C: r5n15kem0d
C: ledakemcpa53
C: r5nd3kem0d
C: ledakemcpa34
C: rolloi256
C: ledakemcpa52
C: ledakemcpa14
C: r5nd5kem5d
C: lake3
C: ledakemcpa54
C: rolloi128
C: r5nd1kem4longkey
C: r5nd0kem2iot
C: rolloi192
C: r5n11kem0d
C: bikel3
C: r5nd1kem5d
C: r5n13kem0d
C: hila5
C: ledakemcpa33
C: r5nd1kem0d
C: r5nd3kem5d
T: sikep503
C: lake1
C: lake2
C: bikel1
C: ledakemcpa32

20221020

https://bench.cr.yp.to

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.

Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair).
Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

md64, bolero, crypto_kem, keypair time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project