Safe for the future?

QKD vs PQC.

Encryption Comparison.

sitehop

EBK-00002 (rev 1.0)

Introduction

As global networks brace for quantum-era threats, the choice between Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) is no longer academic. It's strategic.

QKD promises theoretically unbreakable security but requires specialised hardware and major infrastructure shifts. PQC offers scalable, high-speed encryption designed to run on today's networks, ready for tomorrow's threats.

The tables that follow outline how these two approaches compare across 20 critical categories. Higher scores reflect stronger real-world performance or strategic fit.

QKD vs PQC: Side by Side Comparison

Category	QKD	PQC
Core Principle	★★★★★ Uses quantum physics for key distribution, offering information-theoretic security	★★★★ Based on quantum-resistant mathematical problems, offering strong computational security
Technology Maturity	★★ Still early-stage with few real-world deployments	★★★★★ Deployment-ready, with ongoing global standardisation (NIST)
Security Model	★★★★★ Theoretically unbreakable due to quantum mechanics	★★★★ Extremely strong, though not mathematically “perfect”
Hardware Requirements	★ Requires quantum optical equipment and custom infrastructure	★★★★★ Runs on standard CPUs, FPGAs and ASICs
Transmission Medium	★★ Limited to fibre/free-space optics and short distances	★★★★★ Works across any digital network, globally
Distance Limitations	★ ~40–70 km as practical quantum repeaters do not exist	★★★★★ No inherent distance limits
Integration Complexity	★★ Complex to integrate, fragile to environmental interference	★★★★★ Simple software or hardware drop-in upgrade
Deployment Cost	★ High CapEx, bespoke systems, niche expertise	★★★★ Efficient, scalable and affordable deployment
Throughput Performance	★ Very low (key material only, not data)	★★★★★ Supports real-time, line-rate encryption (e.g., 100 Gbps)
Scalability	★ Not suitable for mass-scale networks or global deployment	★★★★★ Easily scales across national and international networks

sitehop

QKD vs PQC: Side by Side Comparison

Category	QKD	PQC
Real-Time Applications	★★★ Not inherently optimised for latency	★★★★★ Ideal for latency-sensitive, high-speed applications
Resistance to Side-Channels	★★★ Some benefits from physical layer, but still vulnerable at endpoints	★★★ Depends on algorithm and implementation quality
Quantum Readiness	★★★★★ Quantum-native by design	★★★★★ Purpose-built to resist quantum computing threats
Suitability for Cloud/Edge	★ Not viable due to infrastructure constraints	★★★★★ Perfect for virtualised, decentralised networks
Energy Efficiency	★ Power-intensive due to laser-based systems and cooling	★★★★ FPGA and ASIC implementations use minimal power
Standardisation	★★ Fragmented global efforts, no dominant standard	★★★★★ Formal standardisation via NIST well underway
Current Use Cases	★★★ Pilots in government/defence or financial sectors only	★★★★★ Active deployment across telecom, cloud, and enterprise
Sovereign Control	★★★ Depends on external quantum supply chains	★★★★★ Easily developed and audited under national control
Future Viability	★★★ Ideal for very short high security links where additional infrastructure can be deployed (new fibre)	★★★★★ Positioned to become the global security standard

Use Cases

QKD

Securing site-to-site VPNs

Adds quantum-grade protection to encrypted tunnels between branch offices or data centres.

Safe backbone for optical networks

Protects short-distance fibre (40Km) links between cities or cloud locations from interception. But require a separate dark fibre to work.

Shielding high-value transactions

Ensures real-time financial or industrial data can’t be tapped during transfer.

Encrypted control links in critical networks

Secures remote commands in utility grids, transport hubs, or military sites.

Trusted link setup between partners

Builds private communication lines between organisations with zero risk of key theft.

PQC

Quantum-safe IPsec and TLS

Upgrades current encryption used in internet and private WAN traffic for long-term safety.

Protecting routers and switches

Secures routing protocols and control plane messages across the network.

Cloud data migration

Ensures encrypted transfers between cloud regions or providers stay safe, even decades from now.

Resilient SD-WAN overlays

Provides quantum-resistant encryption for traffic across dynamic, multi-site networks.

Secure partner interconnects

Keeps APIs and B2B data exchanges protected across organizational boundaries, even at high speed.

The Verdict

Total Scores

QKD: 50 / 100

PQC: 92 / 100

Key Takeaways

- QKD is brilliant theory, but difficult to apply at commercial scale.
- PQC offers practical, scalable cryptography, ready for enterprise, cloud and telecoms and compatible with existing infrastructure.
- For performance, simplicity and global adoption, PQC wins decisively and offers diverse algorithm options.
- QKD may have niche use cases, but PQC will be the backbone of post-quantum security.

Verdict

PQC Is the Real-World Winner

In high-speed, high-stakes environments, from hyperscaler data centres to telecom cores, PQC is the only viable path to scalable, post-quantum protection. It's ready now, efficient, highly compatible and it's designed to evolve.

sitehop