Title: Comparative Study of Post-Quantum and Classical Cryptography Algorithms

Author: Akshit | Sanket | Vaibhav | Meharvan

Lab Assignment 2 – Post-Quantum Cryptography with liboqs

1. Introduction

Quantum computing threatens classical cryptographic systems like RSA and ECDSA, which rely on mathematical problems solvable by quantum algorithms. Post-Quantum Cryptography (PQC) aims to secure communications against such threats. This report compares PQC algorithms Kyber512 and Falcon-512 with classical RSA-2048 and ECDSA P-256 in terms of key sizes, ciphertext/signature sizes, and performance.

2. Algorithms Evaluated

Category	Algorithm
KEM (PQC)	Kyber512
SIG (PQC)	Falcon-512
Classical	RSA-2048, ECDSA P-256

3. Experimental Setup

- **OS**: Ubuntu 24.04 LTS
- **Compiler**: GCC 9.2.0
- **liboqs version**: 0.14.0
- **Timing method**: `clock_gettime(CLOCK_MONOTONIC, &ts)`
- **Message used**: `"Post-Quantum Cryptography is the future"`

---

4. Key and Signature/Ciphertext Sizes

Algorithm	**Public Key**	**Private Key**	**Ciphertext / Signature**
Kyber-512	800B	1632B	768B
Falcon-512	897B	1281B	666B
RSA-2048	256B	1190B	256B
ECDSA P-256	64B	32B	64B

---

5. Execution Time Comparison

Algorithm	**KeyGen Time (s)**	**Enc/Sign Time (s)**	**Dec/Verify Time (s)**
Kyber-512	0.0039	0.00004	0.00005
Falcon-512	0.0182	0.00072	0.00009
RSA-2048	0.0981	0.0015	0.00004
ECDSA P-256	0.00011	0.00005	0.00009

6. Observations

🔐 Kyber-512 (KEM)

- Key generation and encapsulation are extremely fast.
- Ciphertext size is larger than classical schemes, but acceptable for modern bandwidth.
- Shared secret was successfully established and matched between Alice and Bob.

✍️ Falcon-512 (SIG)

- Key generation is slower than ECDSA but still practical.
- Signature verification is fast and reliable.
- Signature size is larger than classical ones, but manageable.

🏛️ Classical Algorithms

- RSA-2048 key generation is significantly slower.
- ECDSA P-256 is lightweight and fast but not quantum-safe.

---

7. Practicality Analysis

- **Kyber-512** is ideal for real-time key exchange due to its speed and moderate key sizes.
- **Falcon-512** offers strong security with efficient verification, suitable for systems with many verifiers.
- **RSA-2048** is outdated for quantum resistance due to slow key generation and small key sizes.
- **ECDSA P-256** is efficient but vulnerable to quantum attacks.

8. Hybrid Scheme Considerations

Combining PQC with classical algorithms (e.g., Kyber + RSA) allows gradual migration to quantum-safe systems while maintaining compatibility. Hybrid schemes:

- Provide layered security
- Allow legacy support
- Future-proof critical infrastructure

---

9. Conclusion

Post-Quantum algorithms like Kyber512 and Falcon-512 are practical for deployment in modern systems. They offer a strong balance of performance and security. Classical algorithms, while still in use, are not suitable for long-term quantum-safe applications. Hybrid approaches offer a smooth transition path.

📚 References

1. Open Quantum Safe Project
2. NIST Post-Quantum Cryptography Standardization
3. OpenSSL Documentation
4. liboqs GitHub Repository