TLS 1.3 with ML-KEM Key Exchange over an Emulated IPv4/IPv6 Internet: Operational Evaluation of Post-Quantum Cryptography

Deepinder Sidhu[123], Matt Eckenrode[12], Sashi Lazar[12]

[1] **TeleniX Corporation**

[2] **Cyberspace Analytics Corporation**

[3] **University of Maryland, Baltimore County**

Abstract

This paper presents an operational evaluation of TLS 1.3 with hybrid ML-KEM (X25519MLKEM768) key exchange executed over a high-fidelity emulated dual-stack IPv4/IPv6 Internet. Using unmodified production TLS implementations, we exercise client and server systems across multiple deployment configurations, routing path variations, induced routing failures, 1000 consecutive handshake negotiations, and remote cross-endpoint interoperability scenarios. Full packet capture confirms correct encapsulation, negotiation stability, and recovery behavior under dynamic routing conditions.

The evaluation leverages an Internet emulation environment that has supported development and operational validation of major Internet protocols—including OSPF, ISAKMP/IKE, IPsec, IPv6, and Mobile IP—and that provides controlled realism through reproducible Internet-scale routed topologies impractical to construct in conventional laboratory settings. The same architecture provides a controlled and observable environment well suited for structured interoperability validation of independently developed TLS and post-quantum implementations.

The results indicate that hybrid ML-KEM integration operates reliably under realistic Internet routing dynamics and support the need for operational evaluation of post-quantum cryptographic deployments beyond isolated algorithmic analysis.

---

1. Introduction

Public-key cryptography underpins secure communication across the Internet, enabling authentication, confidentiality, and integrity for applications ranging from web services to critical infrastructure. The security of widely deployed systems—RSA, Diffie–Hellman, and elliptic-curve

cryptography—relies on computational hardness assumptions that do not hold against sufficiently capable quantum adversaries.

Shor demonstrated that quantum computers can efficiently solve integer factorization and discrete logarithm problems [1], rendering these classical schemes vulnerable. Consequently, encrypted data captured today may be retained and decrypted retroactively once large-scale quantum systems become available—a threat commonly described as “harvest now, decrypt later.”

In response, the cryptographic community has developed post-quantum algorithms designed to resist both classical and quantum attacks. After a multi-year evaluation process, the National Institute of Standards and Technology (NIST) standardized ML-KEM as FIPS 203 for post-quantum key establishment [2]. ML-KEM is now being integrated into Transport Layer Security (TLS) 1.3 [3], the dominant protocol securing Internet communications.

However, standardization does not equate to deployability. Internet history shows that protocol correctness at the cryptographic or specification level does not guarantee operational robustness under real-world routing dynamics, retransmissions, failures, or heterogeneous implementations. Major protocol transitions—IPsec, IPv6, and TLS itself—required extensive operational validation beyond formal cryptographic assurance.

The post-quantum transition represents a similar Internet-scale evolution. While ML-KEM has been cryptographically analyzed, far less attention has been given to its behavior when embedded within TLS 1.3 and exercised across realistic IPv4/IPv6 Internet conditions.

This paper evaluates TLS 1.3 with hybrid ML-KEM key exchange as an operational Internet system. Using a large-scale dual-stack emulated Internet environment, we examine handshake correctness, routing resilience, repeated session stability, and remote interoperability under controlled but realistic network dynamics.

---

2. TLS 1.3 with ML-KEM Key Exchange Evaluation

2.1 Implementation Details

ML-KEM, standardized by NIST as FIPS 203, is a post-quantum key encapsulation mechanism designed for integration within higher-level security protocols. In Internet deployments, key establishment is performed by Transport Layer Security (TLS), which combines key exchange, authentication, and session key derivation into a unified security architecture. Accordingly, ML-KEM is evaluated here as integrated within TLS 1.3 rather than as a standalone primitive.

The experiments use TLS 1.3 with hybrid X25519MLKEM768 key exchange. In this construction, a classical X25519 elliptic-curve Diffie–Hellman exchange is combined with ML-KEM-768, and both shared secrets are cryptographically bound within the TLS handshake. This hybrid design reflects current transition practice, providing security provided that at least one constituent mechanism remains sound.

All evaluations were conducted using unmodified, production-grade TLS 1.3 implementations incorporating ML-KEM through widely deployed cryptographic libraries. No protocol instrumentation, stack modification, or kernel alteration was introduced. Authentication employs standard TLS 1.3 signature algorithms; post-quantum authentication is outside the scope of this work.

All protocol behavior was observed externally via packet capture and routing instrumentation.

2.2 Evaluation Objectives

This study evaluates TLS 1.3 with hybrid ML-KEM key exchange as an operational Internet protocol. The focus is limited to handshake-level behavior, including:

- Correct session establishment
- Proper encapsulation and termination
- Robustness under routing dynamics

Because ML-KEM participates exclusively in TLS key establishment, the evaluation centers on handshake correctness under realistic Internet conditions. Specifically, we examine whether TLS negotiations:

- Complete successfully across routed IPv4 and IPv6 paths
- Terminate correctly under normal conditions
- Recover appropriately when routing changes, packet loss, or reconvergence events occur during active negotiation

The study does not measure cryptographic strength, application throughput, long-lived session behavior, or workload-specific performance. Those analyses require defined application models and are deferred to future work.

Successful handshake establishment under realistic routing conditions is treated as a necessary operational prerequisite for post-quantum deployment.

2.3 Evaluation Platform

The evaluation was conducted using Q-ENV™, a portable Internet emulation platform designed for operational validation of Internet protocols under realistic routing conditions.

Q-ENV supports live–virtual integration, enabling physical or virtual routers and endpoint systems to attach directly to the emulated routing fabric in a plug-and-play manner. Real routers may be connected to virtual routers within the emulated topology without modification to operating system kernels, networking stacks, cryptographic libraries, or applications. Configuration requirements are limited to standard interface provisioning (e.g., IPv4 and IPv6 address assignment).

Within the emulated Internet, routing nodes execute full IPv4 and IPv6 protocol stacks, including standard forwarding behavior and dynamic routing protocols such as OSPF and BGP. Routing state changes arise from protocol execution rather than scripted simulation. Links and router configurations may be provisioned to reflect real network deployments, enabling construction of Internet topologies of varying size, path diversity, and failure characteristics.

The platform supports creation of multi-path routed environments with configurable hop counts and failure domains. Routing dynamics—including path modification, link failure, and reconvergence—occur as a consequence of routing protocol behavior. Resulting packet loss, delay, and reordering reflect realistic operational effects.

Full packet capture may be performed at any attachment point within the emulated topology, providing end-to-end observability across routing domains. TLS 1.3 traffic incorporating ML-KEM traverses the routed environment exactly as it would in a live Internet context, without hidden instrumentation or stack modification.

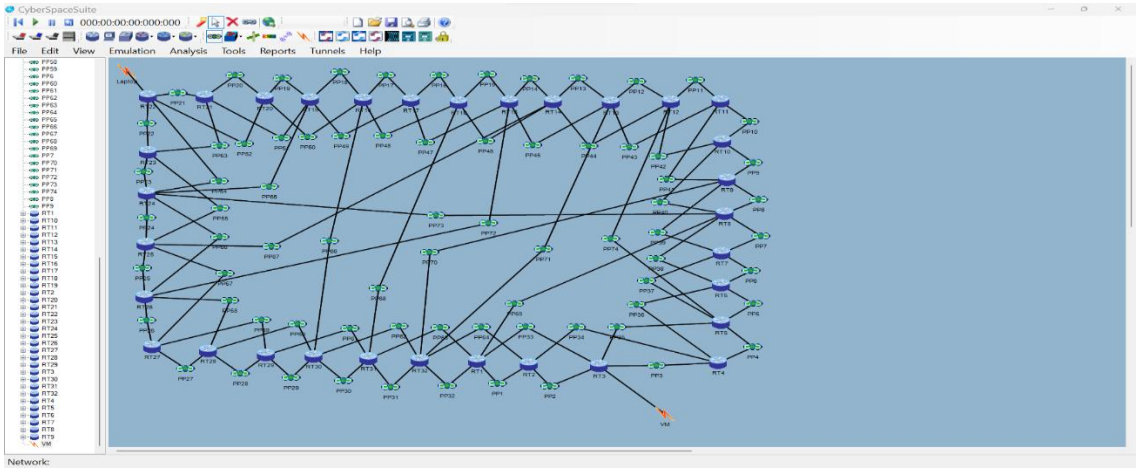
This architecture enables evaluation of protocol correctness, encapsulation integrity, termination behavior, and robustness under dynamic routing conditions while preserving deployment realism.

Effective operational evaluation of TLS 1.3 with hybrid ML-KEM key exchange cannot be achieved using isolated host-to-host testbeds or uncontrolled public Internet experiments. Simple laboratory environments lack realistic routing dynamics, while testing directly on the public Internet does not provide controlled topology design, repeatable failure scenarios, or comprehensive observability. The Internet emulation platform provides bit-level fidelity of Internet communications while enabling controlled construction of routed topologies of varying size and complexity—topologies that would be cost-prohibitive or operationally impractical to replicate physically in a laboratory setting. This controlled realism enables systematic testing and validation of new protocol integrations under conditions that approximate operational Internet behavior without sacrificing reproducibility or measurement integrity.

2.4 Emulated Internet Topology

The emulated Internet comprised more than 30 routing nodes forming multiple paths of varying hop lengths between endpoints.

Figure 1: Emulated dual-stack IPv4/IPv6 Internet topology used for evaluation. Live–virtual interfaces connect real endpoint systems to a routed environment composed of fully functional networking nodes. No kernel or protocol modifications are required.



3. Evaluation Methodology and Observation

This section describes the methodology used to observe TLS 1.3 with hybrid ML-KEM key exchange as it executes over the emulated Internet topology described in Section 2.4. Analysis is based exclusively on externally observable packet-level evidence, focusing on handshake correctness, encapsulation integrity, termination behavior, and robustness under routing dynamics.

3.1 Packet Capture and Protocol Observability

All experiments employed full packet capture at the interfaces connecting real endpoint systems to the emulated Internet. Packet capture was performed externally using standard tools, without kernel hooks, application logging, or protocol instrumentation.

Each pcap preserves complete encapsulation down to the link layer, including Ethernet framing, IPv4 or IPv6 headers, TCP sequence and acknowledgment behavior, TLS 1.3 message exchanges, byte counts, and timing information.

Figure 2 presents a representative server-side IPv4 packet capture. The trace shows correct TCP three-way handshake progression followed by TLS 1.3 negotiation incorporating hybrid X25519MLKEM768 key exchange and transition to encrypted
application data.

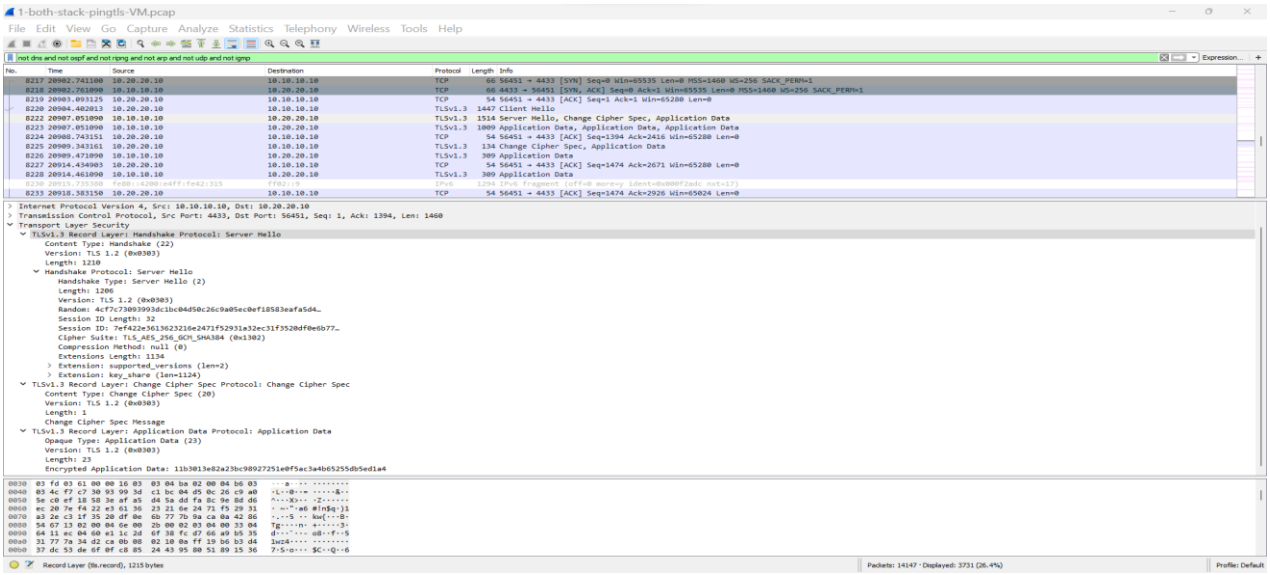
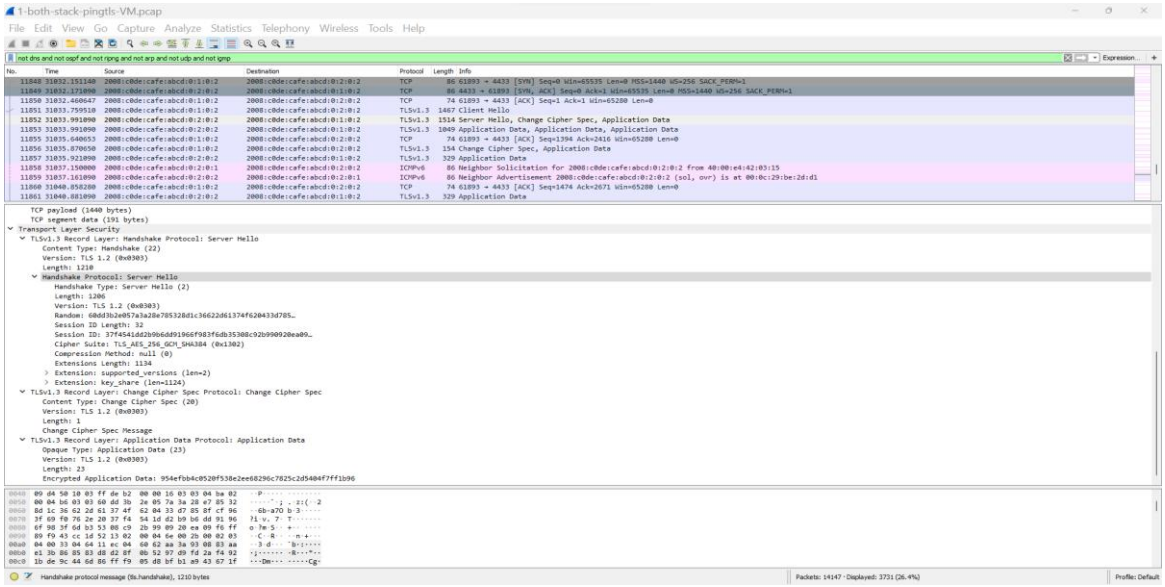


Figure 3 presents the corresponding IPv6 server-side capture. The TLS handshake behavior is equivalent, demonstrating consistent protocol semantics across dual-stack routing environments. Observed differences between IPv4 and IPv6 traces arise from routing conditions rather than implementation.



3.2 Routing Dynamics and Failure Injection

Routing changes, including path modification and reconvergence events, were introduced within the emulated topology during both idle periods and active TLS handshakes.

During routing transitions, packet captures record transient packet loss, delay, and reordering consistent with realistic routing behavior. Affected TLS handshake messages are retransmitted at the transport layer as required. When routing stabilizes within expected bounds, handshakes complete successfully.

No cryptographic state corruption or abnormal termination was observed during routing events.

3.3 Metrics and Observational Scope

Analysis is restricted to handshake-level behavior. Observed metrics include:

- Handshake completion
- Message sequencing correctness
- Retransmission behavior
- TCP and TLS byte counts during negotiation
- Timing variations associated with routing changes

The application throughput, sustained encrypted traffic performance, and workload-specific behavior are outside the scope of this study.

3.4 Repeated Handshake Stability Testing

To evaluate sustained negotiation robustness, 1000 consecutive TLS 1.3 sessions were initiated and terminated across the emulated Internet.

Each session included:

- TCP connection establishment
- Hybrid X25519MLKEM768 handshake
- Encrypted application data exchange
- Connection closure

Across 1000 iterations:

- All sessions completed successfully
- No progressive timing degradation was observed
- No resource exhaustion occurred
- No handshake state inconsistencies were detected

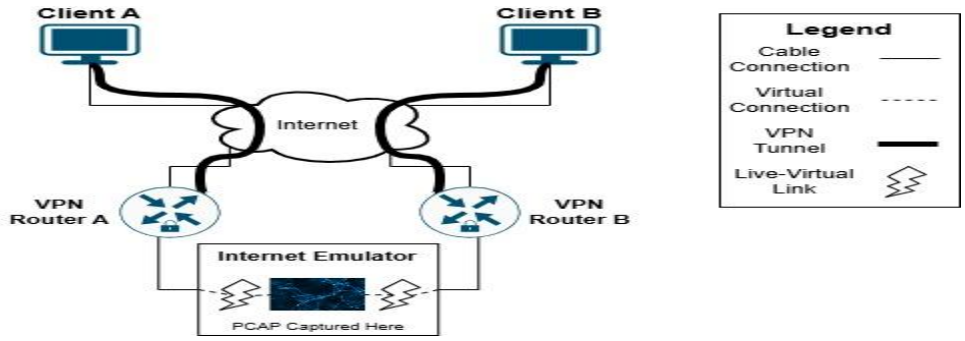
Packet-level analysis confirmed correct encapsulation and termination for each session, demonstrating stability under sustained session churn.

3.5 Remote Interoperability Testing Architecture

Figure 4 illustrates the remote interoperability testing architecture supported by the Internet Emulator. In this model, independent vendor products (clients, servers, or security gateways) connect from remote locations through VPN routers into the emulated Internet using live–virtual links. The emulator provides a controlled routed IPv4/IPv6 environment with configurable path length, routing dynamics, and failure conditions, while preserving end-to-end protocol fidelity.

This architecture enables vendor-to-vendor interoperability validation of TLS 1.3 with hybrid ML-KEM key exchange under realistic Internet behavior. Because the endpoints remain operational vendor systems, interoperability testing can be performed without modifying endpoint kernels, TLS stacks, or cryptographic libraries. Packet capture is performed within the emulated Internet, enabling consistent, tool-based evidence collection (pcap) independent of vendor instrumentation.

In the experiments reported in this paper, we validated the remote attachment model by exercising TLS 1.3 with hybrid X25519MLKEM768 key exchange across network-separated endpoints connected through the Figure 4 architecture. Successful session establishment and packet-level observability confirm that the emulator can support remote endpoint participation and evidence-grade capture in a controlled Internet environment. Multi-vendor interoperability campaigns using heterogeneous TLS stacks and cryptographic providers are enabled by the same architecture and are a primary target for continued evaluation.



4. Summary and Future Work

This study evaluated TLS 1.3 with hybrid X25519MLKEM768 key exchange as an operational Internet protocol executed over a routed dual-stack IPv4/IPv6 environment. Using unmodified production implementations and external packet capture, we verified handshake correctness, encapsulation integrity, termination behavior, routing resilience, repeated session stability across 1000 consecutive negotiations, and remote interoperability across separated endpoints.

All observed behavior aligned with established TCP and TLS semantics, including during routing transitions and failure events. No handshake corruption, progressive instability, or interoperability anomalies were detected.

These results demonstrate that hybrid ML-KEM integration operates reliably when exposed to realistic Internet routing dynamics. The findings reinforce that post-quantum cryptography must be validated as an operational system—where deployability and robustness emerge from protocol interaction under live routing conditions — not solely as an algorithmic construct.

This work establishes a baseline operational validation layer for post-quantum Internet security. Future efforts will expand in three directions:

1. Additional FIPS-Standardized Mechanisms

   Extend evaluation to other NIST-standardized post-quantum algorithms integrated within TLS 1.3 to enable comparative operational assessment.

2. Cross-Implementation Interoperability

   Conduct validation across independently developed TLS stacks and cryptographic libraries to detect interoperability issues that may only surface under heterogeneous deployment conditions.

3. Application-Layer and Performance Studies

   Incorporate real client and server workloads to evaluate session latency, throughput, and long-lived connection stability once handshake-level behavior is established.

The evaluation environment provides controlled realism, exposing protocol behavior to dynamic routing conditions within reproducible Internet-scale topologies that are impractical to construct using conventional laboratory infrastructure.

The framework supports systematic scaling of topology size, path diversity, and controlled failure conditions, enabling rigorous operational validation of post-quantum protocol behavior under progressively demanding Internet deployment scenarios. Such validation represents a necessary technical foundation for confident and orderly post-quantum transition planning. The same infrastructure provides an ideal controlled environment for vendor-to-vendor interoperability testing during the post-quantum transition, where heterogeneous implementations must be validated under realistic routing conditions.

References

[1] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *FOCS*, 1994.
[2] NIST, “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM),” 2024.
[3] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, IETF, 2018.
[4] NIST, “Post-Quantum Cryptography Standardization,” https://csrc.nist.gov/projects/post-quantum-cryptography