C: r5n15kem0d
C: rolloi192
C: lake2
C: r5nd1kem4longkey
C: ledakemcpa54
C: ledakemcpa32
C: ledakemcpa34
C: ledakemcpa52
C: lake1

C: bikel1
C: r5n13kem0d
C: r5nd1kem0d
C: ledakemcpa12
C: ledakemcpa53
C: r5nd0kem2iot
C: bikel3
C: ledakemcpa14
C: rolloi256
C: r5n11kem0d
C: r5nd3kem5d

2

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES)
Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc).

\(\text{C:"} \) means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. \(\text{\textbullet} \) means that the SUPERCOP database does not list constant time as a goal for this implementation.