# Post-Quantum Cryptography in Practice: A Literature Review of Protocol-Level Transitions and Readiness

Obianuju Egbuagha and Emmanuel Ikwunna
*Oulu University Secure Programming Group*
*Biomimetics and Intelligent Systems Research Unit*
*Faculty of Information Technology and Electrical Engineering*
*University of Oulu, Finland*
{obianuju.egbuagha, emmanuel.ikwunna}@student.oulu.fi

**Abstract**

This paper presents a structured literature review of ongoing global efforts to integrate post-quantum cryptography (PQC) into widely deployed communication and identity protocols. We analyze current readiness, standardization initiatives, hybrid cryptographic approaches, and deployment challenges across multiple layers of the protocol stack, including TLS, SSH, VPNs, certificate infrastructure, and messaging protocols.

The report also discusses hybrid cryptographic strategies, current deployment efforts, and the technical challenges facing real-world implementation, including performance, interoperability, and resistance to side-channel attacks. With insights from recent research, industry trials, and open source tools, the report aims to provide a clear and accessible overview of the growing role of PQC in securing the future of digital communication.

We aim to guide researchers, developers, and policymakers in understanding the state of PQC integration and encourage broader involvement in the testing, implementation, and evaluation of next-generation cryptographic solutions.

**Keywords:** Post-Quantum Cryptography, Quantum Computing, Cryptographic Protocols, TLS, SSH, VPN, QKD, MQTT, IPsec, NIST, Hybrid Cryptography

CONTENTS

# I. Introduction

Public-key cryptography serves as the cornerstone of secure digital communication, enabling protocols like TLS, SSH, and VPNs to protect data in transit [1], [2]. These systems depend on computationally difficult mathematical problems, such as integer factorization and discrete logarithms with elliptic curves, which classical computers struggle to solve efficiently [3]. By leveraging this asymmetry, public-key cryptosystems ensure that private keys remain practically unrecoverable from their public counterparts, thereby upholding confidentiality, authentication, and trust in modern communications.

However, the rise of quantum computing threatens this security foundation. Algorithms like Shor's algorithm could efficiently break widely used cryptographic schemes, undermining the protection of sensitive data [4]. This vulnerability poses a critical challenge to the future of secure communications, necessitating the development of post-quantum cryptography (PQC) to safeguard digital infrastructure [5], [6].

PQC refers to cryptographic algorithms believed to be secure against both classical and quantum adversaries. These schemes, including lattice-based, code-based, multivariate, and hash-based constructions, have been the subject of intense research, with the U.S. National Institute of Standards and Technology (NIST) currently leading a multi-year standardization effort [6]. In March 2025, Hamming Quasi-Cyclic (HQC) was selected as a Key Encapsulation Mechanism (KEM) for standardization among the fourth-round finalists [7]. This complements the previously standardized CRYSTALS-Kyber KEM. The currently approved NIST digital signature algorithms include CRYSTALS-Dilithium, SPHINCS+, and Falcon.

The practical integration of Post-Quantum Cryptography (PQC) has entered a new phase of deployment, moving beyond theoretical design. Following the publication of the foundational NIST standards FIPS 203, 204, and 205 in 2024 [8], [9], [10], the IETF has also formalized hybrid PQC mechanisms for key protocols like TLS 1.3 and SSH [11], [12]. While these new standards provide a clear path for implementation, they introduce significant operational hurdles. Protocols must not only support the new cryptographic primitives but also guarantee backward compatibility, manage the performance overhead of larger keys and signatures, and defend against newly relevant side-channel attacks.

Hybrid cryptographic approaches, where classical and quantum-resistant algorithms are used together, have emerged as a transitional solution [13]. These schemes allow for forward compatibility without immediate infrastructure overhaul, and several industry trials (e.g., by Google, Cloudflare, and Microsoft) have demonstrated early feasibility in real-world environments.

This paper presents a structured literature review of the current state of PQC transition. We evaluate the readiness and implementation challenges across major security protocols focusing on application-layer systems (TLS, SSH, email, messaging), transport-layer technologies (IPsec), identity infrastructures (X.509, code signing), BLE and MQTT. We aim to provide a holistic view of how post-quantum standards are influencing the future of digital trust and communication.

### A. Motivation for PQC Transition

The motivation for this review arises from the urgency of preparing digital infrastructure for the post-quantum era. With quantum computers rapidly evolving in research labs and the cryptographic community actively evaluating PQ-safe algorithms, it is essential to assess not just algorithmic proposals but also deployment realities. This includes integration bottlenecks, developer tooling, standardization timelines, and public-key infrastructure (PKI) updates [14].

### B. Scope and Objectives of the Review

The scope of this review is protocol-centric. We examine how PQC is being integrated into widely deployed communication and trust protocols, evaluate challenges across protocol layers, and highlight hybrid designs and experimental deployments. Our objective is to map the current readiness and provide information for researchers, implementers, and policymakers.

### C. Organization of the Paper

The remainder of the paper is organized as follows. Sections **II** through **VII** examine the adaptation of post-quantum cryptography (PQC) across various protocols, highlighting associated challenges, research gaps, and future directions. Section **VIII** concludes the report with a summary of the findings and recommendations.

## II. Transport Layer Security (TLS)

### A. Overview of TLS

Transport Layer Security (TLS) is a widely adopted cryptographic protocol that ensures secure communication over networks. It provides confidentiality, integrity, and authentication through a combination of symmetric and asymmetric cryptographic techniques. TLS operates primarily over TCP and supports various key exchange mechanisms, including RSA, Diffie-Hellman (DH), and Elliptic Curve Diffie-Hellman (ECDH), with ephemeral variants offering forward secrecy [15].

### B. Quantum Threat to TLS

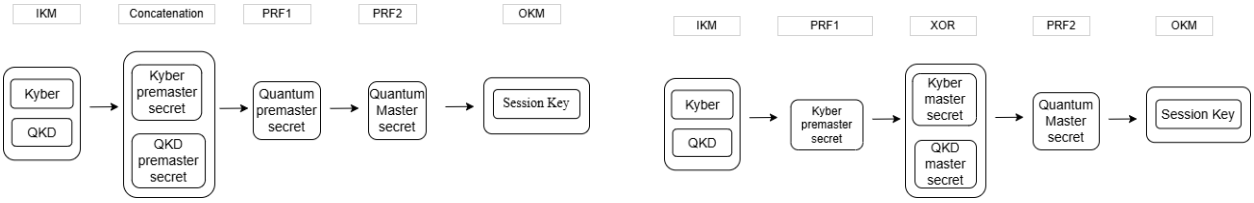
Quantum computing threatens the foundational assumptions of TLS security. Algorithms such as RSA and ECC, which rely on the hardness of integer factorization and discrete logarithms, are vulnerable to Shor's algorithm [4]. This has led to the concept of "Q-Day," the anticipated point when quantum computers can break current public-key cryptography. Although projected around 2031 [6], the risk of "harvest now, decrypt later" attacks necessitates early adoption of (PQC).

### C. Post-Quantum Integration Strategies

#### 1) Hybrid PQC-QKD Implementation by Garcia et al

Garcia et al. proposed a hybrid TLS handshake that combines Quantum Key Distribution (QKD) with PQC algorithms like Kyber inside Mbed TLS, a real-world, industry-grade TLS stack. Two novel key combination methods were developed:[16].

- Concatenation: Combines shared secrets from both Kyber and QKD end-to-end to form a single quantum premaster secret, which is then input into the TLS key schedule via a pseudorandom function; the confidentiality of these session keys is maintained so long as at least one contributing cryptographic primitive remains uncompromised.
- XOR Integration: The Kyber-derived premaster secret is first processed through a pseudorandom function to generate a post-quantum master secret, which is then XORed with a master secret derived from QKD, ensuring that breaking both the Kyber and QKD secrets is necessary to compromise the session, thereby enhancing robustness.




(a) Quantum-hybrid premaster secret generation via concatenation, adapted from Fig. 5 in Garcia et al. [16].

(b) Quantum-hybrid master secret generation via XOR, adapted from Fig. 6 in Garcia et al. [16].

Fig. 1: Illustration of concatenation- and XOR-based key combination methods in hybrid PQC-QKD TLS.

They found out that using only PQC-based TLS improves handshake performance by approximately 9% over classical methods. However, the full hybrid PQC-QKD solution increases handshake latency by 117%, indicating a significant security-performance trade-off.

*2) Benchmarking Post-quantum Cryptography in TLS 1.3*

Paquin et al. benchmarked PQC algorithms in TLS 1.3 using the Open Quantum Safe (OQS) project [17]. Their experiments evaluated hybrid key exchange and post-quantum authentication under real and emulated network conditions. Key findings include:

Table I summarizes the classical, hybrid, and post-quantum cryptographic (PQC) algorithms utilized in the experimental evaluations conducted by the researchers.

Their key findings were as follows.

- *Kyber512-90s* was identified as the most practical candidate for PQC key exchange, offering a good trade-off between performance and resilience.
- *Dilithium2*, based on structured lattices, was considered viable for authentication. However, Picnic-L1-FS was discouraged due to its large bandwidth requirements.
- Packet loss and fragmentation significantly affect PQC performance, emphasizing the need for optimized, size-efficient cryptographic primitives.

*3) Post-Quantum Hybrid KEMTLS Performance in Simulated and Real Network Environments*

Giron et al. proposed a hybrid version of the KEMTLS protocol by combining classical cryptographic primitives (P256, P384, P521) with post-quantum candidates (Kyber, Saber, NTRU). [24]. Key features include:

TABLE I: Key exchange and signature algorithms used in the experiments, adapted from Table 3 in Paquin et al. [17].

| Notation | Hybrid | Family | Variant | Implementation |
|---|---|---|---|---|
| **Key Exchange** | | | | |
| ecdh-p256 | × | Elliptic-curve | NIST P-256 | OpenSSL optimized |
| ecdh-p256-sike-p434 | ✓ | Supersingular isogeny | SIKE p434 [18] | Assembly optimized |
| ecdh-p256-kyber512-90s | ✓ | Module LWE | Kyber 90s Level 1 [19] | AVX2 optimized |
| ecdh-p256-frodo640aes | ✓ | Plain LWE | Frodo-640-AES [20] | C with AES-NI |
| **Signatures** | | | | |
| ecdsa-p256 | × | Elliptic curve | NIST P-256 | OpenSSL optimized |
| dilithium2 | × | Module LWE/SIS | Dilithium2 [21] | AVX2 optimized |
| qtesla-p-i | × | Ring LWE/SIS | qTESLA Provable 1 [22] | AVX2 optimized |
| picnic-l1-fs | × | Symmetric | Picnic-L1-FS [23] | AVX2 optimized |

- *Dual KEM Key Pairs:* Both classical and post-quantum key pairs are used for ephemeral and static key exchanges.
- *Concatenated Key Shares:* Public keys and ciphertexts from both KEM types are sent together.
- *Modified Key Schedule:* Shared secrets are combined using the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) with a dualPRF combiner, ensuring security even if one algorithm is compromised.
- *Signature-less Authentication:* The handshake uses KEM-based implicit authentication. However, X.509 certificates still include traditional digital signatures to maintain backward-compatible trust chains.

Table II presents the results of both simulation and real-world experiments in various TLS variants, highlighting the corresponding security trade-offs and performance implications. In addition, Table III details the cryptographic components employed by each variant, highlighting their impact on handshake latency, message size, and key implementation observations.

TABLE II: Comparative analysis of TLS variant performance and security trade-offs.

| **Variant** | **Simulated Network Impact** | **Real-World Network Impact** | **Security Trade-offs / Observations** |
|---|---|---|---|
| Baseline (Classical TLS) | Lowest latency by design; Small message size ( 1.7 KB) | Remains fastest; Minimal overhead | Uses classical ECC (P256/P384/P521); not quantum-resistant; Serves as performance reference. |
| PQTLS (Pure PQC) | Highest latency due to expensive PQC signature ops; Very large message size | Signature verification delays; Excessive message size | Fully quantum-safe assuming PQC primitives hold; impractical for latency/bandwidth-sensitive settings. |
| Hybrid PQTLS | Slightly faster than PQTLS; still high due to signature overhead | Signature-based handshake remains slower than KEM variants | Dual protection (classical + PQC); higher latency is the trade-off. |
| KEMTLS (PQC-only, signatureless) | +3–5 ms over baseline due to encapsulation overhead; Moderate message size | Acceptable delay relative to RTT; Small-to-moderate message size increase | Uses implicit authentication via PQC KEM and HKDF-based combiner. |
| Hybrid KEMTLS | Similar delay to KEMTLS; Larger messages ($\approx$ 11 KB–36 KB) | Minor extra latency vs. RTT; Message size acceptable under TCP window | Adversaries must break both classical and PQC KEMs; enhanced security with slight overhead. |
| KEMTLS-PDK | Fastest among quantum-safe (+2–4 ms over Baseline); Keys pre-distributed | Excellent with cached keys; Message size like KEMTLS | Quantum-safe using PQC KEMs with pre-shared keys; slightly sacrifices duality for speed. |
| Hybrid KEMTLS-PDK | Slightly slower than KEMTLS-PDK by 1–2 ms | Good performance; Message size similar to Hybrid KEMTLS | Best security: dual protection + predistribution; Minimal added overhead. |

TABLE III: Cryptographic components and handshake message sizes for TLS variants.

| **Variant** | **Cryptographic Elements** | **Handshake Delay** | **Message Size Impact** | **Key Observation** |
|---|---|---|---|---|
| Baseline | Classical ECC (e.g., P256, etc.) | Lowest (by design) | Small ( 1.7 KB) | Fastest but lacks post-quantum security. |
| KEMTLS | PQC KEM-only (no signatures) | Modest overhead vs. baseline | Moderate size increase | PQC-only, efficient compared to signature-based PQC. |
| Hybrid KEMTLS | Classical + PQC KEMs (dual PRF combiner) | +3–5 ms over baseline | Larger ($\approx$ 1–36 KB) | Dual security at modest latency cost. |
| PQTLS | PQC KEM + PQC signatures | Highest latency | Very large messages | Quantum-safe but impractical for latency-sensitive apps. |
| Hybrid PQTLS | Classical + PQC (PQC signatures) | Slower than KEM variants | Larger than Hybrid KEMTLS | Classical fallback but higher signature cost. |
| KEMTLS-PDK | PQC KEM-only with pre-distributed key | Lowest among quantum-safe options | Moderate size (like non-hybrid) | Efficient from reduced round trips. |
| Hybrid KEMTLS-PDK | Classical + PQC KEMs with pre-distributed key | Slightly higher than KEMTLS-PDK | Message size comparable to Hybrid KEMTLS | Predistribution boosts speed. |

Here are their key findings.

- Hybrid KEMTLS and Hybrid KEMTLS-PDK provide enhanced security by requiring the compromise of both classical and post-quantum cryptographic components, thereby offering robust protection against quantum-capable adversaries.
- While non-hybrid KEMTLS-PDK achieves superior performance due to reduced round-trip operations, hybrid variants maintain strong cryptographic guarantees with only marginal latency increases, making them practical for deployment.
- Despite the high security of PQTLS and Hybrid PQTLS, their reliance on post-quantum digital signatures results in significant message size and latency overhead. In contrast, hybrid KEMTLS variants demonstrate minimal performance degradation at lower NIST security levels, supporting their suitability for real-world TLS applications.

*4) Fully Hybrid TLSv1.3 in WolfSSL on Cortex-M4*

Anastasova et al.[25] propose a fully hybrid TLSv1.3 protocol that integrates both classical and post-quantum cryptographic algorithms to ensure secure communication on resource-constrained embedded systems like the Cortex-M4. Their design combines Curve448 (ECDH) and Crystals-Kyber1024 for hybrid key exchange, and Ed448 with Crystals-Dilithium5 for hybrid digital signatures and authentication. They enhance the X.509 Public Key Infrastructure to support hybrid certificates containing both classical and post-quantum components and implement this design using OpenSSL for key and certificate generation and wolfSSL for embedded cryptographic operations. This architecture guarantees resilience against classical and quantum adversaries while remaining efficient enough for low-power IoT devices.

Table IV summarizes and contrasts the performance of classical and fully hybrid TLSv1.3 implementations across different execution contexts capturing key exchange methods, authentication, certificate verification, and measured impacts on cycle count and latency.

*5) Quantum-Resistant TLS 1.3: Improved Triple-Hybrid Handshake and Key Derivation*

Garcia et al. [28] implemented a triple-hybrid cryptographic framework to TLS 1.3, building upon their earlier work by introducing architectural and performance improvements. This implementation integrates classical cryptography, PQC, and QKD into the TLS handshake, offering enhanced security against both classical and quantum adversaries.

The TLS 1.3 implementation is built on OpenSSL and Liboqs, with custom modules for QKD integration. The authors use X25519 for classical key exchange, ML-KEM-1024 for post-quantum key encapsulation, and QKD-derived keys retrieved via a key management system (KMS). Authentication is handled using CRYSTALS-Dilithium (ML-DSA-65), and symmetric encryption is performed using AES-256-GCM.

A key improvement over their previous work [16] is the change to client-initiated QKD key retrieval, which mitigates the risk of server-side key exhaustion attacks and improves handshake performance. All key negotiation steps, including QKD, are triggered before the ClientHello message is sent, ensuring a more secure and efficient handshake process.

For key combination, the authors adopt a concatenation-based approach. The IKM is formed by concatenating three 32-byte secrets, one each from classical, PQ, and QKD sources, into a single 96-byte array. This IKM is then

| Work | Execution Scenario | KEX | Auth | Cert Verify | Performance Note |
|---|---|---|---|---|---|
| Classical TLSv1.3 | Classical TLSv1.3 | X448 | Ed448 | Ed448 | Baseline for comparison based on previous work by wolfSSL [26] and Anastasova et al. [27] |
| Fully Hybrid TLSv1.3 | Handshake only | X448 + Kyber1024 | Ed448 + Dilithium5 | Ed448 + Dilithium5 | Took around 114 million cycles to complete. |
| | Handshake only (Excl. Server Cert Verify) | X448 + Kyber1024 | Ed448 + Dilithium5 | – | ∼17.5% faster handshake; not a typical scenario. |
| | Handshake + Short AEAD Encrypted Message | X448 + Kyber1024 | Ed448 + Dilithium5 | Ed448 + Dilithium5 | Adds ∼20.3 million cycles to the handshake. |
| | Handshake + AEAD Msg (Excl. Server Cert Verify) | X448 + Kyber1024 | Ed448 + Dilithium5 | – | ∼16% faster overall execution; not a typical use case. |

TABLE IV: Execution time comparison of Classical and Fully Hybrid TLSv1.3 on the STM32F413 Cortex-M4 platform, highlighting the performance overhead introduced by post-quantum key exchange and authentication.

processed using the standard HKDF-based TLS 1.3 key schedule to derive handshake and application traffic keys. This method allows for seamless integration of multiple cryptographic assumptions without altering the protocol structure.

Experimental results show that the triple-hybrid handshake adds approximately 57 milliseconds of overhead, primarily due to QKD key retrieval latency. Despite this, the system maintains compatibility with existing TLS infrastructure and does not introduce significant packet size overhead. The authors also demonstrate that their implementation can support up to 78 high-speed TLS connections per second using QKD-derived keys, validating its practicality for real-world deployment.

### *D. Challenges*

Several challenges hinder the seamless integration of PQC into TLS:

- PQC algorithms often require more computational resources and produce larger messages, increasing handshake latency.
- The structure of TLS 1.3 that does not support early peer authentication before key retrieval complicates QKD integration, making it more feasible in TLS 1.2.
- PQC keys are large and more susceptible to fragmentation and retransmission delays.
- Inefficient key usage can lead to denial-of-service attacks if QKD keys are depleted prematurely.
- The security of the hybrid model critically relies on the dualPRF combiner introduced by Bindel et al., whose ability to securely merge outputs from distinct key encapsulation mechanisms presents a complex and

unresolved challenge. [29]

- Accurate evaluation of PQC under real-world conditions is challenging due to the need for large-scale test environments, which are typically inaccessible to smaller research groups
- Some PQC candidates have been proven insecure, highlighting the need for hybrid approaches until standards stabilize.

### *E. Research Gaps*

- More research is required to adapt hybrid PQC–QKD and KEMTLS models to the TLS 1.3 protocol.
- Only a few publications on the hybrid integration of KEMTLS exist. The study by Giron et al. [24] is one of the first evaluations of its security and performance characteristics.
- The feasibility of deploying hybrid KEMTLS in resource-constrained environments such as IoT and 5G networks remains an area that needs further research.

### *F. Future Work*

- Develop workarounds within TLS 1.3 to support early peer authentication, which is essential for the integration of QKD and hybrid key exchange mechanisms.
- Conduct comprehensive cryptographic analysis and optimization of the dualPRF combiner used in hybrid KEMTLS to ensure secure and efficient merging of classical and quantum-derived secrets.
- Investigate the applicability of hybrid KEMTLS in constrained environments such as IoT and 5G networks, with particular emphasis on reducing performance overhead and energy consumption.
- Evaluate server throughput under high client load conditions to identify scalability bottlenecks and inform deployment strategies for PQC-enabled TLS implementations.

### *G. Summary*

TLS is among the most actively researched protocols in the context of PQC integration and is progressing steadily toward quantum resilience through KEMTLS, PQ-only, hybrid, and triple-hybrid implementations that incorporate classical, PQC, and QKD primitives. Prototype implementations have demonstrated feasibility; however, the cryptographic research community must address several challenges to enable broader, interoperable deployments. These include performance overheads, fragmentation due to large key sizes, and resource.

## III. Secure Shell (SSH)

### *A. Overview of SSH*

Secure Shell (SSH) is a foundational protocol for encrypted remote access, file transfer, and tunneling across untrusted networks [2]. It underpins secure infrastructure across operating systems, cloud environments, and embedded devices, providing confidentiality and integrity while enabling authenticated administration over networks.

### B. Quantum Threat to SSH

Classical SSH key exchange and authentication methods, including RSA and elliptic curve Diffie-Hellman (ECDH), are susceptible to quantum attacks. Shor's algorithm can efficiently break these schemes, compromising confidentiality and authentication [4]. To ensure long-term security, SSH must transition to post-quantum cryptographic (PQC) primitives.

### C. Hybrid Post-Quantum Key Exchange (KEX): Mechanisms and Standards

Recent versions of OpenSSH (10.0+) have integrated hybrid key exchange (KEX) using `mlkem768x25519-sha256`, combining the NIST-standardized ML-KEM (Kyber-based) with classical X25519 ECDH [30]. This mechanism aligns with the IETF draft `draft-ietf-sshm-mlkem-hybrid-kex-02` [31], where clients send concatenated post-quantum and classical public keys, and both KEM operations are performed in parallel. Derived secrets are combined using HKDF, ensuring the connection remains secure if at least one algorithm remains secure, while aligning with FIPS-approved key derivation guidelines.

#### 1) Key Exchange Method Variants

TABLE V: Supported ML-KEM + ECDH Hybrid SSH KEX Variants

| **Method Name** | **Classical KEX** | **Post-Quantum KEM** |
|---|---|---|
| `mlkem768x25519-sha256` | X25519 | ML-KEM-768 (Kyber) |
| `mlkem1024nistp384-sha384` | NIST P-384 | ML-KEM-1024 (Kyber) |
| `mlkem768nistp256-sha256` | NIST P-256 | ML-KEM-768 (Kyber) |

These hybrid algorithms are designed to fit within SSH's packet size constraints (32KB payload, 35KB total) while offering dual security and improving future cryptanalysis resistance [31].

#### 2) Security Properties and FIPS Compliance

Hybrid KEX secures connections against adversaries who would need to break *both* classical (e.g. X25519) and PQ (ML-KEM) components [31], [30]. Formal proofs within the ACCE model under the quantum random oracle framework show the construction achieves IND-CPA and, under strengthened assumptions, IND-CCA2 security [31]. The concatenation HKDF combiner aligns with NIST SP 800-56C rev.2 and FIPS-SP 800-135 guidelines, enabling FIPS-certified SSH deployments [31], [32].

#### 3) Performance and Interoperability

Benchmarks indicate hybrid SSH KEX introduces moderate handshake latency ranging from 0.5% to 50%, depending on network conditions and KEM size but remains practical for typical use cases [33]. AWS Transfer Family offers configurable hybrid policies (e.g. `mlkem768x25519-sha256`) using FIPS-certified libraries, recommending operational testing due to bandwidth/latency variance [32]. OpenSSH 10 includes this KEX by default, signaling strong ecosystem adoption [30].

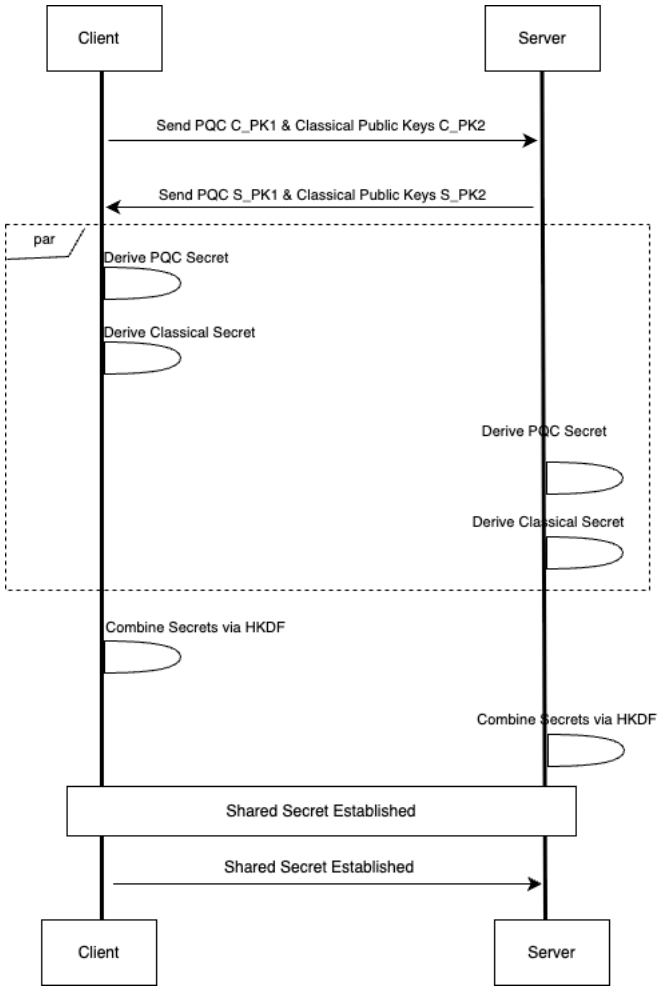



Fig. 2: Hybrid SSH KEX handshake flow: client/server exchange both PQC and classical public keys, derive secrets in parallel, combine via HKDF.

*4) Ongoing Implementation Efforts*

Frameworks such as OQS-OpenSSH prototype additional PQC options (e.g. NTRU, Falcon) via liboqs; however, many remain experimental [34]. Standard SSH clients like SmartFTP also list support for `mlkem768x25519-sha256`, indicating expanding market support [35].

*5) Summary*

Through hybrid KEX, SSH achieves protocol-level agility by integrating quantum-safe cryptography while preserving backward compatibility and compliance. Formal proofs, real-world adoption (OpenSSH, AWS), and interoperability frameworks indicate a robust and practical path toward post-quantum readiness.

### *D. Formal Security Analysis*

Formal ACCE-model proofs demonstrate that SSH hybrid KEX achieves session key confidentiality under quantum adversaries if at least one KEM remains secure, even with only IND-CPA post-quantum KEMs, by

leveraging the quantum random oracle model [36]. This enables SSH to adopt faster CPA-secure PQC variants while preserving robust session secrecy.

### *E. Performance and Deployment*

Prototype testing using `liboqs` with OpenSSH 7.9 demonstrated the feasibility of hybrid KEX with moderate CPU and bandwidth overheads [37]. In practice, AWS Transfer Family has deployed ML-KEM-based hybrid SSH in production, supporting FIPS-validated environments [38], while Red Hat Enterprise Linux 10 enables post-quantum SSH by default [39]. The Go 1.24 toolchain and Kubernetes environments are also integrating hybrid PQC KEX for secure internal communications.

### *F. Authentication: PQ Signatures and Remaining Gaps*

Despite hybrid KEX deployment, post-quantum signatures (e.g., Dilithium, Falcon, SPHINCS+) for SSH authentication remain experimental. Current tooling like `ssh-agent`, HSMs, and PKI workflows do not yet support PQC signatures, leaving authentication quantum-vulnerable despite quantum-safe key exchange [40].

TABLE VI: Trade-offs in Post-Quantum SSH Migration

| **Aspect** | **Summary** |
|---|---|
| **Handshake Security** | Requires breaking both classical and PQ KEM for compromise, providing strong forward secrecy. |
| **Computational Load** | PQ KEM encapsulation introduces CPU and bandwidth overhead, but optimized ML-KEM mitigates performance penalties [41]. |
| **Formal Guarantees** | Provides ACCE-level security under quantum adversarial models using IND-CPA PQ KEMs [36]. |
| **Interop Readiness** | Widely supported hybrid KEX, but partial deployments risk fallback vulnerabilities. |
| **Authentication** | PQC signatures remain under standardization and lack broad tooling support. |

### *G. Research Gaps and Future Directions*

To achieve full quantum resilience in SSH, further efforts are required:

- Standardization and deployment of PQC signature schemes (e.g., Dilithium, Falcon) for SSH authentication.
- Development of clear interoperability profiles to prevent fallback vulnerabilities in hybrid environments.
- Optimization of CPU, memory, and bandwidth use in PQ SSH for cloud and embedded systems.
- Practical deployment guidance and tooling support for enterprises migrating to PQ SSH.
- Extended formal proofs covering authentication alongside key exchange in the quantum model.

### *H. Summary*

SSH is among the most advanced protocols in post-quantum readiness, with hybrid KEX now deployed across major platforms and services. Remaining challenges include the standardization and operational deployment of PQC signatures, optimization of hybrid handshake mechanisms, and improvement of interoperability and tooling to enable end-to-end post-quantum secure SSH in the quantum computing era.

# IV. BLUETOOTH

## A. Overview of Bluetooth

Bluetooth technology secures wireless communication using a suite of cryptographic algorithms tailored to its architecture and energy constraints. During device pairing, Bluetooth employs key generation methods that vary by version and pairing model, with Bluetooth 4.2 and later using FIPS-approved algorithms. For Bluetooth Low Energy (BLE), encryption and message integrity are provided by AES-CCM with 128-bit keys. Authentication is achieved through challenge-response protocols, and key exchange in BLE Secure Connections leverages Elliptic Curve Diffie-Hellman (ECDH) to resist eavesdropping and man-in-the-middle attacks. Session keys are periodically refreshed to maintain confidentiality, and Bluetooth defines multiple security modes and levels to enforce encryption and authentication policies throughout communication. [42], [43]

## B. Quantum Threat to Bluetooth

Bluetooth faces a limited but noteworthy quantum threat, primarily due to its reliance on Elliptic Curve Diffie Hellman (ECDH) for key exchange in BLE Secure Connections. ECDH is susceptible to Shor's algorithm, which can efficiently solve the elliptic curve discrete logarithm problem on a sufficiently powerful quantum computer, thereby compromising the confidentiality of session key establishment.

In contrast, Bluetooth's core encryption and authentication mechanisms such as AES-CCM and AES-CMAC are based on symmetric cryptography and are not directly vulnerable to Shor's algorithm. However, Grover's algorithm theoretically reduces the effective security of symmetric ciphers from $n$ bits to $\sqrt{n}$ bits, implying that longer key lengths are advisable to maintain post-quantum resilience [44], [45]. Consequently, the primary quantum vulnerability in Bluetooth lies in its public key key exchange process.

## C. Post-Quantum Integration Strategies

### 1) Backward-Compatible Approach to Secure BLE Key Exchange Against Quantum Threats

Tao et al. introduced a backward-compatible Post-Quantum Key Exchange (PQKE) mechanism for Bluetooth Low Energy (BLE) using the Kyber-512 algorithm. Integrates Kyber-512 into BLE without altering the BLE core specification, implemented through a custom (Generic Attribute Profile) GATT service for wider compatibility with legacy BLE devices. [46]. Their findings include:

- With the minimum MTU size (65 bytes), the PQKE pairing latency increased to approximately 2.94 seconds, compared to 0.33 seconds for BLE SC at a distance of 0.05 m. However, increasing the MTU to 185+ bytes reduced latency substantially, bringing PQKE performance within 1.2–1.6× of BLE SC
- Enabling DLE eliminated fragmentation at the L2CAP layer, significantly improving throughput. For instance, a DLE-enabled configuration with MTU = 185 bytes led to pairing times under 1 second, far closer to BLE SC performance.
- Latency increased slightly under non-Line-of-Sight and longer distances (up to 3m), but remained within a feasible range. Even in the worst-case pairing configuration (low MTU and no DLE), PQKE time was still under 4 seconds.

Table VII is a comparison that captures average pairing latency (in seconds) between BLE SC and PQKE in key configurations.

TABLE VII: Comparison of BLE SC and PQKE Pairing Latencies

L2CAP PDU: Maximum size of BLE Link Layer packet payload after adaptation by the Logical Link Control and Adaptation Protocol. Affects data fragmentation efficiency.

| Configuration | ATT MTU | L2CAP PDU | DLE | Avg. SC Time (s) | Avg. PQKE Time (s) | Slowdown Factor |
|---|---|---|---|---|---|---|
| Default BLE SC | 65 | 27 | No | 0.33 | — | — |
| PQKE: Low MTU, no DLE | 65 | 27 | No | — | 2.94 | 8.9× |
| PQKE: Medium MTU (185), DLE | 185 | 185 | Yes | — | 0.69 | ∼2.1× |
| PQKE: High MTU (400), DLE | 400 | 251 | Yes | — | 0.46 | ∼1.4× |

*2) Enabling Quantum-Resistant EDHOC: Design and Performance Evaluation*

Pocero Fraile et al. introduce PQ-EDHOC, a post-quantum variant of the EDHOC protocol designed for constrained IoT devices. By replacing classical ECDH and ECDSA with post-quantum algorithms such as ML-KEM and HAWK, the protocol ensures quantum-resistant key exchange and authentication. Implemented on a Nordic nRF52840 over BLE, PQ-EDHOC demonstrates strong performance and efficiency, with the handshake securely establishing a shared session key using compact, quantum-safe credentials. [47]

The proposed PQ-EDHOC handshake is shown in Figure 3.

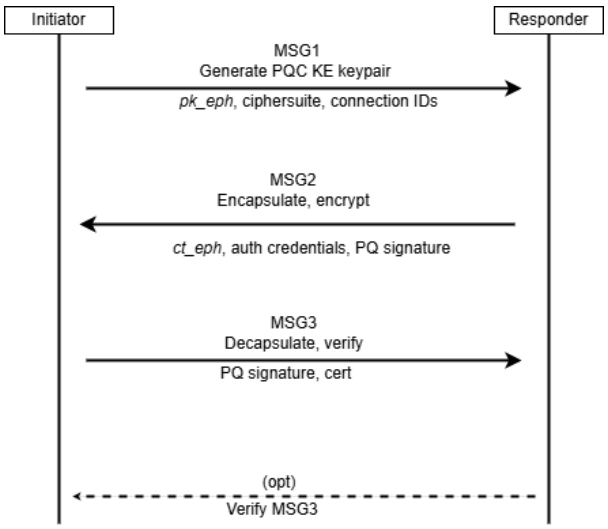



Fig. 3: PQ-EDHOC handshake messages, adapted from Fig.1 in Pocero Fraile et al. [47].

Table VIII summarizes their findings in terms of handshake time, energy consumption, and memory usage.

## *D. Challenges*

- Post-quantum key establishment (PQKE) faces implementation challenges due to limited computational resources and large key sizes in embedded systems.

TABLE VIII: Summary of PQ-EDHOC evaluation findings.

| **Aspect** | **Description / Findings** |
|---|---|
| Most Efficient Cipher Suite | **ML-KEM-512 + HAWK1** exhibited the best overall performance, offering the lowest handshake time, minimal memory use, and the least energy consumption. |
| Energy Efficiency | ML-KEM-512/HAWK1 consumed approximately **80% less energy** than classical ECDSA/secp256r1 when tested over BLE. |
| Handshake Time | ML-KEM-512/HAWK1 achieved a handshake time approximately **54% faster** than classical ECDH/ECDSA. Other suites showed slower times due to larger signature sizes. |
| RAM Usage | ML-KEM-512/HAWK1 used about **13% more RAM** than the classical baseline, while heavier suites (e.g., BIKE1/FALCON1) used up to **474% more**, exceeding embedded constraints. |
| FLASH Usage | All evaluated cipher suites stayed within the **1MB Flash limit** of the test platform. However, **BIKE1 and FALCON1** consumed up to **59% more** Flash than the classical reference. |
| Real-World BLE Test | All cipher suites were successfully tested over **BLE/6LoWPAN**, except **HQC1 and BIKE1**, which failed due to **memory limitations** on the target platform. |

- Bluetooth Low Energy (BLE) imposes restrictions such as restricted ATT MTU sizes and platform-specific limitations, which hinder efficient transmission of PQ messages.
- Incorporating and validating PQ-X.509 certificates within EDHOC's compact message format presents a significant engineering challenge, particularly for handling certificate chains and revocation mechanisms.

### *E. Research Gaps*

- Most prior work on PQC focuses on TLS-based protocols, with limited research addressing RF-based communication protocols such as BLE and Zigbee, which are widely used in IoT.
- There is limited analysis of hybrid cipher suites combining classical and PQ primitives, particularly regarding their impact on protocol agility and backward compatibility.

### *F. Future Work*

- Broaden the deployment of PQKE across BLE-based systems, including the exploration of alternative sets of parameters ML-KEM and other candidates for PQ KEM.
- Improve or adapt memory-heavy algorithms (e.g. HQC1) for viability on constrained embedded platforms.
- Incorporate additional PQ algorithms as standardization progresses, prioritizing those designed for lightweight cryptographic use.
- **Hybrid Cipher Suite Support:** Extend PQ-EDHOC to support hybrid and agile cipher suites in accordance with the evolving IETF guidelines.

### *G. Summary*

Research on post-quantum integration within the Bluetooth protocol remains limited. Although a few studies have examined the use of post-quantum algorithms, hybrid approaches have not yet been explored in this context.

This indicates a clear need for continued and focused research at the lower layers of communication protocols. Advancing post-quantum security in Bluetooth, alongside ongoing efforts at higher protocol layers, is essential to achieving end-to-end quantum-resistant communication.

## V. Email Security (S/MIME and OpenPGP)

### *A. Introduction to Email Security and the Quantum Threat*

Email remains a cornerstone of digital communication, facilitating everything from personal correspondence to critical business and governmental exchanges. The security of this medium, traditionally safeguarded by established cryptographic protocols, faces an unprecedented challenge with the advent of quantum computing. This section examines the current landscape of secure email, focusing on S/MIME and OpenPGP, and analyzes the profound implications of the quantum threat, particularly concerning the integration of post-quantum (PQ) secure signatures and the complex interoperability challenges arising during this critical transition.

### *B. Overview of S/MIME and OpenPGP: Foundations of Secure Email Communication*

Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP), including its open standard implementation OpenPGP, represent the two predominant technologies for securing email communications. Both aim to ensure confidentiality, authenticity, and integrity, yet they diverge significantly in their underlying architectures, trust models, and operational paradigms.

S/MIME is a security-enhanced version of Multipurpose Internet Mail Extensions (MIME), designed to process both plain text and multimedia files [48]. It provides confidentiality through encryption and assures authenticity and data integrity via digital signatures [48]. The cryptographic foundation of S/MIME is public-key cryptography, where senders utilize recipients' public keys for encryption, and only intended recipients with corresponding private keys can decrypt messages [49]. For digital signatures, the sender's private key generates a unique signature that recipients verify using the sender's public key, confirming identity and ensuring message integrity [49].

S/MIME's operational model is rooted in a hierarchical Public Key Infrastructure (PKI), where users obtain public-private key pairs and digital certificates from trusted Certificate Authorities (CAs) [48]. This centralized trust model implies that certificate validity is vouched for by the CA, which acts as the governing body for issuing digital certificates and providing unique identities [48]. This reliance on certificates and robust PKI infrastructure typically makes S/MIME more expensive to implement and maintain [48].

In contrast, OpenPGP operates on a decentralized "Web of Trust" model. Instead of relying on centralized CAs, users validate each other's keys through digital signatures, fostering a distributed network of trust [48]. PGP employs hybrid cryptographic methods, combining symmetric-key and public-key cryptography, where asymmetric encryption handles key exchange and digital signatures while symmetric-key cryptography manages bulk data encryption [48]. Due to its decentralized nature and lack of reliance on commercial CAs, OpenPGP is generally considered a less expensive solution compared to S/MIME [48].

The fundamental difference in trust models between S/MIME and OpenPGP significantly influences their respective paths to post-quantum readiness. S/MIME's reliance on PKI enables more controlled and standardized rollout

TABLE IX: Comparative Analysis of S/MIME and OpenPGP Trust Models and PQC Migration Implications

| **Aspect** | **S/MIME** | **OpenPGP** |
|---|---|---|
| Trust Model | Centralized PKI (Certificate Authorities) | Decentralized Web of Trust |
| Key Management | CA-issued certificates, hierarchical validation | User-generated keys, peer validation |
| PQC Migration Strategy | Top-down standardization through CAs, controlled rollout of hybrid certificates | Bottom-up, community-driven adoption, individual user updates |
| Migration Coordination | Centralized coordination via PKI infrastructure | Distributed coordination, potential fragmentation |
| Backward Compatibility | CA-managed dual certificates, uniform client updates | User-dependent key re-signing, varied adoption rates |
| Integration Complexity | PKI infrastructure upgrades, certificate lifecycle management | Client software updates, user education requirements |

of PQ-secure certificates, as CAs can issue hybrid certificates and clients can be uniformly configured to trust new formats. However, this centralized approach introduces potential bottlenecks if CA infrastructure is slow to adapt. Conversely, OpenPGP's decentralized nature means PQC adoption depends largely on individual user and client software updates, risking fragmentation but providing inherent flexibility without single points of control.

### *C. The Quantum Threat: Cryptographic Vulnerabilities and Timeline Projections*

The advent of quantum computing poses an existential threat to public-key cryptographic systems underpinning email security. Quantum computers leveraging Shor's algorithm can solve integer factorization and discrete logarithm problems exponentially faster than classical computers [50]. This directly compromises widely used asymmetric cryptographic systems such as RSA, which relies on factoring large integers, and Elliptic Curve Cryptography (ECC), which depends on the elliptic curve discrete logarithm problem [50].

Projections for practical quantum attacks on RSA-2048 vary significantly: conservative scenarios suggest breach by 2040, moderate scenarios place it between 2030 and 2035, and aggressive scenarios indicate potential compromise as early as 2027 [50]. While symmetric cryptosystems like AES are generally quantum-safe against Shor's algorithm, Grover's algorithm can reduce their effective security by half, mitigated by doubling key sizes (e.g., AES-128 to AES-256) [51].

The "harvest now, decrypt later" (HNDL) threat is particularly critical for email security. Emails encrypted with current RSA or ECC algorithms can be intercepted and stored today, then decrypted when quantum computers become available [50]. This is especially concerning for data requiring long-term confidentiality intellectual property, personal identifiable information (PII), medical records, and classified government information often have confidentiality requirements spanning decades [51]. This transforms PQC adoption from a reactive measure into a proactive strategic imperative, as reflected in early adopters like Tuta Mail implementing hybrid PQC [52] and regulatory pushes for PQC adoption by 2030 [53].

### D. Post-Quantum Cryptography Integration Strategies

#### 1) IETF LAMPS Working Group: S/MIME Standardization

The IETF LAMPS Working Group (Limited Additional Mechanisms for PKIX and S/MIME) is specifically chartered to update X.509 certificate documents (PKIX) and electronic mail security documents (S/MIME) [54]. This mandate includes maintaining essential protocols such as Certificate Management Protocol (CMP), Cryptographic Message Syntax (CMS), and S/MIME protocols while addressing quantum threats to widely deployed public key algorithms [54].

LAMPS is actively developing formats, identifiers, enrollment procedures, and operational practices for hybrid cryptographic approaches. This includes hybrid key establishment combining shared secret values from traditional Key Encapsulation Mechanisms (KEMs) with NIST PQC KEMs (e.g., ML-KEM) using Key Derivation Functions like HKDF [54]. Additionally, the group works on dual or composite signatures combining traditional signature algorithms with NIST PQC signature algorithms (e.g., ML-DSA, SLH-DSA) [54].

To address increased PQC signature sizes and bandwidth impacts, particularly for constrained devices, LAMPS investigates techniques for streamlined processing, such as using unsigned X.509 certificates to convey subject information [54]. Recent progress includes ML-DSA and SLH-DSA in Working Group Last Call (WGLC), with drafts for Composite ML-DSA and Composite ML-KEM adopted [55]. However, open design issues persist, particularly concerning ML-DSA pre-hash modes and practicalities of KEM certificate issuance from PKI [55].

#### 2) OpenPGP Working Group: Decentralized PQC Integration

The OpenPGP Working Group initiated a dedicated project in March 2022 to integrate PQC into OpenPGP protocol without disrupting existing deployments [56]. Current draft implementations define hybrid approaches: ML-KEM combined with X25519 and X448 for key establishment, and ML-DSA combined with Ed25519 and Ed448 for signatures [56]. SLH-DSA is being defined as a standalone public key signature scheme within OpenPGP context [56].

The OpenPGP group has adopted drafts for specific hybrid combinations, including ML-DSA-65+Ed25519, ML-DSA-87+Ed448, ML-KEM-768+X25519, and ML-KEM-1024+X448 [55]. Implementation progress includes GnuPG 2.5.1 released with FIPS-203 (ML-KEM) support [57], and its underlying cryptographic library, Libgcrypt 1.11, now supporting common quantum-resistant algorithms [57]. Projects like PQC@Thunderbird (funded by BSI) and Proton (using OpenPGP.js and GopenPGP libraries) actively implement the OpenPGP PQC draft [56].

#### 3) Hybrid Cryptographic Approaches: Balancing Security and Compatibility

Hybrid cryptographic schemes combining classical and post-quantum algorithms serve as crucial transition strategies, driven by several compelling rationales. Primary among these is considerable uncertainty surrounding long-term robustness of new PQC algorithms [58]. Unlike classical algorithms with decades of scrutiny, PQC algorithms are relatively new, and their resilience to unforeseen weaknesses remains under evaluation [58]. Hybrid schemes provide prudent hedges against these uncertainties while ensuring backward compatibility during graceful, phased migration [51].

**Hybrid Key Establishment**

Hybrid key establishment combines shared secret values from traditional key-establishment algorithms (e.g., ECDH, X25519, RSA-OAEP) with NIST PQC algorithms (e.g., ML-KEM), securely combining them using Key Derivation Functions such as HKDF [54]. Real-world implementations demonstrate this approach's viability.

Apple's iMessage PQ3 protocol employs hybrid design combining post-quantum Kyber-1024 Key Encapsulation Mechanism (KEM) public key with classical P-256 Elliptic Curve key agreement public key [59]. To manage larger wire sizes associated with PQC keys, PQ3 employs quantum-secure rekeying periodically rather than with every message, amortizing message size overhead while balancing user experience in limited connectivity scenarios and optimizing server capacity [59].

Tuta Mail has re-engineered its cryptographic protocol to integrate Kyber with AES-256 and ECDH x25519 in hybrid setup for asymmetric public key encryption of emails [52]. This hybrid approach protects against HNDL threats, requiring attackers to break both PQC and classical cryptography to compromise data [52]. New users automatically benefit from PQC by updating to the latest app version, with gradual rollout planned for existing users [52].

**Dual/Composite Signatures**

Dual/composite signature approaches combine traditional signature algorithms (e.g., ECDSA, RSA) with NIST PQC signature algorithms (e.g., ML-DSA, SLH-DSA) [54]. Microsoft encourages composite approaches, recommending ML-DSA use alongside existing algorithms like ECDSA or RSA during transition periods [60]. Research prototypes demonstrate viability of hybrid digital signature schemes based on combinations like ECDSA and Dilithium, designed to maintain security even if one underlying building block is compromised [61].

However, challenges exist for offline or non-negotiated protocols like S/MIME email. It becomes difficult to determine which signature type (classical or PQC) is intended when using multiple certificates or parallel PKIs [62]. Although Cryptographic Message Syntax (CMS), used by S/MIME, theoretically supports multiple SignerInfos for dual signatures, not all clients implement this feature correctly, leading to practical interoperability issues [62].

### *E. Industry Implementation: Microsoft's Email Security PQC Strategy*

Microsoft is actively integrating PQC into its email ecosystem, particularly focusing on S/MIME infrastructure and Exchange Server security. Microsoft's Active Directory Certificate Services (ADCS) enhancements specifically target email certificate issuance, allowing Certificate Authorities to issue PQC-based S/MIME certificates for secure email communication [60]. Through Intune, organizations can now enroll users for quantum-safe email certificates, enabling automatic deployment of PQC S/MIME certificates across enterprise email clients [60].

Microsoft's email security strategy emphasizes hybrid S/MIME implementations, encouraging the use of ML-DSA alongside existing algorithms like ECDSA or RSA for email signatures during the transition period [60]. This composite approach ensures email remains readable by legacy clients while providing quantum resistance for future-compatible systems. For email transport security, Microsoft strongly recommends transitioning Exchange Server configurations to TLS 1.3, as older TLS protocols used for SMTP over TLS remain vulnerable to quantum attacks [53].

The company's email-focused crypto agility approach enables Exchange administrators to seamlessly upgrade S/MIME certificate profiles and email encryption policies as PQC standards evolve [60]. This includes automated key rotation for email certificates and backward-compatible message formatting that supports both classical and post-quantum S/MIME signatures [63]. Microsoft recognizes that secure email migration requires coordinated updates across Exchange servers, Outlook clients, mobile email applications, and PKI infrastructure to maintain interoperability during the quantum transition [60].

### *F. PKI and Key Management Considerations for PQC Integration*

PQC algorithm integration introduces significant complexities for existing PKI and key management practices crucial for secure email deployment. Issuing PQC or hybrid certificates from PKI presents new hurdles. Key Encapsulation Mechanism (KEM) keys like ML-KEM are designed for key exchange and cannot inherently create digital signatures typically required for self-signed certificates or Certificate Signing Requests (CSRs) [55]. Solutions being explored include server-generated private keys or using already-issued signing certificates to sign KEM CSRs [55].

Larger public keys and signatures associated with PQC algorithms translate into larger certificate sizes, significantly impacting bandwidth, particularly for constrained devices [54]. LAMPS WG actively explores mitigation techniques, such as using unsigned X.509 certificates to convey subject information [54]. Deploying hybrid signatures introduces new complexities for PKI and CAs in managing key revocation and ensuring Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) protocols prevent synchronization failures [64].

Key management faces substantial challenges. Sensitive data with long or indefinite retention periods renders it vulnerable to future decryption if encrypted with legacy algorithms [65]. This necessitates re-encryption of stored data using PQC algorithms to ensure long-term confidentiality [51]. Organizations must undertake comprehensive inventories and prioritization of their most sensitive data, understanding where cryptography is employed within their systems [65].

### *G. Interoperability Challenges During Post-Quantum Transition*

#### *1) Technical Hurdles: Message Format Changes and Performance Overhead*

PQC algorithm adoption imposes practical technical challenges on email message formats, system performance, and resource utilization. Hybrid S/MIME content types and attachment extensions can lead to new email formats that existing mail servers and clients may not recognize [66]. This lack of recognition can cause mail servers to modify message headers, block emails entirely, or issue warnings to recipients, leading to delivery failures or user confusion [66].

Performance overhead represents another major consideration. PQC algorithms necessitate larger keys and signatures compared to classical counterparts. Dilithium signatures range from 2.4 to 4.6 KB, SPHINCS+ can reach 40KB, and ML-KEM public keys and ciphertexts range between 800-1568 bytes and 768-1568 bytes respectively [51]. These larger cryptographic elements contribute to increased overall message sizes, particularly when hybrid modes are employed [51].

While some PQC algorithms like Dilithium are relatively fast for signing and verification [67], PQC algorithms generally demand more computational resources than classical ones [51]. This increased computational load can impact system performance and affect handshake latency in protocols like TLS [60]. Resource constraints further complicate deployment, as larger signature sizes consume more bandwidth, potentially making utilization prohibitive for constrained devices [54].

*2) Algorithm Negotiation and Backward Compatibility in Non-Negotiated Protocols*

S/MIME email characteristics as ”offline” or ”non-negotiated” protocol present specific challenges for algorithm negotiation and maintaining backward compatibility [62]. Unlike protocols such as TLS, VPN, or SSH, S/MIME senders and recipients do not actively negotiate cryptographic algorithms in real-time before message transmission [62]. In negotiated protocols, clients can advertise supported signature algorithms, allowing servers to select appropriate algorithms and certificates for sessions [62]. This active negotiation mechanism is absent in S/MIME.

When organizations implement dual certificates or parallel PKIs (e.g., one classical and one PQC certificate for the same entity), it becomes difficult for S/MIME clients to determine which signature type is intended for given documents [62]. This complexity is ”forwarded to the client” [62], placing significant burden on end-user applications to manage cryptographic choices without explicit protocol-level negotiation. While CMS theoretically allows multiple SignerInfos supporting dual signatures, not all clients implement this feature correctly, leading to practical interoperability issues in real-world deployments [62].

### *H. Real-World Implementation Experiences and Lessons Learned*

Early deployments provide critical insights, confirming technical feasibility while highlighting significant operational, performance, and interoperability challenges. Tuta Mail and Apple’s iMessage demonstrate that hybrid protocols can effectively secure emails, protecting against HNDL threats by requiring attackers to break both classical and PQC algorithms [52], [59]. Prototypes aim to ensure simple user experiences by handling hybrid cryptography at the cryptographic layer, minimizing end-user friction [66].

However, practical challenges are substantial. Mail server processing issues occur when existing email plugins, policies, or anti-malware systems modify message headers, block emails, or issue warnings due to unrecognized hybrid S/MIME content types [66]. Compatibility with existing systems presents broad challenges, as transition necessitates updating and replacing cryptographic infrastructure across diverse platforms and applications [60].

Mitigation strategies emerging from early deployments include consistent adoption of hybrid designs ensuring overall security posture never weaker than existing protocols [52], strategies like periodic rekeying to amortize overhead associated with larger PQC key sizes [59], and building solutions with crypto agility enabling resilience to different algorithms and easy upgrades to future standards [60].

### *I. Future Directions and Strategic Recommendations*

The transition to post-quantum email security requires comprehensive strategic approaches. Organizations must conduct cryptographic inventories prioritizing sensitive data with long confidentiality periods, implement hybrid cryptography strategies combining classical and PQC algorithms, and prioritize crypto agility in security architectures

[65]. Engaging with standardization efforts and industry partners is vital for ensuring interoperability, adhering to NIST PQC standards and IETF LAMPS/OpenPGP Working Group specifications [54].

Addressing performance and resource implications proactively through benchmarking and testing PQC algorithms within specific environments is necessary [60]. Securing executive buy-in and allocating sufficient resources is non-negotiable, as PQC migration represents strategic investment requiring strong leadership and dedicated teams [68].

Research gaps extend beyond algorithmic optimization to include interoperability, tooling, PKI evolution, and user experience [64]. Success of PQC adoption is intrinsically linked to widespread updates across diverse platforms and applications [60], necessitating ”whole-of-ecosystem” approaches where cryptographers, software engineers, system administrators, policymakers, and end-users play coordinated roles. Future research must increasingly adopt interdisciplinary perspectives, moving beyond isolated cryptographic problems to address complex interplay of technical, operational, and human factors determining quantum-safe email security success.

## VI. Internet Protocol Security(IPsec)

### A. Overview of IPsec

IPsec is a protocol suite that secures IP communications by employing cryptographic algorithms to ensure confidentiality, integrity, and authentication. It uses symmetric encryption algorithms to encrypt packet payloads, protecting data from unauthorized access [69]. For integrity and authentication, IPsec applies HMAC in combination with hash functions like SHA-2 [70]. Key management is handled through the Internet Key Exchange (IKE) protocol, which uses Diffie-Hellman key exchange to securely negotiate cryptographic parameters and establish Security Associations (SAs) [71]. IPsec operates through two main protocols: Encapsulation Security Payload (ESP), which provides encryption and authentication, and Authentication Header (AH), which offers authentication without encryption. These mechanisms collectively enable secure and authenticated communication over IP networks.

### B. The Impact of Quantum Computing on IPsec

IPsec faces a significant quantum threat due to its reliance on traditional public-key cryptographic algorithms such as RSA and Diffie-Hellman (DH) for authentication and key exchange, particularly within the Internet Key Exchange (IKE) protocol. These algorithms are vulnerable to quantum attacks, notably Shor’s algorithm, thereby rendering RSA and DH insecure once large-scale quantum computers become practical. This vulnerability poses a critical risk to the confidentiality and authenticity of IPsec-protected communications, especially for data requiring long-term secrecy. To mitigate this risk, the IETF has proposed hybrid authentication schemes for IKEv2 that combine traditional and PQC algorithms [72], or integrating Post-quantum Preshared Keys (PPKs) into the protocol [73], ensuring continued security as long as at least one algorithm remains unbroken. The following section reviews research efforts aimed at developing quantum-resistant IPsec protocols.

### C. IPsec Post-Quantum Integration Strategies

#### 1) Real-World Quantum-Resistant IPsec

Herzinger et al. [74] investigated the real-world feasibility and security of integrating PQC into the IKEv2 protocol used in IPsec by implementing and evaluating three proposed IETF drafts [75], [76], [77] designed to integrate

PQC key exchanges into the protocol. They extended OpenIKED to support intermediate exchanges [75], large payloads [76], and follow-up exchanges [77], enabling hybrid configurations using classical algorithms alongside PQC schemes like FrodoKEM and McEliece.

Through a series of experiments simulating real-world network conditions, they assessed the performance and resilience of these mechanisms. Their findings revealed that while the combined protocol is functionally viable, it suffers from high complexity, configuration risks, and severe performance degradation over lossy or bandwidth-constrained networks.

Table X summarizes their findings under 100 Mbps and 1 Mbps conditions with varying error rates.

TABLE X: Performance of Post-Quantum IKEv2 Handshake under Varying Network Conditions

| **Network Condition** | **Throughput** | **Packet Loss** | **Observed Performance** | **Reliability** | **Notes** |
|---|---|---|---|---|---|
| Ideal (Lab) | 100 Mbps | 0–0.5% | Fast handshake times (median $<$ 2 seconds) | High | Suitable for stable datacenter links |
| Moderate Degradation | 100 Mbps | 1–2% | Handshake times increase; occasional failures | Moderate | Performance remains usable |
| Lossy Wired/Wireless | 100 Mbps | 5%+ | Frequent handshake failures and retransmissions due to fragment loss | Low | High packet loss overwhelms McEliece's fragmentation overhead |
| Constrained Bandwidth | 1 Mbps | $<$1% | Long handshake durations; high delay even at low loss | Moderate–Low | Unsuitable for time-sensitive or mobile deployments |
| Worst Case | 1 Mbps | $\geq$2% | Most handshakes failed or exceeded acceptable duration | Very Low | Performance breakdown in embedded or wireless environments |

Based on these results, they proposed an alternative design that eliminates intermediate exchanges and instead integrates a hybrid key exchange; combining classical and lightweight post-quantum algorithms (e.g., ECDH + FrodoKEM), directly into the initial `IKE_SA_INIT` message. Larger PQC algorithms such as McEliece are deferred to a single, authenticated follow-up exchange after `IKE_AUTH` to mitigate DoS risks. This streamlined design reduces protocol complexity, minimizes misconfiguration risks, and improves maintainability without compromising long-term security.

*2) A Formal Analysis of IKEv2's Post-Quantum Extension*

Gazdag et al. [78] conducted the first formal security analysis of the IKEv2 handshake under a quantum-capable threat model, referred to as *Minimal-IKEv2*. Their study demonstrated that the standard protocol becomes vulnerable in the presence of quantum adversaries. Utilizing the Tamarin Prover, they automated the verification of both classical and post-quantum-enhanced variants of IKEv2.

The authors evaluated a proposed extension that augments the traditional Diffie–Hellman key exchange with multiple quantum-resistant key exchanges. They do not specify exact PQC algorithms used in their formal model. Their results show that this hybrid approach successfully restores the desired security properties. Furthermore, they provided open-source verification code[1], enabling reproducibility and facilitating future research. The study also highlighted the practical challenges involved in verifying complex cryptographic protocols.

[1]https://github.com/mnm-team/tamarin-ikev2

Their key findings include:

- IKEv2 satisfies all intended security properties in the classical setting, provided that no specific keys are compromised. Notably, the protocol remains robust against most attacks unless the responder's static key is leaked.
- The `IKE_INTERMEDIATE` extension, when used with quantum-resistant key exchanges, preserves the security properties of the original protocol. The formal model confirms that this extension does not introduce new vulnerabilities.
- The results are consistent with previous analyses using tools such as Scyther, thereby reinforcing the correctness and reliability of the proposed model.

*3) A Performance Evaluation of IPsec with Post-Quantum Cryptography*

Bae et al. [79] present a comprehensive performance evaluation of the integration of PQC algorithms into the IPsec protocol, specifically focusing on IKEv2. They assess the trade-offs between security and performance by analyzing execution speed and packet size across various PQC Key Encapsulation Mechanisms (KEMs), including NIST Round 3 finalists (Kyber, NTRU, Saber) and regionally developed algorithms RLizard from Korea, LAC and AKCN from China). The evaluation is implemented using strongSwan, a widely used open-source IPsec implementation, with custom integration of PQC algorithms via the liboqs library.

These are their findings:

- Higher security levels in IPsec with PQC generally lead to increased latency and packet sizes, with Kyber and Saber showing around 40% performance degradation and RLizard experiencing particularly severe drops in performance and packet efficiency at higher security tiers.
- Kyber512 and LightSaber delivered the fastest performance in both KEM and IKEv2 stages at lower security levels, NTRU-HPS-2048509 achieved the quickest encapsulation time, while AKCN-SEC showed the highest latency and packet sizes due to its large parameter set.
- Packet sizes scaled proportionally with public key and ciphertext sizes across all algorithms, with RLizard and AKCN exhibiting the most significant increases, thereby degrading overall network performance.

*4) Quantum-Resistant MACsec and IPsec for Virtual Private Networks*

Gazdag et al.[80] initiate the standardization process for quantum-resistant Virtual Private Networks (VPNs) at Layers 2 (MACsec) and 3 (IPsec) of the OSI model by utilizing the MACsec/MKA and IPsec/IKEv2 protocols, respectively. They propose practical hybrid and post-quantum cryptographic (PQC) enhancements to the key exchange mechanisms of these protocols.

For IPsec, they implement and evaluate several integration strategies within the IKEv2 protocol, including the use of compact post-quantum keys in the initial handshake, intermediate exchanges for larger keys, support for fragmentation to transmit large payloads, and deferring post-quantum key exchange to later phases. However, they did not test post-quantum certificates for authentication in their IPsec setup. Example algorithms used include classical Diffie-Hellman, NTRU Prime, CRYSTALS-Kyber, and FrodoKEM-640. These approaches were tested for performance and reliability, and the authors contributed to ongoing standardization efforts at the IETF.

Their findings highlight that:

- VPN protocols should ideally combine classical and post-quantum cryptography for resilience, while remaining crypto-agile to accommodate future cryptographic updates.
- IPsec should efficiently handle large post-quantum keys, support fast initial handshakes, and allow integration of multiple cryptographic schemes (e.g., via `IKE_INTERMEDIATE`), though this may increase complexity and latency.
- Large-key schemes like McEliece are impractical in many networks due to fragmentation issues, whereas smaller and more efficient schemes like FrodoKEM offer strong security with minimal performance impact, making them more suitable for most use cases.

*5) Performance Evaluation of Quantum-Resistant IKEv2 Protocol for Satellite Networking Environments*

Mutlugun et al. [81] present a comprehensive evaluation of integrating PQC algorithms into IKEv2 protocol used for IPSec framework, motivated by the emerging threat that quantum computing poses to classical cryptographic schemes. The study explores the performance implications of deploying PQC within IKEv2, particularly in satellite communication environments characterized by high propagation delays and packet loss.

To perform this evaluation, the authors use a StrongSwan Open Source VPN implementation enabled with PQ, simulating various network conditions to assess the impact of key PQ KEMs and digital signatures on latency, fragmentation, and reliability. The experimental setup included comparison between classical cryptographic algorithms like RSA, ECDSA, ED25519, and Curve25519 (x25519) and post-quantum algorithms such as Kyber, Falcon and Dilithium.

Their findings reveal that PQ algorithms, especially those with larger key and signature sizes such as Dilithium, introduce significant message fragmentation and are more susceptible to packet loss, leading to increased latency and retransmissions. However, the study also demonstrates that the high propagation delays inherent in satellite communications can partially offset these performance drawbacks. Under certain conditions, particularly with moderate packet loss and higher latency, Falcon and Dilithium exhibit performance levels that approach those of classical cryptographic solutions, suggesting their potential viability in future satellite-based secure communication systems.

*6) Quantum-Resistant IPsec: Triple-Hybrid Key Exchange and Derivation*

Garcia et al. [28] present a novel triple-hybrid cryptographic framework that integrates classical cryptography, PQC and QKD into both TLS 1.3 and IPsec. This section focuses on their IPsec implementation, while TLS is discussed separately in the TLS section II-C5.

For IPsec, the authors implemented their solution using the `strongSwan` VPN stack and followed the IETF's RFC 9370, which enables multi-key exchange in IKEv2. Their approach integrates three key exchange mechanisms: classical (X25519), post-quantum (ML-KEM-1024), and QKD. Authentication is handled using CRYSTALS-Dilithium (ML-DSA-65), and symmetric encryption is performed using AES-256-GCM.

To combine the keys, the authors employed a cascade-based approach for IKE SA (control plane) key derivation, where each new shared secret (from classical, PQ, and QKD exchanges) is sequentially incorporated into the key derivation process using a pseudorandom function (PRF), updating the key seed (`skeyseed`) at each step. This

layered derivation ensures that the final key material is secure unless all underlying cryptographic assumptions are broken.

For the data plane (child SAs), a concatenation-based approach is used. Here, all shared secrets are combined at once and fed into a PRF+ function to derive the final key material. This separation of methods allows for efficient and secure key management across both control and data planes.

Their findings show that the triple-hybrid key exchange adds approximately 34 milliseconds of overhead, while QKD key retrieval contributes an additional $\sim$30 milliseconds. Importantly, this overhead is confined to the control plane, with no measurable impact on data plane performance. This makes the solution practical for real-world deployment, offering strong quantum resilience without sacrificing throughput or latency in encrypted traffic.

### *D. Challenges*

1) Poorly configured hybrid key exchanges, which may result from integration challenges, can expose the handshake process to downgrade attacks.
2) The increased computational and transmission overhead associated with post-quantum cryptographic (PQC) algorithms leads to performance degradation and packet fragmentation in networks.
3) High latency and limited bandwidth in satellite networks further exacerbate the performance degradation introduced by PQC.
4) Network-induced variability affects latency measurements, necessitating careful interpretation of experimental results.
5) QKD is constrained by the secret key rate (SKR) and transmission distance, and requires trusted nodes and dedicated infrastructure. Integration with classical networks remains essential for achieving quantum resistance.

Research Gaps

1) Existing literature predominantly focuses on PQC-only integration, with fewer studies exploring classical-PQC hybrid approaches.
2) Most evaluations are conducted in controlled LAN environments; performance in real-world, high-latency, or lossy networks remains underexplored.
3) There is a need for more efficient fragmentation and reassembly mechanisms to accommodate large PQC key sizes.
4) While performance evaluations are common, comprehensive security analyses of PQC integration in IKEv2 under adversarial conditions are lacking.
5) There is a lack of standardized methods for integrating QKD into mainstream communication protocols.

### *E. Future Work*

1) Conduct field tests across diverse network environments to evaluate real-world feasibility and resilience of PQC integration.
2) Explore additional classical-PQC hybrid schemes to balance security and performance during the transition to quantum-resistant systems.

3) Investigate compression techniques, message batching, and adaptive fragmentation strategies to mitigate PQC-induced overhead. Further algorithmic and implementation-level optimizations are also needed to reduce latency and packet size.
4) Examine the potential of quadruple or quintuple hybrid models, although current benefits appear limited.

### *F. Summary*

IPsec's reliance on RSA and DH in IKEv2 renders it vulnerable to quantum attacks. Hybrid key exchange schemes that combine classical cryptography with post-quantum algorithms or even QKD can restore long-term confidentiality and authenticity, as supported by both experimental evaluations and formal security proofs. However, these approaches introduce significant challenges, including increased handshake complexity, large key and signature sizes that lead to fragmentation, and heightened latency and packet loss in constrained or lossy networks. The risks of misconfiguration and infrastructure demands further complicate the deployment. Achieving practical quantum-safe IPsec will require extensive field testing across diverse network environments, adaptive fragmentation and compression strategies, modular crypto-agile implementations, and standardized integration of QKD.

## VII. Message Queuing Telemetry Transport (MQTT)

### *A. Overview of MQTT*

MQTT is a lightweight, publish-subscribe messaging protocol designed for low-bandwidth, high-latency, or unreliable networks, making it particularly suitable for Internet of Things (IoT) applications. It operates on a client-broker architecture in which devices publish messages to specific topics and other devices subscribe to those topics to receive relevant data via the broker. MQTT is widely adopted due to its minimal resource requirements, efficient message delivery, and support for multiple levels of quality of service (QoS), which ensure reliable communication even in constrained environments [82]. Its simplicity and scalability have established it as a foundational protocol for IoT data transmission [83].

### *B. Quantum Threat to MQTT*

Although MQTT itself does not define encryption or authentication mechanisms, it typically relies on TLS to secure communications. However, TLS uses public-key cryptographic algorithms such as RSA and ECC, which are vulnerable to quantum attacks. Quantum computers, once sufficiently advanced, could break these algorithms using techniques such as Shor's algorithm, rendering the current MQTT security models obsolete [4]. This poses a significant threat to IoT ecosystems, where MQTT is widely deployed, especially in critical infrastructure and privacy-sensitive applications. As a result, researchers are actively exploring PQC to replace vulnerable components and future-proof MQTT-based systems against quantum adversaries [84].

### *C. MQTT Post-Quantum Integration Strategies*

#### *1) Quantum-Resistant and Secure MQTT Communication*

Malina et al. [85] present a novel framework for integrating PQC directly into the MQTT protocol. Recognizing the limitations of TLS-based security in constrained environments and its vulnerability to quantum attacks, they

propose a multi-level, lightweight, quantum-resistant alternative that omits TLS handshakes. The solution is tailored for scenarios involving short, irregular messages and resource-constrained devices, aiming to ensure secure communication with minimal latency. Their model comprises two security levels: Security Level 1 uses Falcon for digital signatures, while Security Level 2 adds confidentiality using Kyber. Additionally, the authors compare Dilithium with Falcon to evaluate performance trade-offs, and benchmark Kyber against other NIST PQC candidates, including Classic McEliece, BIKE, and HQC, to justify its selection based on efficiency and resource requirements.

Key findings of their work include the following.

- Falcon signing is the most computationally expensive operation, requiring approximately 145 ms on a Raspberry Pi Zero.
- Kyber encapsulation and decapsulation are significantly faster, taking around 15–17 ms.
- Dilithium offers simpler signing operations, but produces larger signatures, which may impact bandwidth efficiency.
- The proposed protocol achieves a sub-300 ms latency, which makes it suitable for real-time IoT applications.
- PQC integration is practically feasible even on constrained devices.

*2) An Optimized Instantiation of Post-Quantum MQTT Protocol on 8-bit AVR Sensor Nodes*

Kim and Seo [86] address the challenge of integrating PQC mechanisms into constrained IoT environments, particularly those employing 8-bit AVR microcontrollers. They propose *KEM-MQTT*, a lightweight and secure variant of the MQTT protocol that takes advantage of the Kyber algorithm. The work introduces several optimizations that render Kyber viable on ultra-low-resource devices, enabling mutual authentication and confidentiality without relying on post-quantum digital signatures, which are typically infeasible in such environments. The KEM-MQTT model modifies the standard MQTT protocol to incorporate post-quantum security features based on Kyber, KEMTLS, PDK authentication and AEAD. Classical cryptographic algorithms, NIST P-256 and Ed25519, were used as benchmarks to evaluate performance trade-offs.

Key Findings from their study.

- The optimized Kyber-512 implementation improves execution speed for KeyGen, Encapsulation, and Decapsulation by 81%, 75%, and 85%, respectively, compared to the reference implementation on AVR.
- Constant-time implementations and masking techniques were employed to mitigate timing and power-based side-channel attacks.
- Full handshake preparation was achieved within 4.32 seconds on AVR devices, utilizing approximately 3 KB of stack memory.
- Energy consumption was estimated at approximately 71.75 mJ per handshake, which is competitive with or superior to ECC-based alternatives.

*3) Assessment of the Impact of Hybrid Post-Quantum Cryptography on the Performance of the MQTT Communication Protocol*

Rampazzo et al. [87] investigate the performance implications of integrating hybrid post-quantum cryptographic algorithms into the MQTT protocol, which is extensively employed in Industrial Internet of Things (IIoT) environ-

ments. In light of the vulnerabilities of current cryptographic standards to quantum computing threats, the authors explore the adoption of hybrid TLS protocols that combine classical and post-quantum cryptographic techniques. Their study focuses on evaluating the impact of these hybrid protocols on memory usage, CPU cycles, and network data transmission within constrained edge computing environments.

Consequently, the authors implemented a testbed that simulates a realistic IIoT environment. Two authentication configurations were evaluated: mutual authentication and broker-only authentication. The subscriber component was deliberately excluded to concentrate the analysis on the performance of the publisher during secure communication with the broker. Post-quantum algorithms such as `Kyber`, `Dilithium`, and `FALCON` were integrated in hybrid mode with classical algorithms across different NIST-defined security levels.

Key Findings:

- Hybrid TLS significantly increased the volume of transmitted data - by up to 850% in certain scenarios. However, substituting `Dilithium` with `FALCON` reduced this overhead by approximately 50%.
- `FALCON` consistently demonstrated lower memory consumption compared to `Dilithium` across all evaluated security levels.
- The increase in CPU usage was proportional to memory consumption. This impact was more pronounced under mutual authentication, but remained within manageable limits.
- Broker-only authentication significantly reduced resource consumption, making it more suitable for deployment in resource-constrained devices.
- Higher security levels (e.g.L5) did not result in proportionally higher resource usage, indicating the feasibility of employing stronger security in more capable edge devices.

*4) Post-Quantum Authentication in the MQTT Protocol*

Samandari and Gritti [88] address the challenge of integrating PQC authentication into the MQTT protocol, which is widely used in IoT environments. Given the resource constraints of IoT devices and the anticipated threat posed by quantum computing to classical cryptographic schemes, the authors investigated the feasibility and performance implications of employing post-quantum digital signatures or KEMs for MQTT authentication.

The authors therefore implement and evaluate two models for post-quantum authentication in MQTT: (i) a digital signature-based authentication model utilizing the CRYSTALS-Dilithium scheme, and (ii) a KEM-based authentication model employing CRYSTALS-Kyber to achieve more efficient authentication by replacing digital signatures with KEMs. Both models are assessed in terms of CPU usage, memory consumption, disk usage, and connection time.

From their experimental results, the authors report the following findings:

- The digital signature-based method incurs higher CPU and memory usage, increased disk activity under constrained memory conditions, and longer authentication times as security levels increase, making it less suitable for resource-limited devices.
- The KEM-based authentication model reduces authentication time by 71% compared to the digital signature approach (10 ms vs. 35 ms), with only a marginal increase in memory usage and minimal additional bandwidth overhead, making it a more efficient and practical solution for secure MQTT communication in IoT contexts.

*5) Novel Hybrid Post-Quantum Encryption Design on Embedded Devices*

Cherkaoui et al. [89] present a comprehensive framework for integrating PQC algorithms into embedded systems, with a particular emphasis on hybrid encryption schemes that combine classical ECC with lattice-based quantum-resistant methods. The authors address the emerging threat posed by quantum computing to conventional cryptographic protocols and propose a secure communication architecture that leverages CRYSTALS-Kyber and X25519 for hybrid key exchange.

A novel mechanism, termed the Secure Private Identification Key (SPID), is introduced to facilitate adaptive encryption based on device capabilities, particularly for resource-constrained platforms such as the ARM Cortex-M4. The proposed system is implemented and evaluated across both embedded and cloud environments. Its effectiveness is demonstrated through performance benchmarking and the establishment of secure communication channels using MQTT for lightweight messaging, TLS for encrypted web traffic, and IPsec tunnels for secure network-layer data transmission. Additionally, Kyber is benchmarked against other post-quantum algorithms, including NTRULPrime653 and McEliece.

Key findings from the experiments include:

- Kyber768 and X25519 achieved a balance between security and computational efficiency, while Kyber512 demonstrated efficient key exchange with moderate resource consumption.
- On the ARM Cortex-M4 platform, the SPID-based ECC scheme exhibited encryption times comparable to standard ECC, with only slight increases for larger payloads.
- The proposed architecture successfully integrated SPID and adaptive ECC into MQTT-based communication, ensuring secure and efficient data transmission.
- Cloud and network deployment validated the use of secure TLS/IPsec tunnels configured with OQS-OpenSSL and strongSwan, utilizing Kyber-based key exchange mechanisms.

### *D. Challenges*

- The latency and computational overhead introduced by TLS handshakes in MQTT communication.
- Resource limitations of IoT devices, particularly in executing computationally intensive cryptographic operations.
- The feasibility of deploying PQC algorithms on low-power platforms such as the Raspberry Pi Zero and AVR microcontrollers.
- Scalability and adaptability of PQC schemes in real-world MQTT-based deployments.

### *E. Research Gaps*

- Limited investigation of features that enhance privacy beyond conventional encryption and authentication mechanisms.
- Lack of suitable dynamic key management and revocation strategies for large-scale IoT deployments.
- Inadequate analysis of side channel vulnerabilities in customized PQC implementations for MQTT environments.

- Existing studies are predominantly experimental, with minimal focus on real-world deployment scenarios and long-term performance evaluation.

### *F. Future Work*

- Extension of the protocol to support additional privacy-preserving properties for both publishers and subscribers.
- Application of the proposed techniques to more constrained platforms, including 16-bit and 8-bit microcontrollers.
- Exploration of hardware acceleration methods to alleviate the computational burden of PQC algorithms, particularly on devices lacking floating-point units.
- Integration of formal verification techniques and threat modeling to improve the security assurance of proposed hybrid cryptographic schemes.

### *G. Summary*

MQTT is evolving beyond its reliance on classical TLS and lightweight link-layer encryption to withstand future quantum threats. Recent research efforts have embedded post-quantum primitives directly into the MQTT protocol, utilizing PQ digital signatures and KEMs for lightweight key confirmation. Given the resource-constrained nature of IoT devices, the implementation of PQC remains challenging due to performance overheads, necessitating careful consideration of trade-offs. Possible major priorities should include defining standardized PQC profiles for brokers and clients, optimizing MTU and fragmentation strategies, and developing mechanisms to ensure seamless interoperability and manage performance impacts on constrained devices. These will be useful in enabling quantum-secure MQTT deployments in real-world IoT environments.

## VIII. Conclusion

Driven by the imminent threat posed by scalable quantum computers to classical cryptographic foundations, this report presents a comprehensive survey of PQC integration across core communication protocols,TLS, SSH, Bluetooth, Email (S/MIME and OpenPGP), MQTT, and IPsec. The findings suggest that hybrid implementations, which combine classical and post-quantum primitives, offer the most realistically secure path forward, since PQC algorithms have not undergone scrutiny as much as their classical counterparts. These hybrid approaches provide strong forward-secrecy guarantees, albeit with modest impacts on latency, bandwidth, and resource consumption. Though pure post-quantum deployments are theoretically robust, they often incur prohibitive overheads, particularly in constrained or high-latency environments; hence, hybrid schemes and the use of KEMs for both key exchange and authentication.

Experimental benchmarks, real-world evaluations, and formal security analyses highlight the urgent need for standardized algorithms, well-defined interoperability profiles, and optimized platform-aware implementations. CRYSTALS-Dilithium (for authentication) and CRYSTALS-Kyber (for key exchange) consistently demonstrate superior performance and lower resource costs. Furthermore, replacing digital signatures with KEMs has been shown to reduce performance overhead. Achieving complete quantum resilience will require sustained collaboration among

cryptographers, protocol designers, and system engineers to refine hybrid schemes, mature PQC toolchains, and facilitate seamless backward compatible transitions across global communication infrastructures.

# REFERENCES


[1] T. Dierks and E. Rescorla, "RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force (IETF), 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5246

[2] T. Ylonen and C. Lonvick, "RFC 4251: The Secure Shell (SSH) Protocol Architecture," Internet Engineering Task Force (IETF), 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4251

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996. [Online]. Available: https://cacr.uwaterloo.ca/hac/

[4] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE, 1994, pp. 124–134.

[5] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Springer, 2009.

[6] N. I. of Standards and T. (NIST), "Post-quantum cryptography project," 2024, accessed June 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[7] G. Alagic *et al.*, "Status report on the fourth round of the nist post-quantum cryptography standardization process," National Institute of Standards and Technology (NIST), NIST Interagency/Internal Report (NIST IR) 8545 (Final), March 2025, accessed: 2025-07-02. [Online]. Available: https://csrc.nist.gov/pubs/ir/8545/final

[8] National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard (ml-kem)," U.S. Department of Commerce, Tech. Rep. FIPS PUB 203, August 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/203/final

[9] ——, "Module-lattice-based digital signature standard (ml-dsa)," U.S. Department of Commerce, Tech. Rep. FIPS PUB 204, August 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/final

[10] ——, "Stateless hash-based digital signature standard (slh-dsa)," U.S. Department of Commerce, Tech. Rep. FIPS PUB 205, August 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/final

[11] D. Stebila, S. Fluhrer, and S. Gueron, "Hybrid key exchange in transport layer security (tls) 1.3," Internet Engineering Task Force (IETF), RFC 9650, March 2025.

[12] M. B, J. Schinzel, T. Lange, and D. J. Bernstein, "Hybrid post-quantum key exchange in secure shell (ssh)," Internet Engineering Task Force (IETF), RFC 9710, May 2025.

[13] P. Kampanakis and T. Lepoint, "Do we need to change some things? open questions posed by the upcoming post-quantum migration to existing standards and deployments," in *Post-Quantum Cryptography*. Springer, 2023. [Online]. Available: https://eprint.iacr.org/2023/266.pdf

[14] N. Alnahawi, A. Wiesmaier, T. Grasmeyer, and J. Geißler, "On the state of post-quantum cryptography migration," in *GI Jahrestagung Informatik 2021*, 2021. [Online]. Available: https://dl.gi.de/bitstreams/dba4839d-5652-4740-8fec-7b3893ee614a/download

[15] Internet Society, "Tls basics," https://www.internetsociety.org/deploy360/tls/basics/, 2024, accessed: 2025-06-18.

[16] C. Rubio García, S. Rommel, S. Takarabt, J. J. Vegas Olmos, S. Guilley, P. Nguyen, and I. Tafur Monroy, "Quantum-resistant transport layer security," *Computer Communications*, vol. 213, pp. 345–358, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366423004012

[17] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking post-quantum cryptography in tls," in *Post-Quantum Cryptography*, J. Ding and J.-P. Tillich, Eds. Cham: Springer International Publishing, 2020, pp. 72–91. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-44223-1_5

[18] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, and G. Pereira, "Sike," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[19] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, and D. Stehlé, "Crystals-kyber," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[20] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila, "Frodokem," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[21] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[22] N. Bindel, S. Akleylek, E. Alkim, P. S. L. M. Barreto, J. Buchmann, E. Eaton, G. Gutoski, J. Kramer, P. Longa, H. Polat, J. E. Ricardini, and G. Zanon, "qtesla," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[23] G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, and V. Kolesnikov, "Picnic," National Institute of Standards and Technology, Tech. Rep., 2019, round-2 submission to the NIST Post-Quantum Cryptography project. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[24] A. A. Giron, J. P. A. do Nascimento, R. Custódio, L. P. Perin, and V. Mateu, "Post-quantum hybrid kemtls performance in simulated and real network environments," in *Progress in Cryptology – LATINCRYPT 2023*, A. Aly and M. Tibouchi, Eds. Cham: Springer Nature Switzerland, 2023, pp. 293–312.

[25] M. Anastasova, R. Azarderakhsh, and M. M. Kermani, "Fully hybrid tlsv1.3 in wolfssl on cortex-m4," in *Applied Cryptography and Network Security Workshops*, M. Andreoni, Ed. Cham: Springer Nature Switzerland, 2024, pp. 376–395.

[26] wolfSSL, "wolfssl embedded ssl library," n.d., accessed: 2025-07-02. [Online]. Available: https://www.wolfssl.com/

[27] M. Anastasova, R. El Khatib, A. Laclaustra, R. Azarderakhsh, and M. M. Kermani, "Highly optimized curve448 and ed448 design in wolfssl and side-channel evaluation on cortex-m4," in *2023 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2023, pp. 1–8, accessed: 2025-07-02.

[28] C. R. Garcia, A. C. Aguilera, C. Stan, J. J. Vegas, S. Rommel, and I. T. Monroy, "Enhanced network security protocols for the quantum era: Combining classical and post-quantum cryptography, and quantum key distribution," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2025.

[29] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila, *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange*. Springer International Publishing, 07 2019, pp. 206–226.

[30] Q. C. Report, "Openssh 10.0 introduces default post-quantum key exchange," 2025. [Online]. Available: https://quantumcomputingreport.com/openssh-10-0-introduces-default-post-quantum-key-exchange-algorithm/

[31] IETF SSHM WG, "draft-ietf-sshm-mlkem-hybrid-kex-02: Ml-kem hybrid key exchange for ssh," 2024, https://datatracker.ietf.org/doc/draft-ietf-sshm-mlkem-hybrid-kex/.

[32] A. W. Services, "Using hybrid post-quantum key exchange with aws transfer family," 2024. [Online]. Available: https://docs.aws.amazon.com/transfer/latest/userguide/post-quantum-security-policies.html

[33] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in tls1.3 and ssh," in *CoNEXT '20*, 2020.

[34] O. Q. S. project, "open-quantum-safe/openssh," 2024. [Online]. Available: https://github.com/open-quantum-safe/openssh

[35] SmartFTP, "Smartftp – ssh algorithms support," 2025. [Online]. Available: https://www.smartftp.com/en-us/client/features/ssh

[36] T. Fritsch, D. Stebila, and W. Whyte, "Hybrid key exchange in the quantum random oracle model," in *Advances in Cryptology – ASIACRYPT 2023*, 2023.

[37] D. Stebila, M. Mosca, and N. Lütkenhaus, "Post-quantum key exchange for the internet and the open quantum safe project," *IEEE Communications Magazine*, vol. 57, no. 11, pp. 40–46, 2019.

[38] A. W. Services, "Using hybrid post-quantum key exchange with aws transfer family," 2025. [Online]. Available: https://docs.aws.amazon.com/transfer/latest/userguide/post-quantum-security-policies.html

[39] R. Hat, "Post-quantum cryptography in red hat enterprise linux 10," 2025. [Online]. Available: https://www.redhat.com/en/blog/post-quantum-cryptography-red-hat-enterprise-linux-10

[40] NIST, "Post-quantum cryptography standardization project," 2024, https://csrc.nist.gov/Projects/post-quantum-cryptography.

[41] J. W. Bos *et al.*, "Efficient implementation of ml-kem: Kyber's fips 203 standardization," *Cryptology ePrint Archive*, 2023, https://eprint.iacr.org/2023/1505.

[42] Bluetooth SIG, "Bluetooth Pairing Feature Exchange," https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/, 2025, accessed: 2025-06-26.

[43] National Institute of Standards and Technology, "Guide to Bluetooth Security (NIST SP 800-121 Rev. 2)," https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final, NIST, Special Publication 800-121 Rev. 2, 2017, accessed: 2025-06-26.

[44] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC)*, 1996, pp. 212–219.

[45] S. D. and P. C., "On the practical cost of grover for aes key recovery," Presentation at the 5th PQC Standardization Conference, NIST, April 2024, uK National Cyber Security Centre; accessed 2025-06-26. [Online]. Available: https://csrc.nist.gov/csrc/media/Presentations/2024/practical-cost-of-grover-for-aes-key-recovery/images-media/sarah-practical-cost-grover-pqc2024.pdf

[46] T. Liu, G. Ramachandran, and R. Jurdak, "Towards quantum resilient iot: A backward-compatible approach to secure ble key exchange against quantum threats," in *2024 IEEE/ACM Ninth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2024, pp. 170–180.

[47] L. P. Fraile, G. Tasopoulos, C. Koulamas, R. K. Zhao, N. Haque Sultan, F. Regazzoni, and A. P. Fournaris, "Enabling quantum-resistant edhoc: Design and performance evaluation," *IEEE Access*, vol. 13, pp. 75 861–75 884, 2025.

[48] GeeksforGeeks, "Difference between pgp and s/mime," accessed July 1, 2025. [Online]. Available: https://www.geeksforgeeks.org/computer-networks/difference-between-pgp-and-s-mime/

[49] NinjaOne, "What is s/mime? — an overview," accessed July 1, 2025. [Online]. Available: https://www.ninjaone.com/it-hub/endpoint-security/what-is-s-mime/

[50] Various, "The impact of quantum computing on encryption: How quantum computers can break current encryption methods such as rsa and ecc and what this means for data security," *ResearchGate*, 2024, accessed July 1, 2025. [Online]. Available: https://www.researchgate.net/publication/390571003_The_Impact_of_Quantum_Computing_on_Encryption_How_Quantum_Computers_Can_Break_Current_Encryption_Methods_Such_as_RSA_and_ECC_and_What_This_Means_for_Data_Security

[51] Halon, "Understanding the impact of post-quantum cryptography (pqc) on email security," accessed July 1, 2025. [Online]. Available: https://halon.io/blog/post-quantum-cryptography-pqc-email-security

[52] Tuta, "Tuta launches post quantum cryptography for email," accessed July 1, 2025. [Online]. Available: https://tuta.com/blog/post-quantum-cryptography

[53] F5 Labs, "The state of post-quantum crypto (pqc) on the web," accessed July 1, 2025. [Online]. Available: https://www.f5.com/labs/articles/threat-intelligence/the-state-of-pqc-on-the-web

[54] IETF, "Limited additional mechanisms for pkix and smime," accessed July 1, 2025. [Online]. Available: https://datatracker.ietf.org/doc/charter-ietf-lamps/

[55] M. Ounsworth, "Pqc standardization at the internet engineering task force," 2025, accessed July 1, 2025. [Online]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/THU_BREAKOUT_0900_Mike-Ounsworth_PQC-Standardization-at-the-IETF.pdf

[56] FOSDEM 2025, "Post-quantum cryptography in openpgp," accessed July 1, 2025. [Online]. Available: https://fosdem.org/2025/events/attachments/fosdem-2025-5992-post-quantum-cryptography-in-openpgp/slides/238257/PQC_in_Op_AcmguXM.pdf

[57] GnuPG, "The gnu privacy guard," accessed July 1, 2025. [Online]. Available: https://www.gnupg.org/

[58] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, "Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-kem-04, 06 2025, work in Progress. [Online]. Available: https://lamps-wg.github.io/draft-composite-kem/draft-ietf-lamps-pq-composite-kem.html#name-asn1-module

[59] Apple Security, "imessage with pq3: The new state of the art in quantum-secure messaging at scale," accessed July 1, 2025. [Online]. Available: https://security.apple.com/blog/imessage-pq3/

[60] Microsoft Security Blog, "Post-quantum cryptography comes to windows insiders and linux," accessed July 1, 2025. [Online]. Available: https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803

[61] Various, "Hybrid post-quantum signatures in hardware security keys," *Cryptology ePrint Archive*, 2022, accessed July 1, 2025. [Online]. Available: https://eprint.iacr.org/2022/1225.pdf

[62] M. Ounsworth, "Architecting pki hierarchies for graceful pq migration," 2025, accessed July 1, 2025. [Online]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1200_Mike-Ounsworth_Architecting-PKI-Hierarchies-for-Graceful-PQ-Migration.pdf

[63] Google Cloud, "Post-quantum cryptography (pqc)," accessed July 1, 2025. [Online]. Available: https://cloud.google.com/security/resources/post-quantum-cryptography

[64] Various, "Quantum-resistant digital signatures via hybrid scheme," *ResearchGate*, 2024, accessed July 1, 2025. [Online]. Available: https://www.researchgate.net/publication/392071206_Quantum-Resistant_Digital_Signatures_via_Hybrid_Scheme

[65] HashiCorp, "Prioritizing data for post-quantum cryptography (pqc)," accessed July 1, 2025. [Online]. Available: https://www.hashicorp.com/blog/prioritizing-data-for-post-quantum-cryptography-pqc

[66] J. Klaußner, "Hybrid pqc e-mail communication: Easing migration pain," 2025, accessed July 1, 2025. [Online]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1430_Jan-Klau%C3%9Fner_Hybrid-PQC-E-Mail-Communication-Easing-Migration-Pain.pdf

[67] PostQuantum, "Post-quantum cryptography (pqc) introduction," accessed July 1, 2025. [Online]. Available: https://postquantum.com/post-quantum/post-quantum-cryptography-pqc/

[68] Tripwire, "Preparing for the quantum future: Insights from the ncsc's pqc migration roadmap," accessed July 1, 2025. [Online]. Available: https://www.tripwire.com/state-of-security/preparing-quantum-future-insights-ncscs-pqc-migration-roadmap

[69] Cloudflare, "What is ipsec?" n.d., accessed: 2025-07-02. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[70] IETF, "Rfc 4305 - cryptographic algorithm implementation requirements for esp and ah," 2005, accessed: 2025-07-02. [Online]. Available: https://datatracker.ietf.org/doc/rfc4305/

[71] Cisco Community, "Crypto map based ipsec vpn fundamentals, negotiation and configuration," 2017, accessed: 2025-07-02. [Online]. Available: https://community.cisco.com/t5/security-knowledge-base/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502

[72] J. Hu, Y. Morioka, and G. Wang, "Post-quantum traditional (pq/t) hybrid pki authentication in the internet key exchange version 2 (ikev2)," Internet Engineering Task Force, Internet-Draft draft-hu-ipsecme-pqt-hybrid-auth-02, May 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth/

[73] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov, "Mixing preshared keys in the internet key exchange protocol version 2 (ikev2) for post-quantum security," https://datatracker.ietf.org/doc/html/rfc8784, 2020, rFC 8784.

[74] D. Herzinger, S.-L. Gazdag, and D. Loebenberger, "Real-world quantum-resistant ipsec," in *2021 14th International Conference on Security of Information and Networks (SIN)*, vol. 1, 2021, pp. 1–8.

[75] I. E. T. Force, "Intermediate exchange in the ikev2 protocol," https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-intermediate-05, Sep. 2020, internet-Draft draft-ietf-ipsecme-ikev2-intermediate-05, Work in Progress.

[76] C. Tjhai, T. Heider, and V. Smyslov, "Beyond 64kb limit of ikev2 payload," https://datatracker.ietf.org/doc/html/draft-tjhai-ikev2-beyond-64k-limit-00, Oct. 2020, internet-Draft draft-tjhai-ikev2-beyond-64k-limit-00, Work in Progress.

[77] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. van Geest, O. Garcia-Morchon, and V. Smyslov, "Multiple key exchanges in ikev2," https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-multiple-ke-02, Jan. 2021, internet-Draft draft-ietf-ipsecme-ikev2-multiple-ke-02, Work in Progress.

[78] S.-L. Gazdag, S. Grundner-Culemann, T. Guggemos, T. Heider, and D. Loebenberger, "A formal analysis of ikev2's post-quantum extension," ser. ACSAC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 91–105. [Online]. Available: https://doi.org/10.1145/3485832.3485885

[79] S. Bae, Y. Chang, H. Park, M. Kim, and Y. Shin, "A performance evaluation of ipsec with post-quantum cryptography," in *Information Security and Cryptology – ICISC 2022*, S.-H. Seo and H. Seo, Eds. Cham: Springer Nature Switzerland, 2023, pp. 249–266. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-29371-9_13

[80] S.-L. Gazdag, S. Grundner-Culemann, T. Heider, D. Herzinger, F. Schärtl, J. Y. Cho, T. Guggemos, and D. Loebenberger, "Quantum-resistant macsec and ipsec for virtual private networks," in *Security Standardisation Research*, F. Günther and J. Hesse, Eds. Cham: Springer Nature Switzerland, 2023, pp. 1–21.

[81] A. Mutlugun, Y. Hanna, and K. Akkaya, "Performance evaluation of quantum-resistant ikev2 protocol for satellite networking environments," in *2024 IEEE Virtual Conference on Communications (VCC)*, 2024, pp. 1–7.

[82] D. Shanmugapriya, A. Patel, G. Srivastava, and J. C.-W. Lin, "Mqtt protocol use cases in the internet of things," in *Big Data Analytics*, S. N. Srirama, J. C.-W. Lin, R. Bhatnagar, S. Agarwal, and P. K. Reddy, Eds. Cham: Springer International Publishing, 2021, pp. 146–162. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-93620-4_12

[83] Amazon Web Services, "What is mqtt?" n.d., accessed: 2025-07-02. [Online]. Available: https://aws.amazon.com/what-is/mqtt/

[84] H. J. Hadi, Y. Cao, M. A. Alshara, N. Ahmad, M. S. Riaz, and J. Li, "Quantum computing challenges and impact on cyber security," in *Digital Forensics and Cyber Crime*, S. Goel and P. R. Nunes de Souza, Eds. Cham: Springer Nature Switzerland, 2024, pp. 333–343.

[85] L. Malina, P. Dobias, P. Dzurenda, and G. Srivastava, "Quantum-resistant and secure mqtt communication," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, ser. ARES '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3664476.3670463

[86] Y. Kim and S. C. Seo, "An optimized instantiation of post-quantum MQTT protocol on 8-bit AVR sensor nodes," Cryptology ePrint Archive, Paper 2025/563, 2025. [Online]. Available: https://eprint.iacr.org/2025/563

[87] F. J. A. Rampazzo and M. A. A. Henriques, "Assessment of the impact of hybrid post-quantum cryptography on the performance of the mqtt communication protocol," in *2023 Symposium on Internet of Things (SIoT)*. IEEE, 2023, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/10390050

[88] J. Samandari and C. Gritti, "Post-quantum authentication in the mqtt protocol," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 416–434, 2023. [Online]. Available: https://www.mdpi.com/2624-800X/3/3/21

[89] I. Cherkaoui, O. Ali, and J. Horgan, "Novel hybrid post-quantum encryption design on embedded devices," in *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2024, pp. 1–8. [Online]. Available: https://doi.org/10.1109/ETFA61755.2024.10710884