C: r5n15kem0d
C: ledakemcpa13
C: rolloi128
C: bikel3
C: r5nd1kem5d
C: ledakemcpa12
C: hila5
C: ledakemcpa54
C: nhcompact1024cca
•
C: r5n13kem0d
T: •
C: lake2
C: lake3
C: rolloi192
C: r5nd1kem0d
C: nhcompact512cca
C: ledakemcpa34
C: ledakemcpa33
C: ledakemcpa14
C: 3bears1248r2cpa,
C: nhcompact768cca
C: r5nd1kem4longkey
C: bikel1
C: r5nd3kem0d
C: ledakem32sl

20220213

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.

https://bench.cr.yp.to