Redefining Secure Connectivity in the Post-Quantum Era

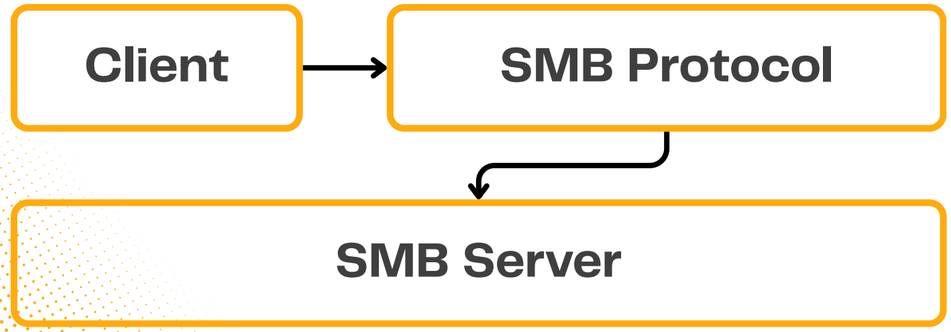
fall 2025

SMB PQ LINK

Unlock Ultra-Secure, High-Performance SMB Communication

by TAREK KAADAN
AHMAD ABDELLATIF
GEORGE GHANEM

What is SMB ?

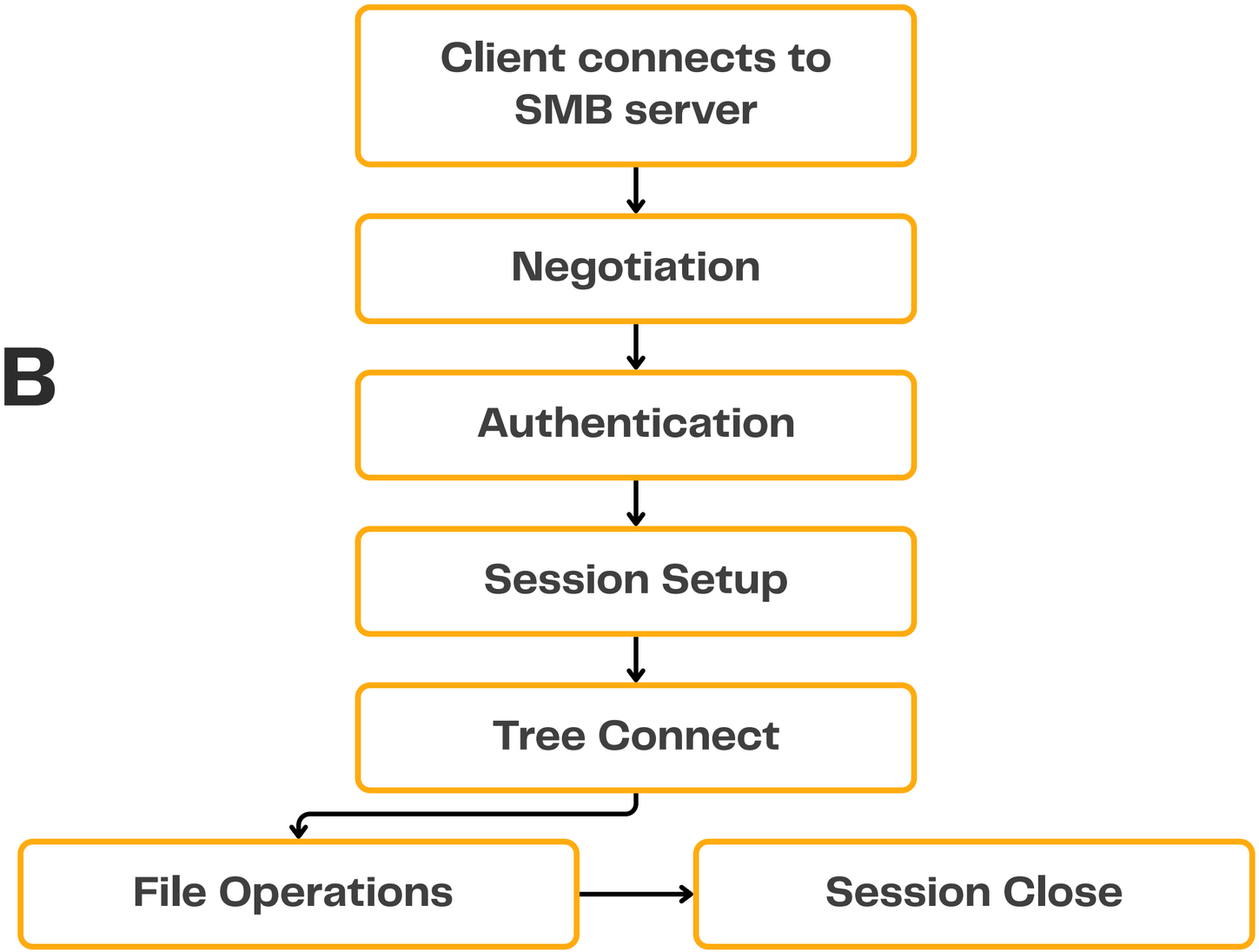


SMB is a network file sharing protocol used primarily by Windows systems. It Allows clients to access files, folders, printers, and services on a remote server. Works over TCP (port 445) in modern versions.

Provides features like:

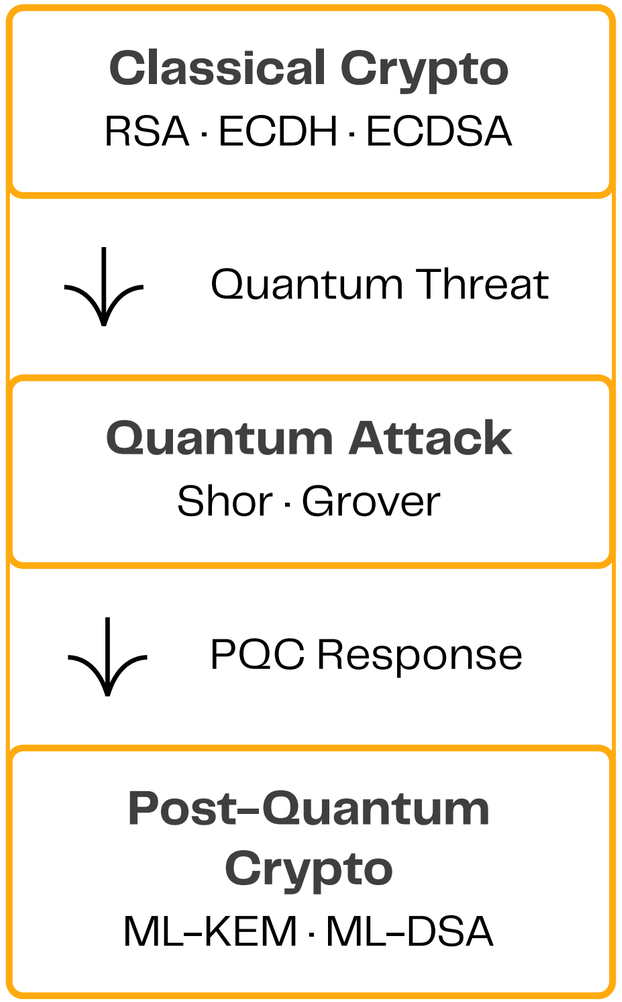
- File read/write
- Directory listing
- File locking
- Printer sharing
- Authentication & session management

How SMB Works ?



Problem Motivation

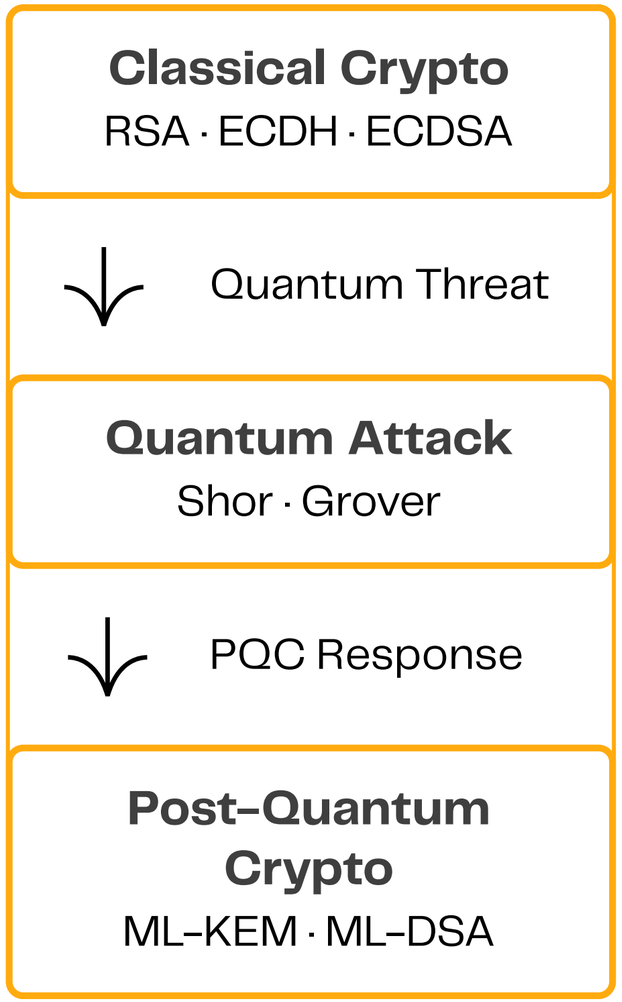
Why Migrate to Post-Quantum Cryptography ?



- Quantum computers break RSA/ECC
- SMB file-sharing depends on classical encryption
- Organizations need future-proof secure tunnels

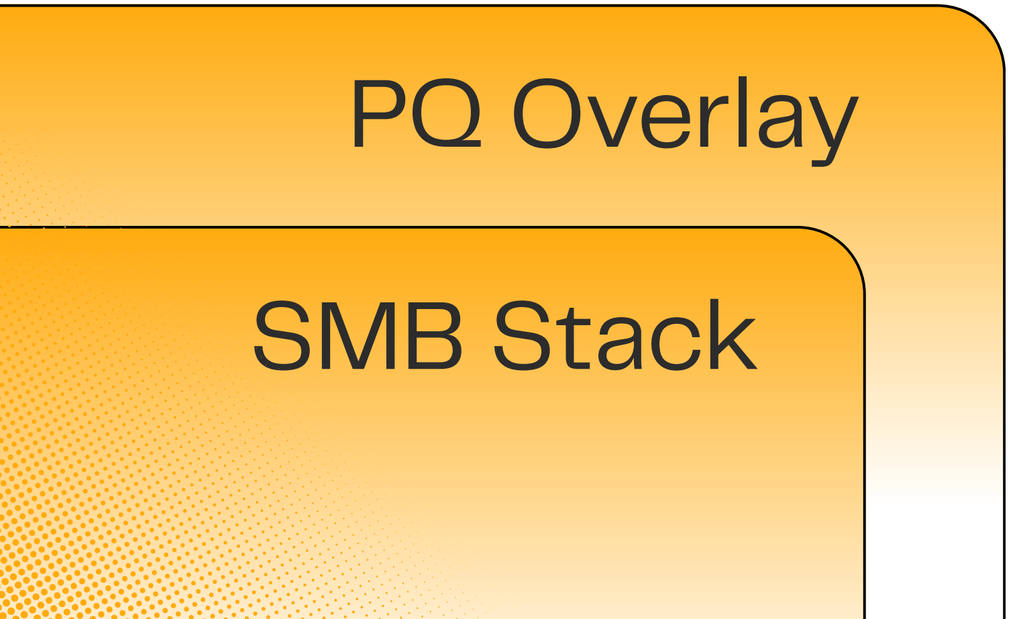
Project Overview

Goal of SMB Post-Quantum Link?



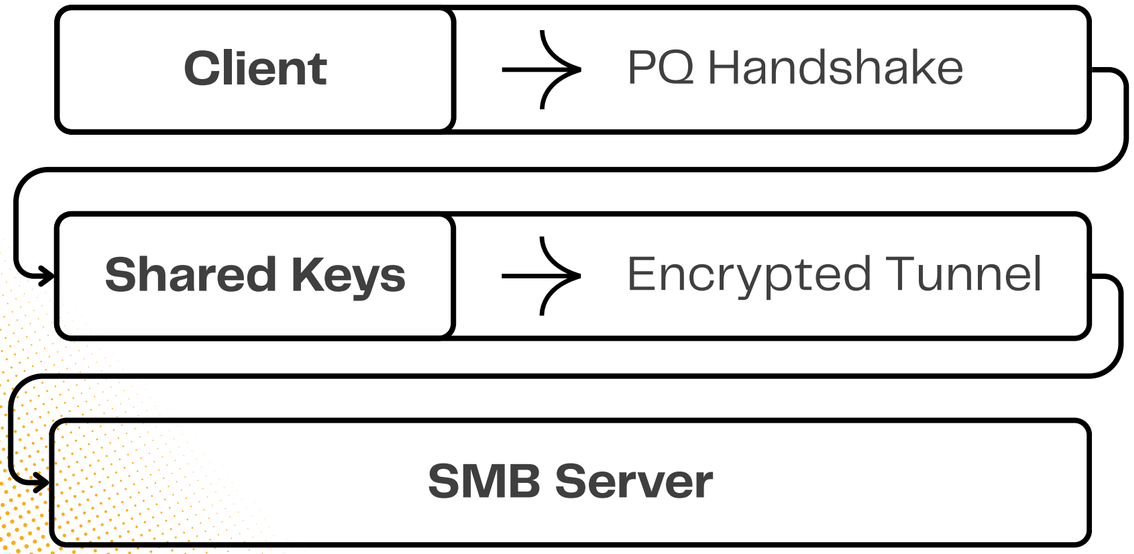
- Build a post-quantum–hardened secure tunnel for SMB traffic
- Use ML-KEM (Kyber) for key encapsulation
- Use ML-DSA (Dilithium) for authentication
- Design a hybrid classical + PQ scheme for compatibility

Why SMB? Protocol Analysis



- SMB used for file sharing, authentication, transport
- Typically relies on classical primitives (ECDH, AES, HMAC)
- SMB lacks built-in post-quantum support
- We migrate the transport path, not SMB internals

SMB PQ LINK Architecture



- PQ handshake establishes session keys
- ChaCha20-Poly1305 used for data encryption
- Tunnel forwards SMB packets after encryption

Post-Quantum Integration

ML-KEM + ML-DSA (Dilithium) in SMB PQ

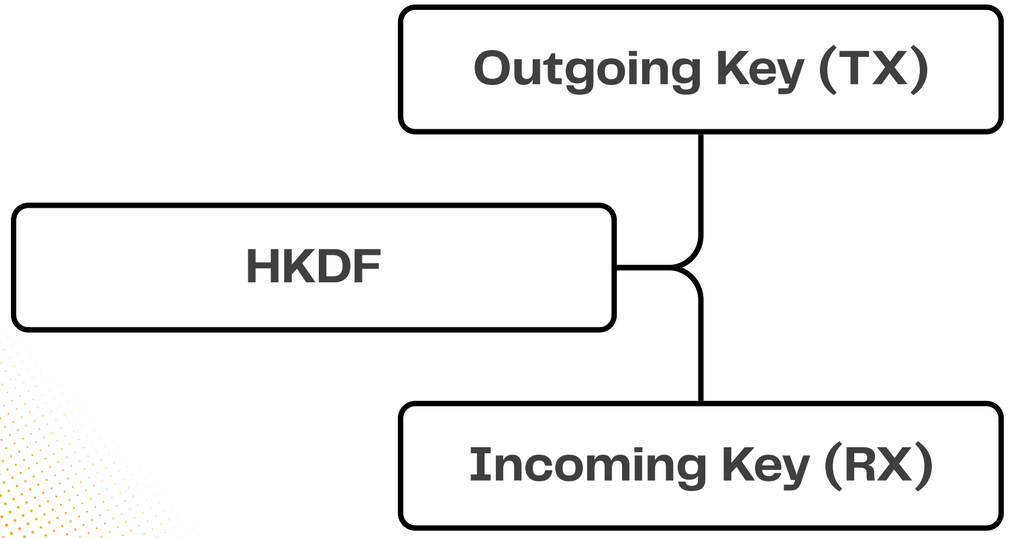
ML-KEM
used to generate high-entropy shared secrets

Kyber

ML-DSA
used to sign the handshake

Dilithium

Hybrid Mode (Classical + Post-Quantum)



We combine:

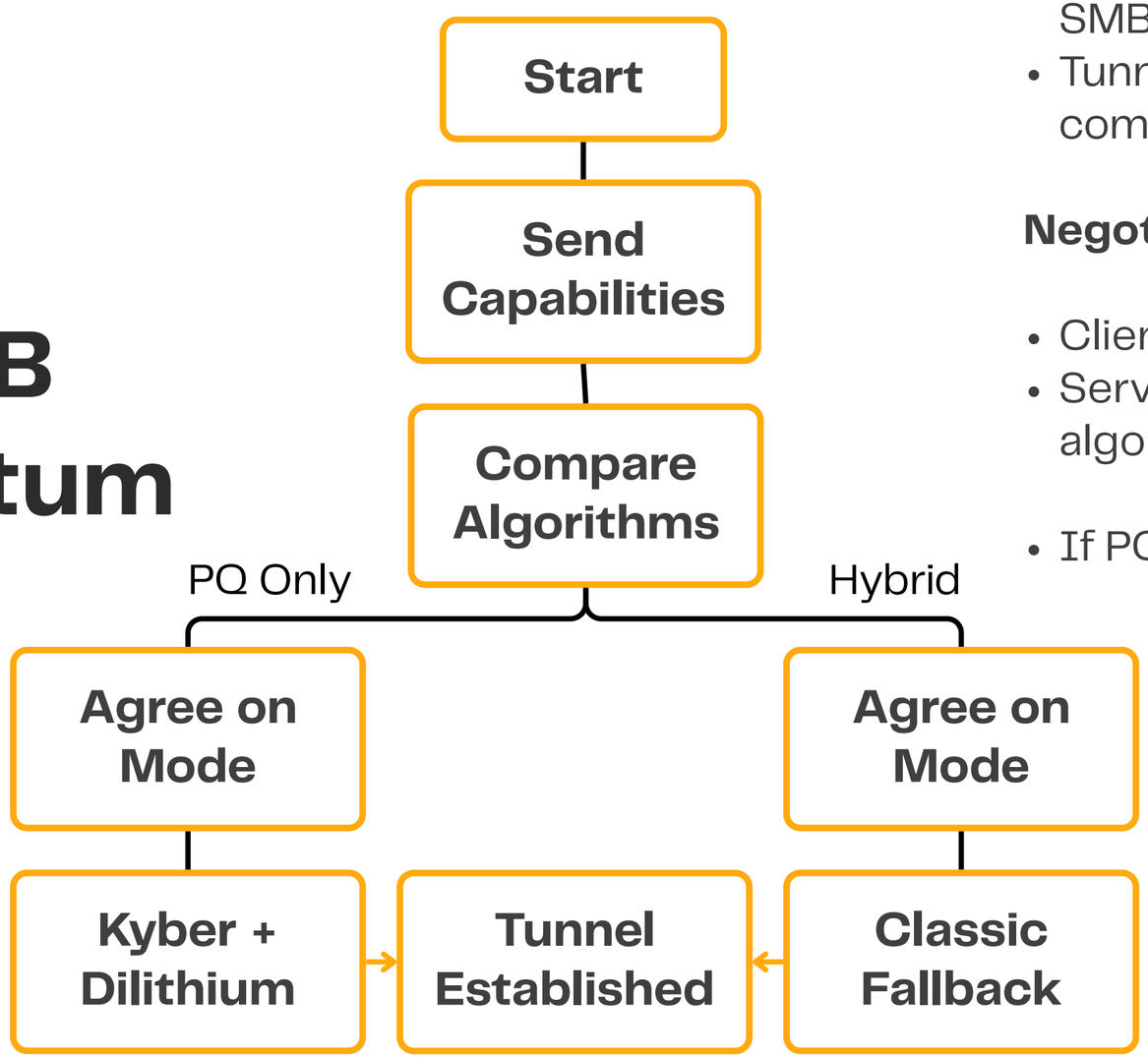
- Classical ECDH-derived secret (optional fallback)
- PQ ML-KEM secret

Use HKDF to derive:

- Outgoing key
- Incoming key
- Ensures security even if one primitive fails

Project Overview

Goal of SMB Post-Quantum Link?



- PQ upgrade does not modify SMB
- Tunnel is fully backward-compatible

Negotiation mechanism:

- Client proposes PQ or hybrid
- Server accepts best available algorithm

- If PQ fails → classical fallback

Performance Measurements

Scenario	Time 10MB (s)	Thru 10 MB/s	Time 100MB/s (s)	Thru 100MB/s
Direct SMB	2.56 secs	3.9	3.10 secs	32.3
PQ-only link	3.21 secs	3.1	3.06 secs	32.6
Hybrid link	2.62 secs	3.8	2.95 secs	33.9

Security Guarantees of the Quantum-Safe SMB Link

PQ Confidentiality

- Kyber-768 replaces classical DH
- Resistant to harvest-now, decrypt-later attacks

Hybrid Security

- Kyber secret + X25519 secret → HKDF
- Secure if either lattice hardness or elliptic-curve hardness survives
- Prevents downgrade attacks because suite is signed inside transcript

Security Guarantees of the Quantum-Safe SMB Link

Authentication & Integrity

- Server → signs transcript using Dilithium2
- Client → signs transcript during ClientAuth
- ChaCha20-Poly1305 protects all SMB frames

Forward Secrecy

- Both Kyber and X25519 keys are ephemeral
- Long-term key compromise does not reveal past tunnels

Security Guarantees of the Quantum-Safe SMB Link

Limitations

- SMB server config unchanged
- Does not prevent DoS or traffic analysis
- SMB authentication remains classical (outside scope)

Conclusion

PQ Migration Without Touching SMB

- PQ link sits transparently between client & server
- SMB remains untouched but now quantum-safe

Using NIST Standards

- ML-KEM (Kyber-768)
- ML-DSA (Dilithium2)

Hybrid Mode Offers Best Practical Performance

- Slight handshake cost
- No significant impact on large transfers

Strong Security with Minimal Overhead

- PQ confidentiality + Dilithium authentication
- Forward secrecy maintained
- Drop-in upgrade path

Thank You !