Comparative Study of Post-Quantum and Classical Cryptography Algorithms

1. Introduction

The advent of quantum computing poses significant threats to classical cryptographic algorithms such as RSA and ECDSA, which rely on the hardness of integer factorization and discrete logarithms. Post-Quantum Cryptography (PQC) algorithms are designed to remain secure against quantum attacks, ensuring confidentiality and integrity in the quantum era.

This study compares selected PQC algorithms with classical counterparts in terms of key sizes, signature/ciphertext sizes, and execution times.

2. Algorithms Evaluated

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

3. Experimental Setup

Environment: Fedora XX, GCC 15.2.1, OpenSSL 3.2.4, liboqs XX.X
Timing Method: clock_gettime(CLOCK_MONOTONIC, &ts) for microsecond resolution

Measurement Steps:
Key generation
Encapsulation / Signing
Decapsulation / Verification
Message: "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

Observation:
"Kyber-512 has larger keys and ciphertexts than ECDSA P-256, but its key sizes are similar to RSA-2048, making it suitable for bandwidth-sensitive applications."

5. Execution Time Comparison

Algorithm	KeyGen Time (s)	Enc/Sign Time (s)	Dec/Verify Time (s)
Kyber-512	0.004028	0.000036	0.000046
Falcon-512	0.017866	0.000706	0.000093
RSA-2048	0.097788	0.001491	0.000038
ECDSA P-256	0.000108	0.000054	0.000093

Observation:

"Kyber-512 key generation is significantly faster than RSA-2048, and Falcon-512 provides efficient signing with slightly higher computational cost than ECDSA-P256."

6. Analysis of Practicality

Key Sizes: PQC keys (Kyber-512, Falcon-512) are larger than ECDSA-P256 keys but smaller or comparable to RSA-2048 keys in some cases.

Performance: Kyber-512 key generation is significantly faster than RSA-2048, and its encapsulation/decapsulation times are extremely low, making it practical for key exchange in real-time systems. Falcon-512 signing is reasonably fast, and signature verification is very efficient, comparable to ECDSA-P256 verification times.

Trade-offs:
Security vs. key size: PQC schemes use larger keys to resist quantum attacks; this increases bandwidth but ensures post-quantum security.

Signing vs. verification time: Some PQC signatures (e.g., Falcon-512) are larger than classical ones, but verification remains fast, which is advantageous in systems with many verifiers.

Overall, Kyber and Falcon demonstrate a good balance between security, key/signature sizes, and performance, making them practical for real-world deployment.

7. Hybrid Scheme Considerations

Combining PQC with classical crypto can provide quantum resistance without breaking legacy systems.

Example: TLS connection using RSA + Kyber ensures compatibility and future-proof security.

Benefits:
Mitigates quantum threats gradually.
Balances performance and security.

8. Conclusion

PQC algorithms like Kyber512 and Falcon-512 are practical for deployment in most scenarios.
Classical algorithms like RSA-2048 remain inefficient for high-security quantum-resistant applications.
Hybrid approaches provide a transitional solution for secure communication in the quantum era.

References

Open Quantum Safe, liboqs: https://openquantumsafe.org
NIST Post-Quantum Cryptography Standardization Project: https://csrc.nist.gov/projects/post-quantum-cryptography
OpenSSL Documentation: https://www.openssl.org/docs/