BRIEFING 04 · QUANTUM

Quantum cybersecurity: the migration that can’t wait

A deep dive into the quantum threat to encryption: how Shor's algorithm breaks RSA, the NIST post-quantum standards, how fast the threat estimates are moving, where QKD fits, and a practical migration playbook.

Mohsin Khan Shaik
AI Infrastructure & Site Reliability Engineer · San Francisco · mohsinkhanshaik.com
Edition of 2026-11-22

04 · QUANTUM

Quantum cybersecurity: the migration that can’t wait

A deep dive into the quantum threat to encryption: how Shor's algorithm breaks RSA, the NIST post-quantum standards, how fast the threat estimates are moving, where QKD fits, and a practical migration playbook.

Aug 2024	60%+	<1M	2035
NIST FIPS 203 / 204 / 205	of human web traffic using hybrid PQ (early 2026)	noisy qubits to break RSA-2048 (2025 estimate)	RSA-2048 disallowed (NIST draft)

Key takeaways

- A large, error-corrected quantum computer could break RSA and elliptic-curve cryptography, which protect most of today's internet.
- Post-quantum cryptography (PQC) is standardized: NIST published FIPS 203, 204 and 205 in August 2024 and picked HQC as a backup in 2025.
- Estimates of the quantum resources needed keep falling: under one million noisy qubits for RSA-2048 (Gidney, 2025), with newer preprints claiming fewer.
- Adoption is real on the client side, over 60% of human web traffic to Cloudflare used hybrid post-quantum key exchange by early 2026, but servers and internal systems lag badly.
- 'Harvest now, decrypt later' means long-lived secrets are already at risk; the migration is an engineering program, not a one-off patch.

Background: why quantum computers threaten encryption

Public-key cryptography relies on math problems that are easy one way and hard to reverse: factoring large numbers (RSA) and the discrete logarithm on elliptic curves (ECDH, ECDSA). In 1994 Peter Shor showed a quantum computer could solve both efficiently. Symmetric encryption (AES) and hashing are affected far less: Grover's algorithm only gives a square-root speed-up, which longer keys offset.

The danger isn't hypothetical just because the machine doesn't exist yet. Adversaries can record encrypted traffic today and decrypt it once a capable quantum computer arrives, known as **"harvest now, decrypt later."** Anything that must stay secret for 10–20 years is already exposed.

The standards

- **FIPS 203 (ML-KEM):** a lattice-based key-encapsulation mechanism (formerly CRYSTALS-Kyber) for establishing shared keys.
- **FIPS 204 (ML-DSA):** a lattice-based digital signature (formerly CRYSTALS-Dilithium).
- **FIPS 205 (SLH-DSA):** a hash-based signature (SPHINCS+) as a conservative backup.
- **HQC:** selected in March 2025 as a code-based backup KEM; FIPS 206 (FN-DSA, Falcon) is in development [1][2].
- **Transition:** NIST's draft IR 8547 deprecates 112-bit algorithms such as RSA-2048 after 2030 and disallows them after 2035 [2].

How fast is the threat moving?

- **2019:** about 20 million noisy qubits were estimated to factor RSA-2048 in hours.
- **May 2025:** Gidney estimated fewer than one million noisy qubits in under a week [3].
- **2026:** a preprint claims under 100,000 physical qubits using quantum LDPC codes under specific hardware assumptions, and a Google paper put elliptic-curve secp256k1 (used by Bitcoin and Ethereum) at around 500,000 physical qubits [2].
- These are estimates under assumptions, not demonstrations; today's largest machines have hundreds to low thousands of physical qubits.

Adoption in 2026

- **Clients:** Cloudflare reported client support for hybrid post-quantum key exchange rising from under 3% in early 2024 to over 60% of human traffic by February 2026 [4].
- **Servers:** only about 10–15% of origin servers Cloudflare connects to support it [4]. OpenSSL 3.5, GnuTLS 3.8.9 and Go 1.24 enabled hybrid PQ key exchange by default in 2025 [4].
- **Messaging:** Signal (PQXDH) and Apple iMessage (PQ3) added post-quantum protection for messages.
- **Big tech:** Google targets 2029 for full post-quantum security, including authentication [2].

Where QKD fits

Quantum key distribution uses quantum physics to detect eavesdropping while sharing keys. China has operated satellite QKD since the Micius satellite (2016), and ESA's Eagle-1 is due around 2026–27 [6]. But the NSA still does not recommend QKD for sensitive US systems: it requires special hardware and dedicated links, doesn't authenticate the source by itself, and is hard to validate [5]. For almost every organization, PQC is the practical path; QKD is a niche complement.

A practical migration playbook

1. **Inventory:** find every place cryptography lives: TLS, SSH, VPNs, code signing, tokens and JWTs, KMS/HSMs, databases, IoT firmware and third-party SaaS.
2. **Prioritize by secrecy lifetime:** data that must stay secret beyond 2030 goes first.
3. **Build crypto-agility:** make algorithms configuration, not code, so they can be swapped without redeploying everything.
4. **Roll out hybrid first:** combine classical and PQ (for example X25519 + ML-KEM) so security never drops below today's level.
5. **Measure:** watch handshake latency, packet sizes, error rates and middlebox breakage; roll out behind feature flags with canaries.
6. **Signatures and PKI:** plan certificate chains with PQ signatures; they are much larger and affect bandwidth and storage.
7. **Vendors:** add PQ readiness to procurement and security reviews.

How it could change life

Done well, users notice nothing: browsers, phones and apps quietly switch to quantum-safe cryptography. Done badly, we could see a sudden loss of trust in banking, health records, elections and

cryptocurrencies when a capable quantum computer appears. The migration protects privacy for decades of data that is being collected right now.

Future scenarios

2027
Hybrid PQ key exchange is default across browsers, clouds and major VPNs.

2030
RSA-2048 deprecated; regulated sectors complete inventories and most migrations.

2033–2035
Government-wide transition deadlines; classical public-key crypto disallowed for most federal use.

Q-day
Unknown. Expert estimates range from around 2029 (aggressive) to well after 2035.

- **Optimistic:** migration completes before a cryptographically relevant quantum computer exists.
- **Base case:** the internet edge is safe, but legacy and embedded systems remain exposed for years.
- **Pessimistic:** an early Q-day exposes harvested data and unmigrated systems, including blockchains.

Effects and risks

- **Migration risk:** rushed rollouts break things; most inventories are incomplete.
- **Performance:** larger keys and signatures affect handshakes, constrained IoT and certificate sizes.
- **Blockchains:** elliptic-curve signatures need coordinated, community-wide upgrades.
- **Inequality:** smaller organizations and countries may lag, becoming easy targets.

What to watch

- Error-corrected logical-qubit counts on real hardware.
- Server-side (origin) PQ adoption rates.
- Final NIST IR 8547 and sector-specific deadlines.
- PQ signatures in the Web PKI and certificate transparency.

My take

This is the largest infrastructure migration most organizations will run this decade, and it should be run like one: inventory, SLOs, canaries, dashboards and rollback plans. The math is settled; the operations are not. Start with long-lived secrets and build crypto-agility so the next algorithm change is a config change.

Key players & programs

NIST	FIPS 203/204/205 (2024), HQC (2025), transition plan IR 8547 [1][2]
NSA	CNSA 2.0 guidance; does not recommend QKD for sensitive US systems [5]
Cloudflare	Measures and deploys hybrid PQ TLS at internet scale [4]
Google	2029 target for full post-quantum security; resource estimates [2][3]
China / ESA	Satellite QKD: Micius (2016); Eagle-1 planned [6]

Frequently asked questions

What is post-quantum cryptography?
Encryption and signature algorithms designed to resist both classical and quantum computers, such as NIST's ML-KEM, ML-DSA and SLH-DSA standards from 2024.

When will quantum computers break RSA?
No one knows. Resource estimates have fallen to under one million noisy qubits for RSA-2048, but no machine is close today; estimates for 'Q-day' range from around 2029 to well after 2035.

What is 'harvest now, decrypt later'?
Recording encrypted data today in order to decrypt it once a capable quantum computer exists. It makes long-lived secrets vulnerable now.

Is quantum key distribution the answer?
For most organizations, no. The NSA does not recommend QKD for sensitive US systems because of hardware, authentication and validation limits. Post-quantum cryptography is the practical path.

Glossary

Shor's algorithm: A quantum algorithm that factors integers and computes discrete logarithms efficiently, breaking RSA and ECC.

ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism, standardized as FIPS 203.

Hybrid key exchange: Combining a classical and a post-quantum algorithm so both must be broken.

Crypto-agility: The ability to change cryptographic algorithms quickly, by configuration.

References

1. NIST — First 3 finalized post-quantum encryption standards (Aug 2024)
   https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
2. The Quantum Insider — Why 2026 matters for quantum security
   https://thequantuminsider.com/2026/04/28/why-2026-matters-quantum-security/
3. Gidney — How to factor 2048-bit RSA integers with less than a million noisy qubits (arXiv, 2025)
   https://arxiv.org/abs/2505.15917
4. Cloudflare — Origin PQ readiness, key transparency and ASPA on Radar (Feb 2026)
   https://blog.cloudflare.com/radar-origin-pq-key-transparency-aspa/
5. NSA — Quantum Key Distribution (QKD) and Quantum Cryptography
   https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
6. GMF — Quantum entangles the heavens (satellite QKD)
   https://www.gmfus.org/news/quantum-entangles-heavens
7. Cloudflare Radar — Post-quantum encryption worldwide (live)
   https://radar.cloudflare.com/post-quantum

Online: https://mohsinkhanshaik.com/research/quantum-cybersecurity · Facts are cited; outlooks and "My take" are the author's opinion.