NSA CSfC Listed

Securing the Future:

Implementing Quantum-Safe Algorithms in Solid-State Drives

the Future of Memory and Storage

CipherDriveOne a KLC Group Company

Experts in DAR

FMS the Future of Memory and Storage

KLC Group delivers a one-of-a-kind Data-at-Rest (DAR) protection products that are unique in technology and certification.

We're experts in encryption and authentication.

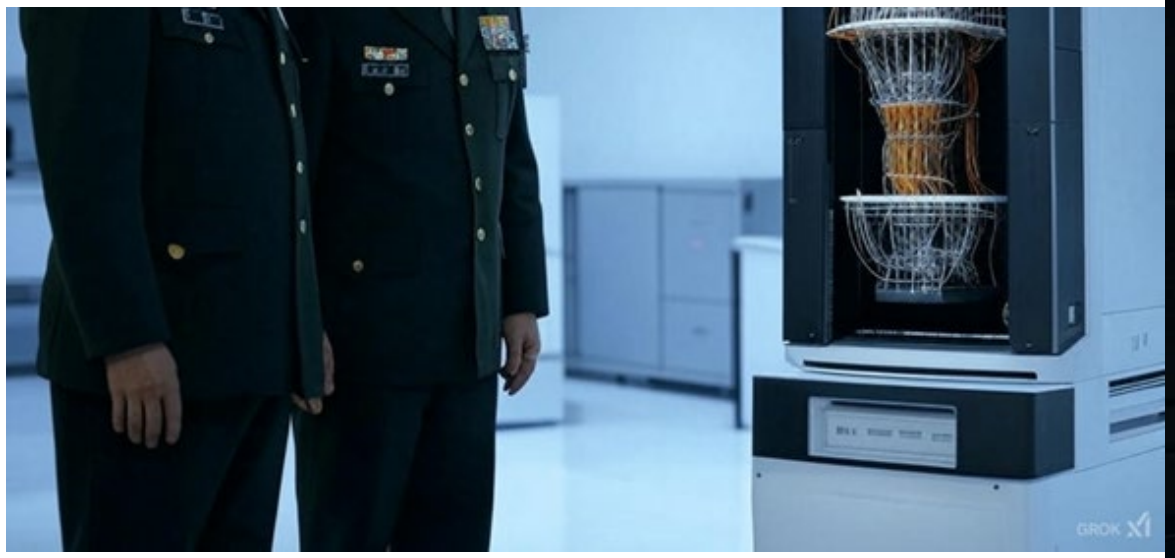
Kurt Lennartsson
KLC Group
Founder and CEO

John C. Myung
KLC Group
President

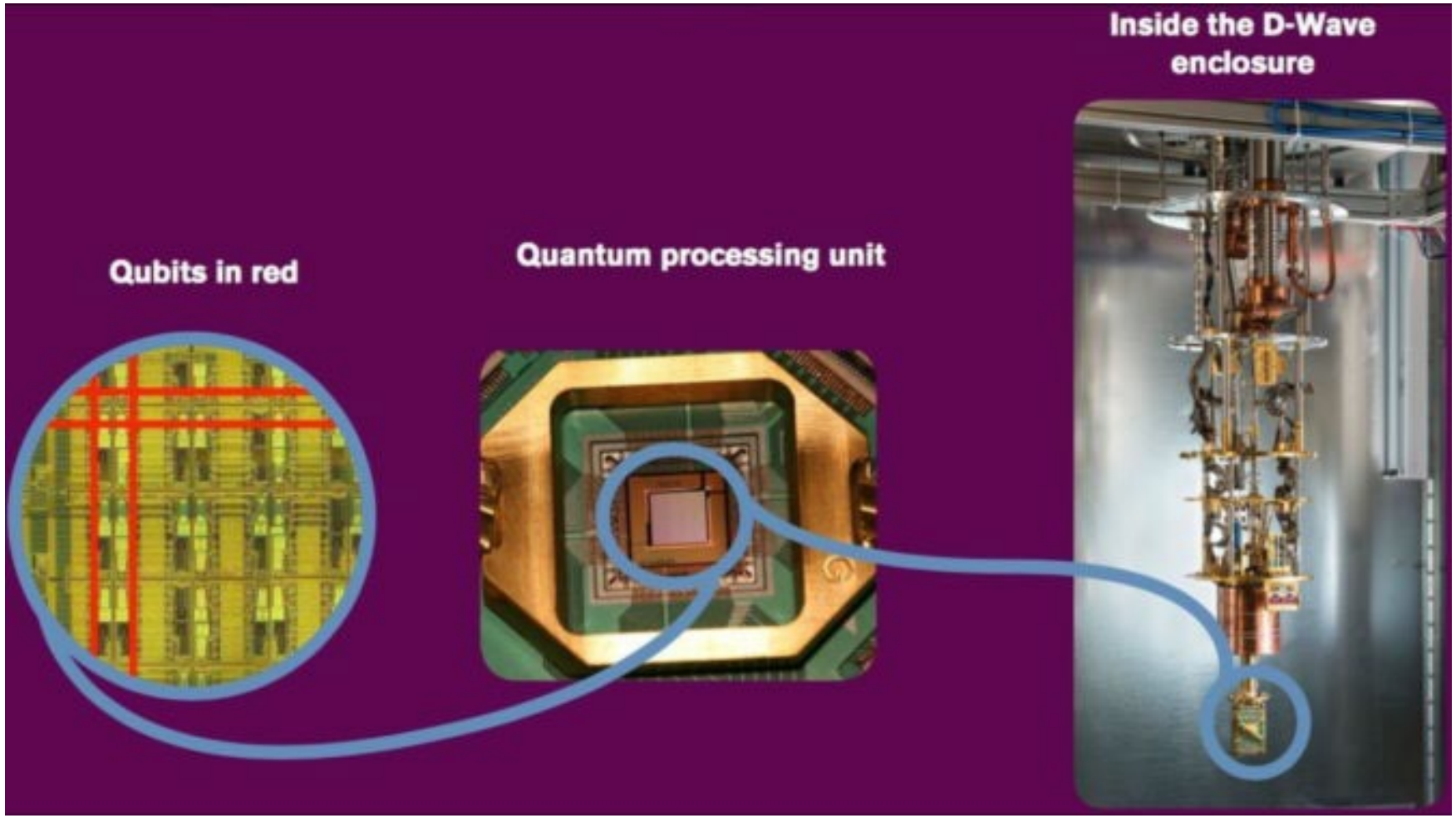
Keith Fuentes
KLC Group
VP of Sales

Waking The Sleeping Giant

FMS the Future of Memory and Storage



Qubit, QPU, D-WAVE



Shor's Algorithm

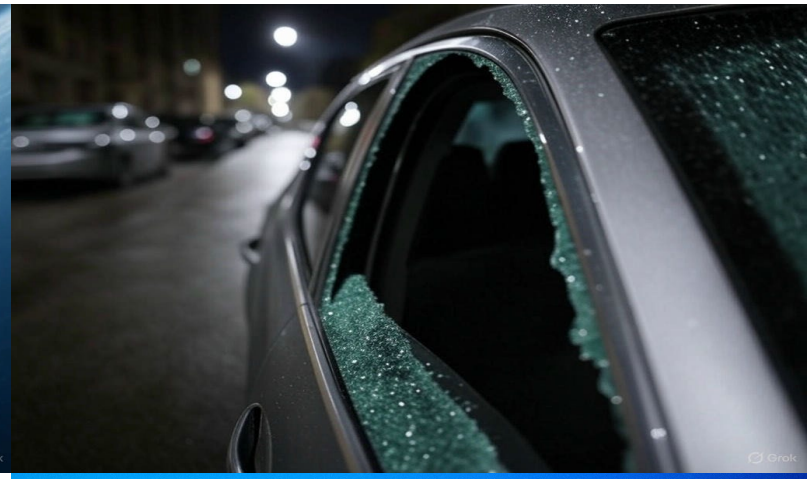
$O((\log N)^2 (\log \log N) (\log \log \log N))$, where N is the number to factor

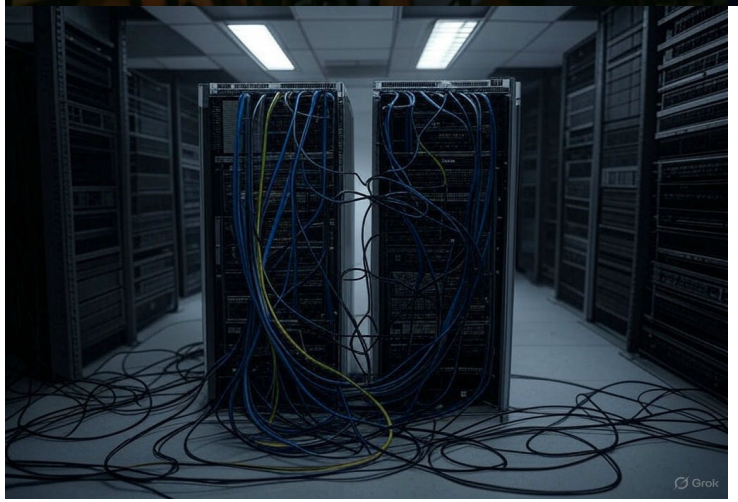
Grover's Algorithm

O(2^256) operations,
but Grover's cuts this to
O(2^128)
Decreases brute force attack on AES 256 to 128 bits

Harvest Now, Decrypt Later

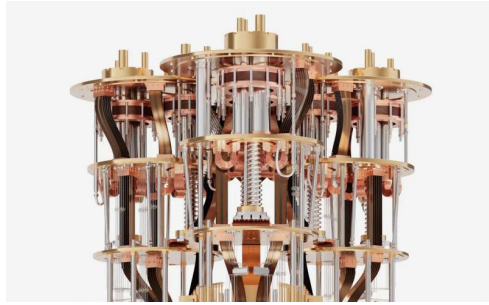
FMS the Future of Memory and Storage





Are We Too Early or Too Late?

IBM Condor: 1,121 Qubits



Atom Computing: 1,125+ Qubits

PsiQuantum: 1M + Qubits

Quantum Safe Algorithms for CSfC

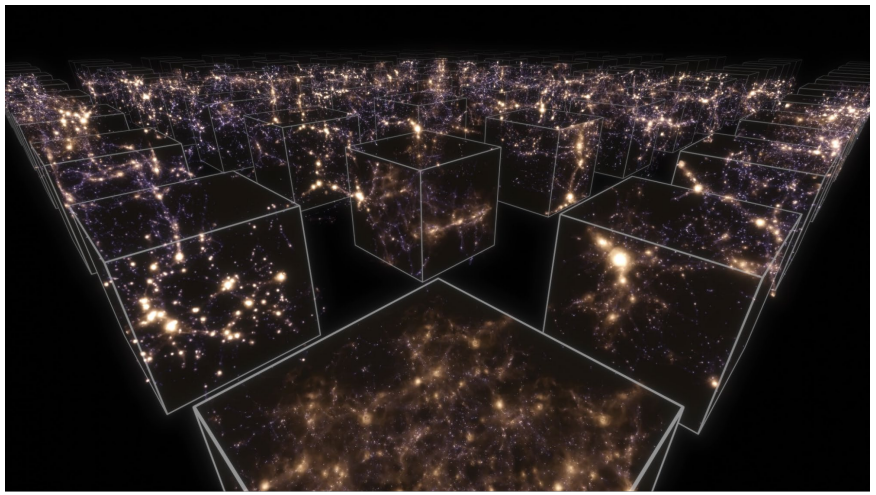
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

1. ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)
   - Previously: CRYSTALS-Kyber
   - Purpose: General encryption (key encapsulation)
   - Standard: FIPS 203[](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)[](https://industrialcyber.co/nist/nist-approves-three-quantum-resistant-encryption-standards-bolsters-cybersecurity-posture/)

2. ML-DSA (Module-Lattice-Based Digital Signature Algorithm)
   - Previously: CRYSTALS-Dilithium
   - Purpose: Digital signatures
   - Standard: FIPS 204[](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards)[](https://industrialcyber.co/nist/nist-approves-three-quantum-resistant-encryption-standards-bolsters-cybersecurity-posture/)

Integrating Post Quantum Into CSfC

1. Software Libraries
2. Hardware Acceleration
3. Longer AES key-length



Quantum Safe: Software Libraries

Availability: Today

Usage:

- Quantum Seed (Quantinium)
- Open Quantum Safe (OQS) project Libogs
- PQShield's PQCryptoLib
- Longer key length – AES 512

Challenges: Processor Use, Testing and Certification

Quantum Safe: Hardware Acceleration

Availability: 3-5 years

Usage:

- NVIDIA cuPQC
- IDEMIA Secure Transactions

Challenges: Industry Adoption, Testing and Certification

Conclusion: Act Now

FMS the Future of Memory and Storage

1. Start a post quantum-safe roadmap
2. Build robust controller architecture
3. Firmware updates

Questions & Thank you

John C. Myung
KLC Group, LLC
President
+1.408-219-5706
john@klc-group.com