Post-Quantum Cryptography

Cryptographic schemes that can defeat quantum computers

- ➡ Still in research (started around 2006)
- ➡ On August 2024, the NIST released final versions of the first three Post Quantum Crypto Standards
- ➡ On November 2024, the NIST has announced prohibiting classical cryptography (RSA, DSA, ECDSA, ECDH) after 2035

	ML-KEM (Module-Lattice Key Encapsulation)	**ML-DSA** (Module-Lattice Digital Signature)	**SLH-DSA** (Stateless Hash-Based Signature)
Standard	FIPS-203	FIPS-204	FIPS-205
Purpose	**Key Exchange** to generate a 256-bits shared key	**Digital Signature Scheme** that offers a good balance of performance relative to signature sizes	**Digital Signature Scheme** designed as a fallback / conservative option with smaller public keys but large signatures and slower performances
Description	Exists in three versions ML-KEM-512 ML-KEM-768 ML-KEM-1024	Exists in three versions ML-DSA-44 ML-DSA-65 ML-DSA-87	Exists in 12 variants as combinations of different key sizes (128, 192, 256), different hash (Sha2, Shake) and different algorithm trade-off (small vs fast)
Algorithm and Mathematical Foundation	Module Learning With Errors (MLWE) based on a lattice approach	CRYSTALS-Dilithium based on lattice signature	SPHINCS+ a purely hash-based signature scheme, does not rely on a lattice approach