C: r5n15kem0d
C: r5nd3kem0d
C: ledakemcpa53
C: bikel3
C: r5nd3kem5d
C: ledakemcpa33
T: hqc2561
C: r5nd1kem5d
C: bikel1
•
C: r5n13kem0d
C: r5nd1kem4longkey
C: ledakemcpa52
C: r5n11kem0d
C: r5nd1kem0d
•
C: r5nd5kem5d
C: ledakemcpa14
C: r5nd0kem2iot
C: ledakemcpa12
C: lake3
C: rolloi256
C: lake1
C: ledakemcpa34
C: lake2
C: hila5
C: ledakemcpa32
C: rolloi128
C: ledakemcpa54
C: ledakemcpa13
C: r5nd5kem0d

md64, saaba, crypto_kem, enc time, ciphertext size, except for NIST Post-Quantum Cryptography Standardization Project
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).
• means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. • means that the SUPERCOP database does not list constant time as a goal for this implementation.
https://bench.cr.yp.to
20221020