Comparative Study — Post-Quantum Cryptography (PQC) vs Classical Algorithms

1. Overview

Post-Quantum Cryptography (PQC) aims to secure communications against attacks from quantum computers, which can break classical algorithms like RSA and ECC. NIST has selected CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+, and Classic McEliece as finalists and standards for post-quantum use. These represent lattice-based, hash-based, and code-based approaches, each with unique trade-offs in key size, performance, and security.

2. Comparison of PQC vs Classical Algorithms

Algorithm	Public Key (bytes)	Private Key (bytes)	Signature/Ciphertext (bytes)	Relative CPU Cost
RSA-3072 (Classical)	≈ 392	≈ 1.6k	≈ 384	Moderate
ECDSA P-256 (Classical)	64	32	≈ 64–72	Very fast
CRYSTALS-Kyber-768 (KEM)	≈ 1184	≈ 2400	≈ 1088	Fast
Classic McEliece	≈ 261–524 KB	≈ 6–10 KB	≈ 128–256	Moderate
CRYSTALS-Dilithium	≈ 896–1312	≈ few KB	≈ 2–3 KB	Fast

3. Practical PQC Algorithms

Among standardized algorithms, Kyber (for key exchange) and Dilithium (for digital signatures) are considered the most practical for real-world deployment due to their efficient performance and moderate key sizes. FALCON provides smaller signatures but is more complex to implement securely. Classic McEliece offers excellent security but has very large public keys, which limits use in bandwidth-constrained environments.

4. Trade-offs: Security, Performance, and Key Sizes

PQC schemes increase resistance to quantum attacks but require larger keys and signatures. Lattice-based schemes like Kyber and Dilithium strike a balance — fast operations with manageable key sizes. Hash-based schemes like SPHINCS+ provide conservative security but have slow signature generation. Code-based systems such as McEliece use very large keys but are extremely secure and well-studied.

5. Hybrid Schemes (PQC + Classical)

Hybrid cryptographic schemes combine classical algorithms (like ECDH or RSA) with PQC (like Kyber) to ensure security even if one system fails. This dual approach eases the transition to post-quantum security while maintaining compatibility with existing infrastructure. Many organizations, including NIST and major browsers, are testing hybrid TLS protocols for secure communication in the post-quantum era.

6. Conclusion

PQC is essential for securing the future of digital communication. Kyber and Dilithium are leading candidates for practical use due to their balance of speed, key size, and implementation simplicity. Hybrid approaches offer a transitional path toward full quantum-safe security, combining the

strengths of both classical and PQC methods.