POST-QUANTUM CRYPTOGRAPHY EXPLAINED

for security professionals

PQC SOFTWARE LIBRARIES

ALFRED MENEZES

PQC ALGORITHMS

- ML-KEM (Kyber)
  - ML-KEM-512: NIST Security Level 1
  - ML-KEM-768: NIST Security Level 3
  - ML-KEM-1024: NIST Security Level 5
- ML-DSA (Dilithium)
  - ML-DSA-44: NIST Security Level 2
  - ML-DSA-65: NIST Security Level 3
  - ML-DSA-87: NIST Security Level 5
- NIST: SLH-DSA (SPHINCS+), LMS, XMSS, FN-DSA (Falcon), HQC.
- Other: FrodoKEM, Classic McEliece.

- A cryptographic primitive has a security level of k bits if the fastest attack known takes approximately 2^k steps.
- In practice, one should aim for the 128-, 192- or 256-bit security levels.
- NIST security levels 1/2, 3/4 and 5, roughly correspond to the 128-, 192-, and 256-bit security levels.

POST-QUANTUM CRYPTOGRAPHY ALLIANCE

- Post-quantum cryptography code projects in the Linux Foundation.

- Open Quantum Safe (OQS): an open-source initiative designed to enable early experimentation and deployment of quantum-safe cryptography.
    - liboqs: a unified API for dozens of PQC algorithms.
- Post-Quantum Code Package (PQCP): open-source high-assurance implementations of standardized PQC algorithms. The code is formally verified, and deemed ready for integration into large software projects and products.

SUPERCOP

- SUPERCOP: System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives.
- Not a deployment library, but a benchmarking framework for comparing the performance of cryptographic primitives, including many PQC algorithms, across a wide variety of hardware platforms.

NETWORKING & CLOUD IMPLEMENTATIONS (1)

- libcrypto (OpenSSL): focused on hybrid TLS deployments.

- The Bouncy Castle project offers open-source APIs for Java, C# and Kotlin that includes production-quality implementations of the NIST PQC algorithms.

- BoringSSL (Google): designed to be used in Google's products such as Chrome and Android. Open source, but not recommended for general, third-party use.

- CIRCL (Cloudflare): written in Go, CIRCL is used for experimental PQC deployments in high-traffic network environments.

NETWORKING & CLOUD IMPLEMENTATIONS (2)

- AWS-Libcrypto and s2n-tls: Maintained by Amazon, AWS-Libcrypto (AWS-LC) is a general-purpose cryptographic library, while s2n-tls provides a TLS implementation capable of hybrid PQC handshakes at a cloud scale.

- CryptoKit (Apple): written in Swift, and includes implementations of Kyber, Dilithium, and ECDH-Kyber hybrid key exchange.

- wolfCrypt (wolfSSL): cryptographic engine for lightweight and embedded environments, emphasizing speed and portability, and supporting most of the NIST-standardized PQC algorithms.

LANGUAGE-SPECIFIC LIBRARIES

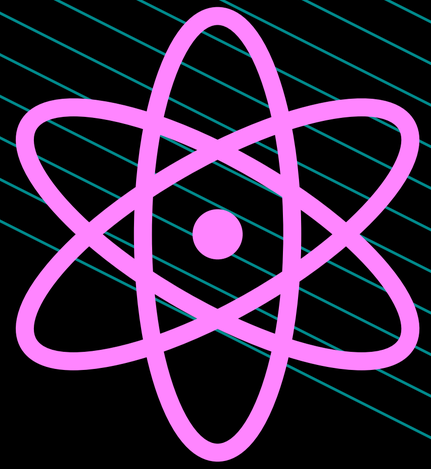
- Java (OpenJDK/JDK 24+):
  Through JEP 496 and JEP 497, Java now includes native support for ML-KEM and ML-DSA within the standard java.security package.

- Rust:
  The RustCrypto project maintains several pure-Rust implementations of PQC algorithms. These are useful for memory-safe systems programming.

COMMERCIAL LIBRARIES

- Two commercial software libraries are:
  - PQCryptoLib-Core (from PQShield):
    FIPS 140-3 CMVP certified general-purpose cryptographic library, designed for a wide variety of applications.
  - Radiate (from ISARA):
    Focuses on integration with existing security infrastructures, especially in government and financial sectors.

CLOSING



- There is already a rich ecosystem of post-quantum cryptographic software libraries.
- These libraries are enabling the global transition towards a quantum-safe future.