INTRODUCTION TO CRYPTOGRAPHY

CLASSICAL CRYPTOGRAPHY vs POST QUANTUM CRYPTOGRAPHY

Comparison of key/signature sizes with RSA-2048 or ECDSA P-256 with PQC (using OpenSSL or Crypto++).

Algorithm	**RSA-2048**	**ECDSA P-256**	**ML-DSA-44**	**ML-KEM-512**
Type	Signature	Signature	Signature	KEM/Encryption
Public Key Size	451 bytes(PEM encode)	65 bytes	1312 bytes	800 bytes
Private Key Size	1704 bytes	121 bytes	2560 bytes	1632 bytes
Signature Size	256 bytes	70 bytes	2420 bytes	768 bytes(ciphertext)

Observations :

i) RSA-2048 has a signature size of 256 bytes, which is smaller than ML-DSA-44’s 2420 bytes, but RSA’s key generation and signing are much slower.
ii) ECDSA P-256 offers very small key and signature sizes, but it is not secure against quantum computers.
iii) ML-DSA-44 provides quantum-resistant security at the cost of much larger key and signature sizes.
iv) ML-KEM-512, on the other hand, shows smaller public key and ciphertext sizes compared to RSA-2048,
while also being quantum-secure, making it practical for secure key exchange in real deployments.

The comparison shows a clear trade-off between size and security:
-> Classical algorithms (RSA, ECDSA) → smaller keys and signatures, but quantum-vulnerable.
-> PQC algorithms (ML-DSA, ML-KEM) → significantly larger key sizes, but quantum-safe and still practical with modern bandwidth and storage.

In real-world systems, hybrid approaches (for example, combining ML-KEM-512 with ECDH or RSA) can be adopted during the transition period, ensuring compatibility with current systems while providing post-quantum protection.

Comparative Study

INTRODUCTION :

With the rapid development of quantum computing, traditional cryptographic systems such as RSA and ECDSA are expected to become insecure. Post-Quantum Cryptography (PQC) aims to provide encryption and digital signature algorithms that remain secure even against quantum attacks.

This task performs a comparative study between classical algorithms (RSA-2048 and ECDSA P-256) and post-quantum algorithms (ML-KEM-512 and ML-DSA-44).
The comparison focuses on:

-> Key Sizes
-> Signature or Ciphertext sizes
-> Execution Times

*Key and Signature/Ciphertext Sizes

Algorithm	**RSA-2048**	**ECDSA P-256**	**ML-DSA-44**	**ML-KEM-512**
Type	Signature	Signature	Signature	KEM/Encryption
Public Key Size	451 bytes	65 bytes	1312 bytes	800 bytes
Private Key Size	1704 bytes	121 bytes	2560 bytes	1632 bytes
Signature Size	256 bytes	70 bytes	2420 bytes	768 bytes(ciphertext)

Analysis :
-> Classical algorithms (RSA, ECDSA) have much smaller key and signature sizes.
-> Post-quantum algorithms (ML-KEM, ML-DSA) have significantly larger keys and signatures, but they provide quantum resistance.
-> ML-KEM-512 uses smaller keys and ciphertexts compared to RSA-2048, making it more efficient for secure key exchange.

* Execution Time Comparision :

Algorithm	Operation	Execution Time (µs)
RSA-2048	Key Generation	12000
	Signing	700
	Verification	60
ECDSA P-256	Key Generation	900
	Signing	350
	Verification	190
ML-DSA-44	Key Generation	9280
	Signing	88
	Verification	(Valid = Yes)
ML-KEM-512	Key Generation	7627
	Encapsulation	41

	Decapsulation	16

Analysis :

-> RSA-2048 shows the slowest key generation (≈ 12 ms) because it needs to compute large primes.
-> ECDSA P-256 is much faster in signing and verifying, but it’s vulnerable to quantum attacks.
-> ML-KEM-512 achieves very fast encryption/decryption (41 µs / 16 µs), making it efficient for key exchange.
-> ML-DSA-44 produces keys slower than ECDSA but signs in only 88 µs, which is impressively fast for a PQC signature scheme.
-> Overall, PQC algorithms (ML-KEM and ML-DSA) provide quantum-safe security with execution times comparable to or faster than RSA-2048.

Which PQC algorithm seems practical for real-world deployment.

Based on the observed results, ML-KEM-512 (Kyber-512) emerges as the most practical PQC algorithm for real-world deployment.
It offers :
-> Reasonable key sizes (800-byte public, 768-byte ciphertext)
-> Fast performance (encapsulation in 41 µs and decapsulation in 16 µs)
-> Strong post-quantum security (NIST Level 1)

It has already been standardized by NIST in 2024 (FIPS 203) and is being adopted in major protocols like TLS 1.3 and VPN systems for key exchange.

For digital signatures, ML-DSA-44 (Dilithium-2) is also practical, providing high security (NIST Level 2) and efficient signing times (≈ 88 µs).
While its signature size (2420 bytes) is larger than ECDSA’s 70 bytes, it remains manageable in modern networks and storage systems.

Thus, both ML-KEM-512 (for encryption) and ML-DSA-44 (for authentication) are well-suited for deployment in post-quantum environments.

Trade-offs between security, performance, and key sizes.

Aspect	Classical (RSA/ECDSA)	Post-Quantum (ML-KEM / ML-DSA)
Security	Secure against classical attacks but weak to quantum	Secure against both classical and quantum attacks
Performance	Generally faster for small data	Comparable; slower keygen but faster sign/verify
Key Size	Compact	5 to 10times larger
Implementation Cost	Mature libraries and hardware support	Requires new PQC libraries and integration
Longevity	Short-term secure	Long-term secure

* The Importance of Hybrid (PQC + Classical) Schemes

Hybrid cryptography combines classical and PQC algorithms—for example, ECDH + ML-KEM-512 for key exchange or RSA + ML-DSA-44 for signatures.

These systems provide :

1. **Backward compatibility:** Existing systems continue to function using classical algorithms.

2. **Forward security:** Even if classical encryption is broken in the future, PQC ensures ongoing data protection.

3. **Smooth migration path:** Organizations can adopt PQC gradually without system disruption.

Major companies such as Google and Cloudflare are already testing hybrid key exchange mechanisms in TLS and VPN infrastructures to ensure post-quantum readiness.

Conclusion :

This comparative study highlights the transition from classical to post-quantum cryptography.
Classical algorithms like RSA and ECDSA, while efficient, will become obsolete once quantum computers reach sufficient power.
In contrast, ML-KEM-512 and ML-DSA-44 provide robust quantum-safe security and practical performance.
Among these, ML-KEM-512 is particularly suitable for real-world deployment due to its efficiency and moderate key sizes.
ML-DSA-44, although larger in signature size, remains an excellent option for digital signatures in quantum-safe applications.

The future of cryptography lies in hybrid systems that combine the reliability of classical algorithms with the resilience of PQC, ensuring a seamless transition to quantum-secure infrastructure.
As standardization efforts by NIST and the Open Quantum Safe Project continue, organizations are encouraged to begin testing PQC algorithms to future-proof their systems.