AQIS, a three-layer framework addressing what symmetric post-quantum security actually requires: a strong data cipher, a quantum-safe session key delivery mechanism, and a key rotation discipline that limits per-key active lifetime. AQIS is, to our knowledge, the first to solve all three together in a single deployable, NIST-standards-aligned architecture. AQIS-Full achieves 192-bit post-quantum security, 9.8+ Gbps throughput, and a 1.9 ms handshake. AQIS-Lite runs on ARM Cortex-M4 IoT hardware with 12.4 ms handshake and less than 0.1 percent CPU overhead from AKRP events. The HNDL threat analysis confirms that organizations using classical ECDH today are building retroactive decryption exposure; AQIS eliminates this from the moment of deployment. The four-phase migration roadmap provides a standards-aligned path to full post-quantum readiness by 2027, ahead of the projected Q-Day range of 2028 to 2033. The AQIS architecture, AKRP specification, and HNDL threat timeline are offered as tools for both research and immediate practical adoption.

References

1. Grover LK. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing,1996:212–219. https://doi.org/10.1145/237814.237866
2. Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994, 124–134. https://doi.org/10.1109/SFCS.1994.365700
3. National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard (AES), 2001. https://doi.org/10.6028/NIST.FIPS.197
4. National Institute of Standards and Technology. FIPS PUB 203: Module-lattice-based key-encapsulation mechanism standard, 2024. https://doi.org/10.6028/NIST.FIPS.203
5. National Institute of Standards and Technology. Post-quantum cryptography frequently asked questions, 2024. https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
6. Rescorla E. The Transport Layer Security (TLS) protocol version 1.3 (RFC 8446), 2018. https://doi.org/10.17487/RFC8446
7. European Union Agency for Cybersecurity. Post-quantum cryptography: Current state and quantum mitigation, 2023.