C: r5n15kem0d
C: ledakemcpa32
C: r5nd0kem2iot
C: r5nd3kem5d
C: hila5
T: sikep503
C: ledakemcpa12
T: locker9
C: bikel3
C: bikel1
•
C: r5n13kem0d
C: lake2
•
C: lake3
C: ledakemcpa54
C: r5nd1kem4longkey
C: ledakemcpa53
C: ledakemcpa13
C: r5nd1kem5d
C: ledakemcpa34
C: r5nd5kem0d
C: r5n11kem0d
C: r5nd1kem0d
C: r5nd3kem0d
C: ledakemcpa52
Vertical axis: Space (bytes) for a ciphertext (cipher_kem_CIPHERTEXTBYTES)
Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc)

"C:" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. "T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.