Tech & AI Systems | Nov 18, 2026 | 5 min read | By Bryan White

Post-Quantum Encrypted Transfer Achieves 100x Throughput Gains Over Intermittent Edge Links

Tech & AI Systems * Natural Science * Research Dispatch

In November 2026, VIA Science announced a transport-layer upgrade to its VIA Quantum Transfer (QT) platform that accelerates quantum-resistant encrypted file transfers by up to 100-fold over degraded, low-bandwidth, and intermittent wireless links. Coinciding with the platform's designation as "Awardable" on the U.S. Department of Defense (DoD) Tradewinds Solutions Marketplace, the benchmark tests highlight a central systems-engineering bottleneck in post-quantum cryptography (PQC): while lattice-based key encapsulation protects data against "Harvest Now, Decrypt Later" (HNDL) adversaries, larger handshake artifacts and stateful transport retries can cripple throughput on edge sensors, uncrewed aerial vehicles, and maritime links.

In representative field-style testing reported by VIA Science, transferring a 5-megabyte sensor payload over a weak, intermittently dropping connection fell from more than one hour to roughly 40 seconds. Even brief 2-to-3-second connectivity windows -- previously sufficient only for minimal status heartbeats -- become usable for transmitting structured maps, operational logs, and high-resolution anomaly captures.

Why Post-Quantum Cryptography Strains Disrupted Edge Links

Classical public-key protocols such as RSA, Diffie-Hellman, and elliptic-curve cryptography (ECC) derive security from integer factorization or discrete-logarithm problems, both of which a fault-tolerant quantum computer running Shor's algorithm could solve in polynomial time. To counter adversaries already intercepting and archiving encrypted traffic for future decryption (the HNDL threat model), the National Institute of Standards and Technology (NIST) standardized Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) under FIPS 203 in August 2024, derived from CRYSTALS-Kyber and grounded in the hardness of the Module Learning with Errors (MLWE) problem.

Transitioning from classical ECC to lattice-based cryptography such as ML-KEM-768 or ML-KEM-1024 -- often deployed in hybrid modes alongside X25519 -- dramatically expands public-key and ciphertext sizes from tens of bytes to roughly one kilobyte or more per handshake. Over high-throughput fiber links, that overhead is negligible. Over congested tactical radios, satellite backhauls, or maritime links experiencing frequent packet loss and 2-to-3-second link dropouts, conventional TCP/TLS session teardowns force repeated multi-kilobyte post-quantum handshakes and congestion-window collapses, stalling payload delivery indefinitely.

| Operational / Cryptographic Metric | | Legacy Transport Over Weak Links | | VIA Quantum Transfer (Nov. 2026 Upgrade) |

| Threat Model Addressed | | Classical eavesdropping; vulnerable to HNDL | | Quantum-resistant encryption mitigating HNDL attacks |

| 5 MB Sensor File Benchmark | | >1 hour on degraded intermittent connection | | ~40 seconds (~100x throughput improvement) |

| Minimum Viable Link Window | | Requires sustained session for full handshake | | 2-3 second windows transfer maps & sensor logs |

| Edge Power & RF Footprint | | Prolonged radio duty cycle & battery drain | | Rapid burst completion reduces RF detection exposure |

| Defense Procurement Status | | Ad-hoc custom edge wrappers | | Awardable on DoD Tradewinds Solutions Marketplace |

Resilient Session Framing and Forward Error Handling

Achieving a 100-fold speedup on a degraded channel without weakening cryptographic guarantees requires decoupling session cryptography from brittle connection-oriented transport. In standard TCP-backed file transfer protocols, packet loss is interpreted as network congestion, triggering exponential backoff and shrinking transmission windows. When a link drops entirely after three seconds, ephemeral session state is lost and the next connection attempt must renegotiate keys and restart or re-synchronize large blocks from scratch.

Quantum-resistant edge transfer architectures bypass this failure mode by combining persistent cryptographic session resumption with aggressive packet-level framing, out-of-order block reassembly, and loss-tolerant transport scheduling. Rather than allowing a brief RF fade to discard partially transmitted ciphertext blocks, each encrypted chunk is independently authenticated and resumable across fragmented 2-to-3-second contact windows. Consequently, nearly 100 percent of available airtime during fleeting line-of-sight or satellite passes goes toward forward payload progress rather than repetitive handshake overhead.

Operational Security: Lowering RF Exposure and Energy Budgets

Compressing a one-hour encrypted transmission down to roughly 40 seconds yields immediate physical-layer advantages beyond raw data throughput. Remote autonomous sensors and uncrewed platforms operate under tight battery budgets where high-power radio-frequency (RF) transmission dominates energy draw; cutting active transmit duration by two orders of magnitude extends field deployment endurance without heavier battery packs.

In contested defense and maritime environments, shorter transmission bursts also reduce electromagnetic emissions signatures. Prolonged RF transmissions give adversary direction-finding arrays ample time to geolocate a transmitter; completing quantum-resistant data exfiltration inside brief, sporadic burst windows minimizes both interception opportunity and electronic-warfare vulnerability.

Standardization Momentum Across Defense and Critical Infrastructure

VIA Quantum Transfer's "Awardable" status on the DoD Tradewinds Solutions Marketplace -- evaluated through the Super Intelligence Office (SIO) -- reflects accelerating federal procurement pressure to transition mission-critical telemetry onto quantum-resistant protocols ahead of federal post-quantum migration deadlines. Because defense, energy-grid, and law-enforcement telemetry often remains sensitive

for decades, protecting edge-to-cloud links against HNDL collection is treated as an immediate operational requirement rather than a distant theoretical upgrade.

As FIPS 203 ML-KEM and companion lattice signature standards proliferate across enterprise and defense networks, engineering efforts like VIA's transport optimization demonstrate that post-quantum security need not come at the expense of edge-network usability -- even when links last only a few seconds at a time.

References & Primary Sources

* [1] National Institute of Standards and Technology (NIST) (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). -- https://csrc.nist.gov/pubs/fips/203/final

* [2] VIA Science (2026). VIA Quantum Transfer (QT) 100x Speed Upgrade & DoD Tradewinds Solutions Marketplace Announcement. -- https://www.solvewithvia.com/

* [3] Quantum Zeitgeist (2026). VIA Science Achieves 100x Quantum-enhanced Encrypted Data Transfer. -- https://quantumzeitgeist.com/