C: ledakem54sl
C: r5nd3kem0d
C: r5nd5kem0d
C: bikel3
C: lake1
C: lake2
T: ledakem14sl
C: rolloi256
C: r5nd3kem5d
C: ledakemcpa54
C: lake3
C: r5n11kem0d
C: ledakemcpa13
C: ledakemcpa32
C: ledakemcpa14
C: rolloi128
• C: r5nd0kem2iot
C: ledakemcpa12
C: r5nd1kem4longkey
C: r5n13kem0d
C: hila5
C: r5nd5kem5d
C: ledakemcpa53
C: ledakemcpa33
C: rolloi192
C: ledakemcpa34
•
C: r5n15kem0d

2

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

C: 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.