



# MLS cipher suites using ML-KEM

## draft-ietf-mls-pq-ciphersuites

---

Rohan Mahy and Richard Barnes

# Current Cipher Suites: Ready for WGLC?

Level	KEM	AEAD	Hash	Sig	KEM/Sig
128	ML-KEM-768+X25519	<i>AES128</i>	<i>SHA256</i>	Ed25519	hybrid/T
128	ML-KEM-768+X25519	AES256	SHA384	Ed25519	hybrid/T
128	ML-KEM-768+P256	<i>AES128</i>	<i>SHA256</i>	P-256	hybrid/T
128	ML-KEM-768+P256	AES256	SHA384	P-256	hybrid/T
192	ML-KEM-1024-P384	AES256	SHA384	P-384	hybrid/T
128	ML-KEM-768	AES256	SHA384	P-256	PQ/T
192	ML-KEM-1024	AES256	SHA384	P-384	PQ/T
192	ML-KEM-768	AES256	SHA384	ML-DSA-65	PQ/PQ
256	ML-KEM-1024	AES256	<i>SHA384</i>	ML-DSA-87	PQ/PQ

1. At “128-bit security level” some wanted AES128/SHA256; others wanted AES256/SHA384. Do **Both**.

2. Nobody wanted SHA512 even for ML-KEM-1024 / ML-DSA-87.

3. One typo fixed in Editor’s copy

All cipher suites use SHAKE256 for KDF