

a Classical security estimates

b NIST categories

RSA-2048

112 bits

ML-KEM-512 /
ML-DSA-44

Category 1

RSA-3072

128 bits

ML-KEM-768 /
ML-DSA-65

Category 3

ECDH/ECDSA P-256

128 bits

ML-KEM-1024 /
ML-DSA-87

Category 5

Falcon-512 /
FN-DSA

Category 1

X25519/Ed25519

128 bits

Classic McEliece
348864

Category 1