HelioLink Technologies

White Paper — Quantum Encryption R&D; | Version 2.0 | December 2025

Photonic Acceleration of Post-Quantum Cryptographic Processes

Author: Jacob McMillan

ABSTRACT

The federal government has committed $7.1 billion to migrate prioritized systems to post-quantum cryptography by 2035. The algorithms are ready. The problem is computational overhead—NIST's standardized PQC schemes demand 30-100x more processing power than classical cryptography on constrained devices. This paper outlines HelioLink's research into addressing that gap through two established technologies: quantum random number generation for cryptographic entropy, and photonic integrated circuits for computational offloading.

1. The Problem is Performance, Not Algorithms

On August 13, 2024, NIST finalized three post-quantum cryptographic standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). A fourth standard based on FALCON is expected in 2025. In March 2025, NIST selected HQC as a backup algorithm, providing cryptographic diversity based on error-correcting codes rather than lattices. [1][2]

The algorithms work. They're mathematically sound against both classical and quantum attack vectors. The challenge is deploying them.

Recent benchmarks paint a clear picture: lattice-based schemes like ML-KEM slow down by 30-50x on resource-constrained platforms compared to desktop implementations. Hash-based signatures (SLH-DSA) can exceed 100x slowdown for signing operations. [3] For a network encryption gateway processing thousands of TLS handshakes per second, or a tactical radio with strict SWaP constraints, those numbers represent a functional barrier.

CISA, NSA, and NIST have been direct about this. Their joint guidance acknowledges that migration will take until 2035 and requires organizations to prioritize systems based on both quantum vulnerability and resource constraints. [4] The Office of the National Cyber Director projects the federal government alone will spend $7.1 billion on this transition. [5]

2. What NIST Actually Standardized

Standard	Algorithm	Type	Primary Bottleneck
FIPS 203	ML-KEM (Kyber)	Lattice KEM	NTT, polynomial mult.
FIPS 204	ML-DSA (Dilithium)	Lattice Sig	NTT, rejection sampling
FIPS 205	SLH-DSA (SPHINCS+)	Hash-based Sig	Hash chain computation
FIPS 206	FN-DSA (Falcon)	Lattice Sig	FFT, floating-point

ML-KEM and ML-DSA share a foundation: the Module Learning With Errors (MLWE) problem. Both rely heavily on Number Theoretic Transform (NTT) operations—essentially specialized FFTs over finite fields. These are computationally intensive but highly parallelizable. [6]

3. Current State: Hardware Acceleration Exists

The obvious response to PQC's computational demands is hardware acceleration. FPGA implementations already demonstrate 3-9x speedups over optimized software, even software using CPU vector instructions like AVX2. [7]

This isn't new territory. Cryptographic offloading has been standard practice in high-assurance environments for decades. NSA Type 1 devices—the encryption systems certified for classified information—have always used dedicated hardware. [8] The CNSA 2.0 transition timeline, published by NSA in December 2024, mandates quantum-resistant algorithms in national security systems by specific dates. [9]

Current accelerators are electronic. ASICs, FPGAs, specialized coprocessors. They work, but they're hitting fundamental limits: power consumption scales with clock frequency, interconnect bottlenecks create latency, and parallelism is constrained by physical interference.

4. Two Technologies We're Researching

4.1 Quantum Random Number Generation

Every cryptographic system needs randomness. Quantum random number generators exploit fundamental quantum mechanical processes—photon arrival times, vacuum fluctuations, beam splitter outcomes—to produce randomness that is provably unpredictable. Not computationally hard to predict; impossible to predict, by the laws of physics.

In April 2025, Quantinuum's Quantum Origin became the first software QRNG to achieve NIST SP 800-90B validation as an entropy source. [10] Hardware QRNGs achieve min-entropy rates above 7.8 bits/byte—near the theoretical maximum of 8. [11]

> *HelioLink Research Direction:* We're developing a QRNG platform (internally designated 'Hugo') based on photon detection timing, targeting NIST SP 800-90B validated entropy generation at rates sufficient for high-throughput PQC key generation.

4.2 Photonic Integrated Circuits for Logic Operations

Photonic computing uses light instead of electrons. Advantages: speed (picosecond switching), parallelism (WDM enables multiple independent channels), power efficiency, and reduced thermal load.

Photonic logic gates aren't theoretical. Mach-Zehnder interferometer configurations have demonstrated XOR, AND, OR, NAND, and NOR operations with response times around 1.56 picoseconds. [12] In April 2025, Nature published research on a large-scale photonic accelerator with over 16,000 integrated components demonstrating ultralow latency for matrix operations. [14]

> *HelioLink Research Direction:* We're investigating photonic implementations of the specific operations that bottleneck PQC: NTT butterfly operations for lattice-based schemes, parallel hash computation for SLH-DSA.

5. The Integration Challenge

Combining QRNG entropy with photonic computation requires solving several engineering challenges: electro-optical interfaces that don't bottleneck processing, control plane architecture that maintains cryptographic sequencing, side-channel resistance appropriate for the photonic domain, and a certification pathway through NIST's CMVP for FIPS 140-3 validation.

None of these challenges are insurmountable. They're engineering problems, not physics problems.

6. Why This Matters for Migration

NSA's CNSA 2.0 guidance specifies: PQC for software/firmware signing by 2025, network equipment by 2026, operating systems by 2027, majority of NSS traffic by 2030, and complete deprecation of classical public-key cryptography by 2033. [9]

Organizations following CISA's guidance are already inventorying cryptographic dependencies. The question isn't 'should we migrate' but 'how do we migrate systems that can't handle the computational load.' Hardware acceleration is the answer. Photonic acceleration may be a better answer for specific use cases.

7. What We're Not Claiming

- We haven't built a production photonic PQC accelerator. No one has. This is R&D.;
- Photonic acceleration isn't required for PQC migration. Electronic accelerators work.
- We're not claiming to replace existing Type 1 devices.
- Quantum computers aren't breaking RSA tomorrow. But 'harvest now, decrypt later' attacks mean data encrypted today may be vulnerable.

What we are claiming: the combination of quantum entropy sources and photonic computation represents a viable research direction for addressing PQC's performance challenges, grounded in demonstrated physics and engineering precedent.

8. Conclusion

Post-quantum cryptography is happening. The algorithms are standardized, the migration timelines are set. HelioLink's research addresses implementation challenges through quantum random number generation for entropy and photonic integrated circuits for computational acceleration. We're pursuing a research direction that could expand options for organizations facing the largest cryptographic transition in computing history.

References

[1] NIST. 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards.' August 2024.

[2] NIST. 'NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption.' March 2025.

[3] Performance Analysis of PQC for Consumer Electronics. arXiv:2505.02239. May 2025.

[4] CISA/NSA/NIST. 'Quantum-Readiness: Migration to Post-Quantum Cryptography.' August 2023.

[5] ONCD. 'Report on Post-Quantum Cryptography.' July 2024. ($7.1B federal migration cost)

[6] Lyubashevsky. 'Basic Lattice Cryptography: Kyber and Dilithium.' ePrint 2024/1287.

[7] ACM TRETS. 'Hardware Acceleration for CRYSTALS-Kyber and Dilithium.' 2024.

[8] Curtiss-Wright. 'NSA Type 1 Encryption for Data-at-Rest.'

[9] NSA. 'CNSA 2.0 FAQ.' December 2024 (Version 2.1).

[10] Quantinuum. 'Quantum Origin Achieves NIST SP 800-90B Validation.' April 2025.

[11] NIST SP 800-90B. 'Recommendation for Entropy Sources.' 2018.

[12] Results in Optics. 'Photonic MUX logic gates via MZI.' February 2024. (1.56ps response)

[13] J. Computational Electronics. 'Photonic crystal logic gates.' December 2024.

[14] Nature. 'Large-scale photonic accelerator with ultralow latency.' April 2025.