LAB ASSIGNMENT - 2

Exploring Post-Quantum Cryptography with liboqs.

- **Post Quantum Cryptography:**

After several rounds of evaluation, NIST has selected three main algorithms for standardization:

- CRYSTALS-KYBER (for key encapsulation and encryption).
- CRYSTALS-DILITHIUM (for digital signatures)
- SPHINCS+ (stateless hash-based signature scheme)

1) CRYSTALS-KYBER.

Kyber is a lattice based Key Encapsulation Mechanism (KEM) designed for fast and secure key exchange. It provides:

- High security against both classical and quantum attacks.
- Efficient computation suitable for constrained devices.
- Moderate key sizes (public key ≈ 800 bytes, ciphertext ≈ 768 Bytes)

- Kyber's performance is sometimes faster than classical ECC, making it ideal for integration into protocols like TLS for secure internet communication.

2) CRYSTALS-DILITHIUM.

- Dilithum is another lattice-based scheme, is used for digital signatures. It balances strong security with manageable key and signature sizes (public key ≈ 1.31KB, ~~cipher~~ signature ≈ 2.7KB)

- Its deterministic nature simplies implementation and reduces the risk of randomness-based vulnerabilities.

3) SPHINCS+

- SPHINCS+ is a hash-based signature algorithm providing conservative, well understood security.
- However, it has large signature sizes (≈ 17KB) and slower signing times, making it less suitable for high performance applications.

It remains valuable in scenarios demanding the highest assurance levels, such as firmware signing or long-term digital archival.

Tradeoffs between security, performance & key-sizes.

Aspect	Classical (RSA/ECC)	PQC
Security	• Broken by quantum computers.	• Resistant to quantum and classical attacks.
Public key size	• small (32-512 bytes)	• Larger (1KB-1MB)
Signature / ciphertext size	• small (64-256 bytes)	• Larger (1-20KB)
Speed	• fast, well-optimised	• slightly slower but improving rapidly
Memory and Bandwidth	• Efficient	• Higher requirements
Maturity	• Widely Adopted	• still in early deployment phase.

- **Security**
  - PQC schemes are designed to withstand both quantum & classical attacks.
  - Lattice based algorithms like Kyber and Dilithium rely on learning with Errors (LWE) problem, which is harder for even quantum computers.

- **Performance.**
  - While some PQC algorithms are slower due to complex mathematical operations, lattice-based schemes perform efficiently on most hardware platforms. Implementation of optimised for modern CPUs and embedded devices show only minimal slowdown compared to ECC.

- **Key and signature sizes.**
  - One of the major challenges in PQC deployment is the increase in key and signature sizes.
  - RSA-2048 uses a 256-byte key, while Kyber's public key is about 800 bytes. ~~and~~
  - Larger keys and ciphertexts lead to increased memory usage and bandwidth consumption, particularly problematic in IOT devices and low-latency system.

• Hybrid Cryptographic schemes :

- A hybrid scheme combines both classical and post-quantum algorithms in a single protocol. For example:
  - In TLS 1.3, both an Ecc key exchange and a Kyber KEM could be used together.
  - The final session key is derived from both components, ensuring that even if one is broken, the overall security remains intact

Benefits :

- Quantum resilience : Security holds even if one component is compromised.
- Compatibility : Allows gradual migration from classical to PQC Algorithms without breaking existing infrastructure.
- Trust Transition : Offers real-world testing of PQC performance and reliability while maintaining classical fallbacks.

Real-World Application

- Google and Cloudfare have implemented hybrid Kyber + X25519 key exchanges in experimental versions of TLS.
- OpenSSL and Microsoft have begun integrating PQC-ready modules for secure communications.
- This gradual adoption ensures interoperability and real-world validation before full PQC migration.