POST-QUANTUM CRYPTOGRAPHY EXPLAINED

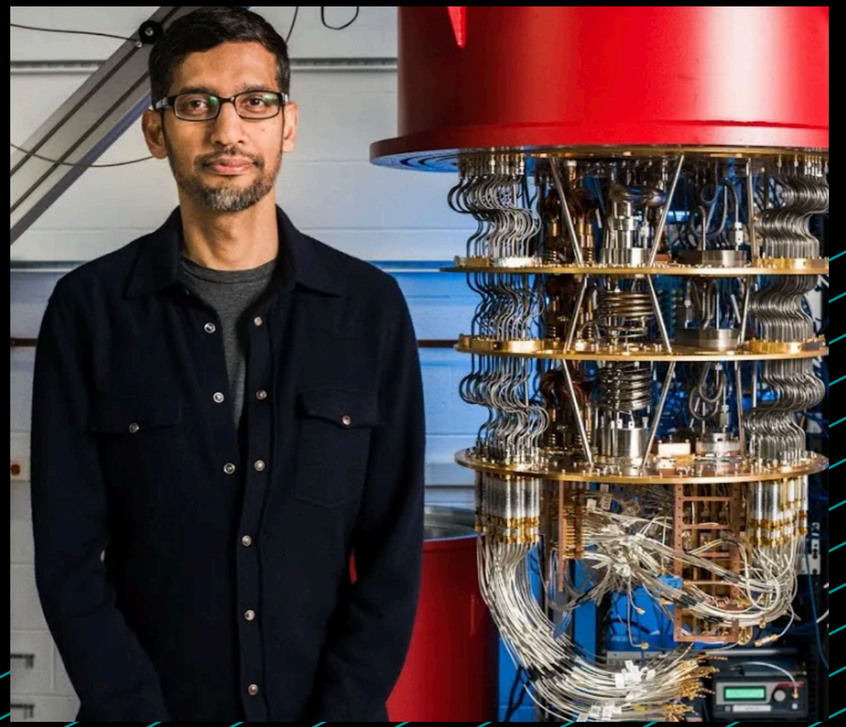
for security professionals

ALFRED MENEZES

https://cryptography101.ca

WHAT IS PQC?

- Cryptographic algorithms designed to remain secure even in the presence of quantum computers.
- RSA and elliptic curve cryptography can be easily broken using Shor's algorithm, which is a quantum algorithm.
- PQC algorithms are built on different mathematical foundations, including:
  - lattices
  - hash functions
  - error-correcting codes

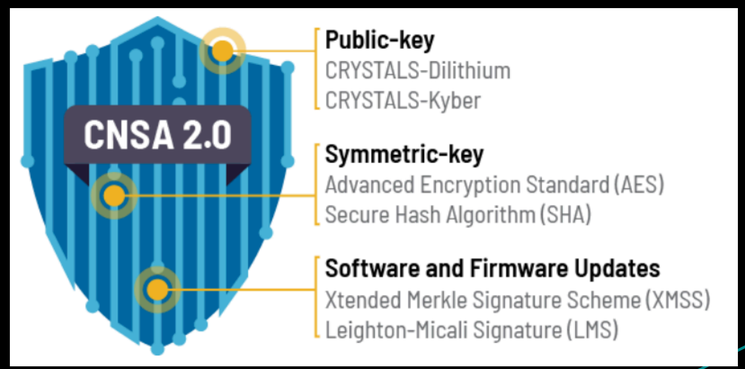


WHY PQC MATTERS

- Quantum computers can decrypt much of today's encrypted communications, including email, web, VPNs.
- Possibility of "Harvest-Now, Decrypt-Later" (HNDL) attacks.
- PQC is being mandated by some governments and industries, with a goal of full migration by 2030-2035.
- Demand for quantum-safe products is growing.

CANADIAN CENTRE FOR CYBER SECURITY

Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)

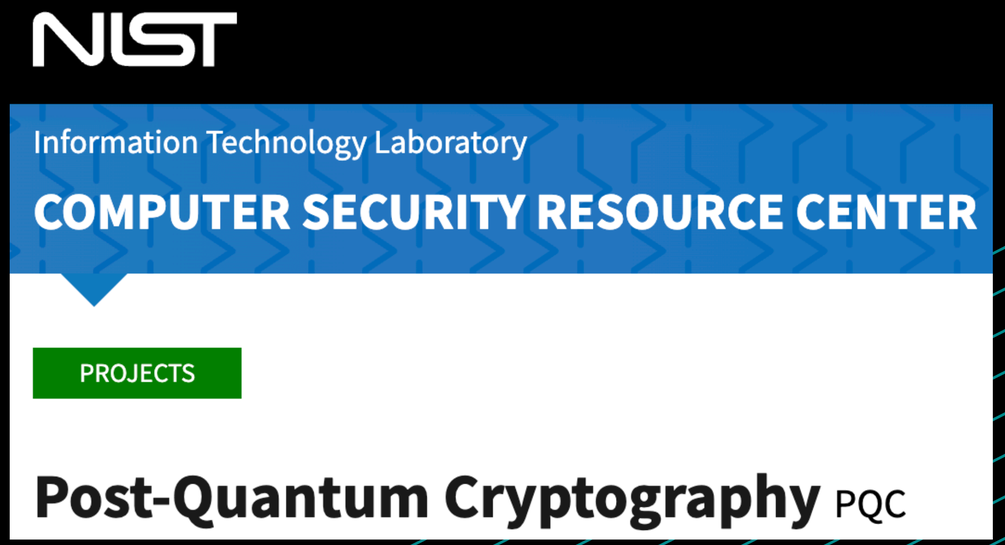


A coordinated implementation of roadmap for the transition to post-quantum cryptography

NIS COOPERATION GROUP

THE PQC LANDSCAPE

- PQC algorithms provide security guarantees against attacks from both classical and quantum computers.
- PQC is being standardized and prepared for real-world deployment.
- The most prominent standardization effort is by the U.S. government's National Institute of Standards and Technology (NIST).
- Leading candidates:
  - Lattice-based
  - Hash-based
  - Code-based

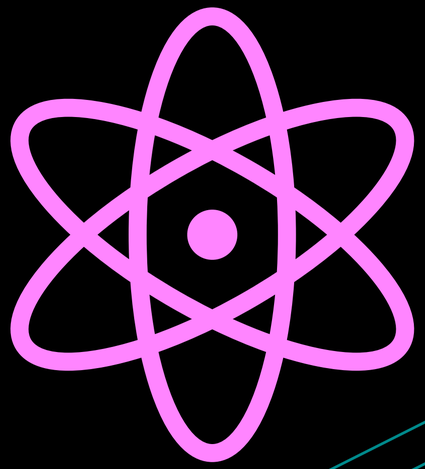


CHALLENGES WITH DEPLOYING PQC

- Various tradeoffs to consider, including:
  - Public key size
  - Ciphertext/signature size
  - Stateful or stateless?
  - Speed
  - Suitability for hardware implementation
  - Suitability for constrained devices

LOOKING AHEAD

- The state of quantum computing.
- Lattice-based encryption and signature schemes:
    - Kyber (ML-KEM), Dilithium (ML-DSA), Falcon (FN-DSA), FrodoKEM
- Hash-based signature schemes:
    - LMS, XMSS, SPHINCS+ (SLH-DSA)
- Code-based encryption schemes:
    - Classic McEliece, HQC
- Hybrid schemes
- Challenges with migrating to quantum-safe systems.



CLOSING

- Quantum computers explained
- The threat of quantum computers
- Quantum-safe cryptography
- PQC standards
- PQC migration timelines
- PQC software
- PQC deployments
- Hash-based signatures
- Lattice-based cryptography
- Kyber (ML-KEM) explained
- Dilithium (ML-DSA) explained
- …… and many more