

	<b>ML-KEM</b> (Module-Lattice Key Encapsulation)	<b>ML-DSA</b> (Module-Lattice Digital Signature)	<b>SLH-DSA</b> (Stateless Hash-Based Signature)
Standard	FIPS-203	FIPS-204	FIPS-205
Purpose	<b>Key Exchange</b> to generate a 256-bits shared key	<b>Digital Signature Scheme</b> that offers a good balance of performance relative to signature sizes	<b>Digital Signature Scheme</b> 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

# Quantum Cryptography