Building a Quantum-Safe Communication Infrastructure

Giuseppe Bruno
Bank of Italy, Economics and Statistics Directorate

CONTEXT & CHALLENGE

The Need for Encryption

Unencrypted messages over public networks can be intercepted and altered by any third party. **Symmetric encryption** transforms plaintext into ciphertext and can be made arbitrarily secure — but requires both endpoints to share the **same secret key** over an untrusted channel. This is the fundamental key distribution problem.

Core challenge: how do two parties securely agree on the same key without ever meeting?

- Symmetric encryption: same key must exist at both ends
- Classical key exchange (Diffie-Hellman, RSA) will be broken by quantum computers
- Encrypted traffic captured today will be decrypted when quantum computers mature
- Migration to quantum-safe solutions must begin now

Key Distribution in a Quantum World

Quantum Key Distribution (QKD)

C. Bennett & G. Brassard — via Physics

Exploits quantum mechanics: any eavesdropping disturbs photon states and is immediately detectable. The security is guaranteed by the laws of nature, not computational hardness.

Symmetric Key Establishment (DSKE)

Claude Shannon — via Logistics & Entropy

Keys are distributed via multiple independent Security Hubs using secret-sharing protocols. No single hub holds the complete key. Quantum-immune because it relies solely on pre-distributed symmetric secrets.

Post-Quantum Cryptography (PQC)

Oded Regev — via Mathematics (Lattices)

Security rests on the hardness of lattice problems (Ring-LWE) believed intractable even for quantum computers. NIST standardised ML-KEM, ML-DSA, and SLH-DSA in 2024. Software-only upgrade path.

Market Readiness — Global Case Study

Case Study: a global quantum-safe network

A real-world deployment integrating QKD, DSKE, and PQC technologies simultaneously into a single network fabric, operated across multiple geographic sites with equipment from competing vendors.

- QKD, DSKE, and PQC integrated in existing infrastructure without forklift upgrades
- Vendors: Cisco, Fortinet, Juniper (encryptors); multiple KME providers
- All encryptor combinations successfully established quantum-safe tunnels
- The technology is commercially ready and deployable today

A multi-vendor, multi-technology quantum-safe network is fully operational and tested.

TECHNOLOGY LANDSCAPE

Post-Quantum Cryptography: R-LWE

Ring Learning With Errors (R-LWE) is the mathematical foundation of NIST-standardised ML-KEM (Kyber). Security rests on the hardness of solving noisy linear equations over polynomial rings — a problem believed hard even for quantum computers.

Key Generation

```
Key gen: a, s are random polynomials; p = a·s + e   (e = small noise vector)
Public key is (a, p); private key is s
```

Encryption

$C_1 = a \cdot e_1 + e_2$ (blinded basis)
$C_2 = p \cdot e_1 + e_3 + m \cdot [q/2]$ (message encoded)

Decryption

Compute: $C_2 - C_1 \cdot s = m \cdot [q/2] + \text{small\_noise}$
Round to recover m (noise cancels out)

Distributed Symmetric Key Exchange

DSKE removes single points of trust. Alice and Bob each obtain a key share from multiple independent Security Hubs and combine them using a secret-sharing protocol. No single Hub ever possesses the complete key.

Security Hub 1 | **Security Hub 2** | **Security Hub 3**

↓ Key Share A_1 ↓ Key Share A_2 ↓ Key Share A_3

$$\text{Final Key} = A_1 \oplus A_2 \oplus A_3$$

- No single Hub can reconstruct the final key alone
- Quantum-immune: relies only on pre-distributed symmetric secrets
- Vendor-neutral: different Hub suppliers can coexist in the same network
- Naturally supports zero-trust network architectures

IKEv2 PPK Extension — RFC 8784

RFC 8784 defines the Post-Quantum Preshared Key (PPK) mechanism for IKEv2. A quantum-safe key (sourced from QKD, DSKE, or PQC) is injected into the standard IKEv2 handshake as an additional secret, protecting the session even if classical Diffie-Hellman is broken by a quantum adversary.

1. **IKE_SA_INIT → exchange algorithms & DH**
2. **IKE_AUTH → inject PPK (quantum-safe key)**
3. **CREATE_CHILD_SA → establish IPsec tunnel**

- Fully backward-compatible with classical IKEv2 / IPsec deployments
- Any quantum-safe key source (QKD, DSKE, PQC) can supply the PPK
- No changes required to existing network tunnel endpoints
- Common interface enabling multi-vendor interoperability in all tests

The single standardised interface enabling all encryptor + KME interoperability in this work.

EXPERIMENTAL RESULTS

Encryptor Interoperability Tests

All tests use the IKEv2 RFC 8784 PPK extension. Each pair of encryptors from different vendors was tested for successful quantum-safe tunnel establishment and authenticated data transfer.

Encryptor A	Encryptor B	PPK Source	Result
Cisco	Cisco	DSKE	✓ Pass
Cisco	Fortinet	DSKE	✓ Pass
Cisco	Juniper	DSKE	✓ Pass
Fortinet	Fortinet	DSKE	✓ Pass
Fortinet	Juniper	DSKE	✓ Pass
Juniper	Juniper	DSKE	✓ Pass
Cisco	Cisco	QKD	✓ Pass
Cisco	Fortinet	QKD	✓ Pass
Cisco	Fortinet	PQC	✓ Pass

All tested encryptor pairs (same-vendor and cross-vendor) achieved quantum-safe communication.

Key Management Entity (KME) Tests

Tests verified that encryptors from Cisco, Fortinet, and Juniper could successfully retrieve quantum-safe PPKs from heterogeneous KME providers. This demonstrates a truly open, multi-vendor quantum-safe ecosystem with no lock-in.

Encryptor	KME Provider	Key Type	Result
Cisco	Vendor KME-A	DSKE	✓ Pass
Fortinet	Vendor KME-A	DSKE	✓ Pass
Juniper	Vendor KME-A	DSKE	✓ Pass
Cisco	Vendor KME-B	QKD	✓ Pass
Fortinet	Vendor KME-B	QKD	✓ Pass
Juniper	Vendor KME-B	QKD	✓ Pass
Cisco	Vendor KME-C	PQC	✓ Pass
Fortinet	Vendor KME-C	PQC	✓ Pass

Any encryptor brand can retrieve keys from any KME brand — no proprietary dependencies.

Key Findings & Conclusions

- QKD, DSKE, and PQC can all serve as RFC 8784 PPK sources interchangeably
- Cisco, Fortinet, and Juniper encryptors interoperate fully via RFC 8784
- Multiple KME vendors coexist seamlessly — no vendor lock-in required
- Crypto-agility allows algorithm swap without re-architecting the network
- NIST PQC standards (ML-KEM, ML-DSA) are final — migration planning should begin now
- The combined quantum-safe ecosystem is commercially available and ready today

Quantum-safe communication with full multi-vendor interoperability is achievable and commercially ready today.