C: r5n15kem0d
C: ledakemc5pa52
C: lake2
C: r5nd0kem2iot
T: )sntrup653
C: ledakemc5pa53
C: hila5
T: )ntruhps2048677
C: ledakemc5pa32
•
C: ledakemc5pa12
C: bikel3
C: bikel1
C: r5nd3kem5d
C: r5nd1kem0d
C: ledakemc5pa33
C: r5nd3kem0d
T: )ntruhps2048509
C: 3bears936r2cpa,
C: ledakemc5pa34
C: r5nd5kem5d
•
C: ledakemc5pa14
•
C: lake1
T: )sntrup953
C: r5n13kem0d
C: 3bears1248r2cpa,
C: 3bears624r2cpa,
T: )sntrup1277
T: )ntruhps4096821
C: r5nd1kem5d
•
T: )sntrup857
C: r5nd1kem4longkey
C: ledakemc5pa13

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).
Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

• 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.