amd64, hydra7, crypto_kem, dec time, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project

Horizontal axis: Time (cycles) to generate a session key given a ciphertext (`crypto_kem_dec`).

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. "`T:`" means that the SUPERCOP database does not list constant time as a goal for this implementation.

Label
T: hqc1922
T: frodokem1344aes
T: frodokem640aes
ntrulpr953
T: frodokem640
T: frodokem640shake
sntrup953
ntrulpr1013
ntrulpr1013
T: hqc2563
T: frodokem976shake
T: ntrulpr857
sntrup953
sntrup1013
T: hqc2562
ntrulpr761
kyber90s1024
sntrup1013
T: hqc1281
T: frodokem976aes
T: hqc2561
T: rqc256
T: newhope1024cca
T: sntrup1013
T: hqc1921
T: frodokem976
T: rqc192
T: ntrulpr761
ntrulpr857
T: ntrulpr1277
T: rolloii192
T: locker9
kyber1024
ntruhrss701
T: lac256
T: locker8
T: C: bikel3
T: C: hila5
T: rqc128
C: 3bears1248r2cpa
T: rolloii256
T: locker7
sntrup761
T: rolloii128
T: locker6
kyber90s768
C: 3bears936r2cpa
ntrulpr1277
T: C: bikel1
T: ntrulpr653
3bears1248r2cca
T: ntrulpr4591761
T: newhope512cca
sntrup1277
T: locker5
kyber768
T: locker3
T: sikep610
T: sntrup4591761
C: 3bears624r2cpa
T: lac192
T: locker2
T: lac128
ntrulpr953
T: locker4
T: sikep751
kyber512
ntruhps4096821
T: locker1
T: ntrukem443
T: sikep503comp
kyber90s512
ntrulpr653
3bears936r2cca
T: C: lake3
T: ntrukem743
sntrup761
sntrup857
T: C: rolloi256
sntrup1277
ntruhps2048509
3bears624r2cca
T: sikep751comp
sntrup653
ntruhps2048677
T: ntruhps4096821
T: C: rolloi192
T: sikep434
T: sntrup653
T: ntruhps2048677
T: C: lake2
T: ntskem13136
T: C: rolloi128
T: C: lake1
T: sikep503
T: sikep610comp
T: ntruhps2048509
T: sntrup857
T: ntskem1264
T: ntskem1380
T: sikep434comp