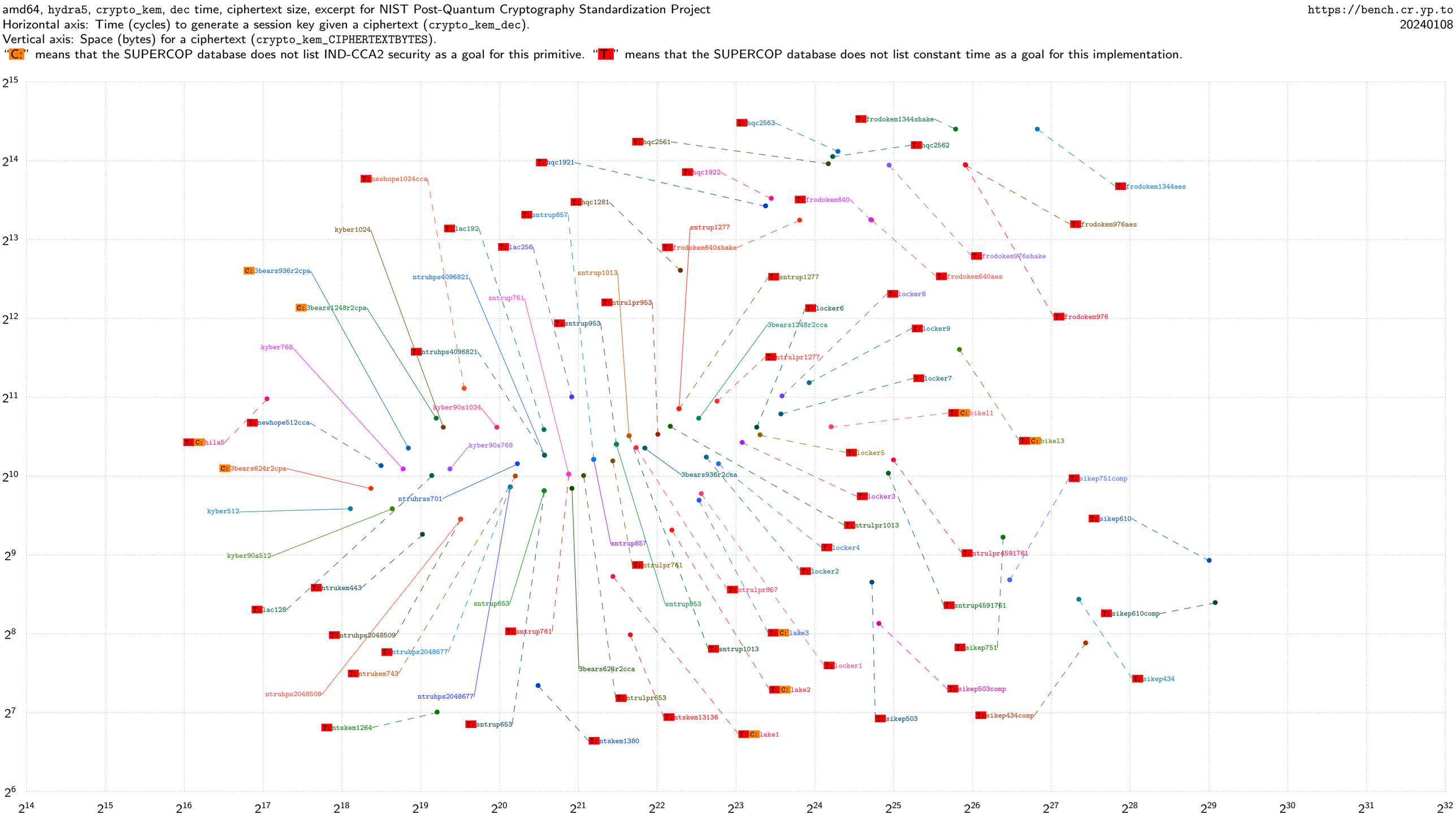
amd64, hydra5, crypto_kem, dec time, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project
https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec).
20240108
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).
"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.
2^15
2^14
2^13
2^12
2^11
2^10
2^9
2^8
2^7
2^6
2^14
2^15
2^16
2^17
2^18
2^19
2^20
2^21
2^22
2^23
2^24
2^25
2^26
2^27
2^28
2^29
2^30
2^31
2^32
T:hqc2563
T:frodokem1344shake
T:hqc2561
T:hqc2562
T:hqc1921
T:hqc1922
T:frodokem1344aes
T:newhope1024cca
T:frodokem640
T:hqc1281
T:sntrup857
T:frodokem976aes
kyber1024
T:lac192
sntrup1277
T:lac256
T:frodokem640shake
T:frodokem976shake
C:3bears936r2cpa
ntruhps4096821
sntrup1013
T:sntrup1277
T:frodokem640aes
sntrup761
T:ntrulpr953
T:locker8
C:3bears1248r2cpa
T:locker6
T:sntrup953
T:frodokem976
3bears1248r2cca
T:locker9
kyber768
T:ntruhps4096821
T:ntrulpr1277
T:locker7
kyber90s1024
T:C:bike1
T:newhope512cca
T:C:hila5
T:C:bike3
kyber90s768
T:locker5
C:3bears624r2cpa
3bears936r2cca
T:sikep751comp
T:locker3
ntruhrss701
T:ntrulpr1013
T:sikep610
kyber512
T:locker4
kyber90s512
T:ntrulpr4591761
T:ntrulpr761
T:locker2
T:ntrulpr857
T:ntrukem443
T:sntrup4591761
T:lac128
sntrup653
sntrup953
T:sikep610comp
T:ntruhps2048509
T:C:lake3
T:sntrup761
T:sikep751
T:ntruhps2048677
T:sntrup1013
T:locker1
T:sikep434
3bears624r2cca
T:ntrukem743
T:sikep503comp
T:C:lake2
ntruhps2048509
ntruhps2048677
T:ntrulpr653
T:sikep434comp
T:ntskem13136
T:sikep503
T:ntskem1264
T:sntrup653
T:C:lake1
T:ntskem1380