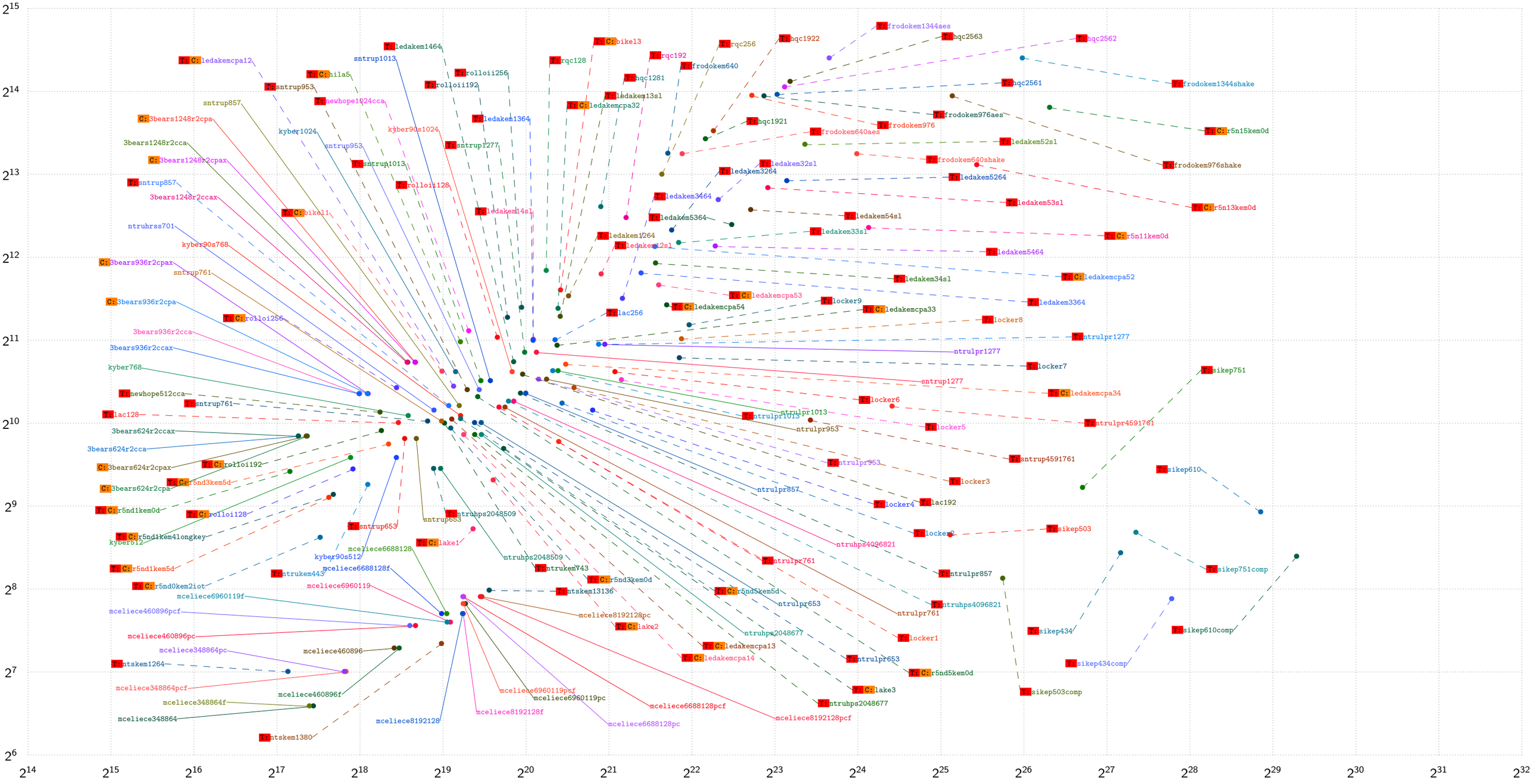
amd64, wooden, crypto_kem, enc time, ciphertext size, excerpt for NIST Post-Quantum Cryptography Standardization Project https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc). 20240127
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).
"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: frodokem1344aes
T: hqc1922
T: hqc2563
T: hqc2562
T: C: bike13
T: rqc256
T: rqc192
T: frodokem640
T: rqc128
T: hqc1281
T: ledakem13s1
T: C: ledakemcpa32
T: hqc1921
T: frodokem640aes
T: frodokem976
T: frodokem976aes
T: hqc2561
T: frodokem1344shake
T: C: r5n15kem0d
T: ledakem52s1
T: frodokem640shake
T: frodokem976shake
T: ledakem32s1
T: ledakem3264
T: ledakem5264
T: ledakem53s1
T: C: r5n13kem0d
T: ledakem3464
T: ledakem5364
T: ledakem54s1
T: ledakem33s1
T: C: r5n11kem0d
T: ledakem1264
T: ledakem12s1
T: ledakem5464
T: C: ledakemcpa52
T: ledakem34s1
T: ledakem3364
T: C: ledakemcpa53
T: C: ledakemcpa54
T: locker9
T: C: ledakemcpa33
T: lac256
T: locker8
T: ntrulpr1277
ntrulpr1277
T: locker7
T: sikep751
sntrup1277
T: C: ledakemcpa34
T: locker6
ntrulpr1013
T: ntrulpr1013
ntrulpr953
T: locker5
T: ntrulpr4591761
T: sntrup4591761
T: ntrulpr953
T: locker3
T: sikep610
ntrulpr857
T: locker4
T: lac192
T: locker2
T: sikep503
ntruhps4096821
T: ntrulpr761
T: ntrulpr857
T: sikep751comp
T: ntruhps4096821
ntrulpr761
ntrulpr653
ntruhps2048677
T: locker1
T: sikep434
T: sikep610comp
T: C: ledakemcpa13
T: C: ledakemcpa14
T: ntrulpr653
T: sikep434comp
T: C: r5nd5kem0d
T: C: lake3
T: sikep503comp
T: ntruhps2048677
mceliece6688128pcf
mceliece8192128pcf
mceliece6960119pcf
mceliece6960119pc
mceliece8192128f
mceliece6688128pc
mceliece8192128
T: ntskem1380
mceliece348864
mceliece348864f
mceliece460896f
mceliece348864pcf
T: ntskem1264
mceliece348864pc
mceliece460896
mceliece460896pc
mceliece460896pcf
mceliece6960119f
mceliece6960119
T: C: r5nd0kem2iot
T: ntrukem443
mceliece6688128f
kyber90s512
mceliece6688128
T: C: r5nd1kem5d
kyber512
T: C: r5nd1kem4longkey
T: C: r5nd1kem0d
T: C: rollOi128
T: C: r5nd3kem5d
C: 3bears624r2cpa
T: C: rollOi192
C: 3bears624r2cpax
3bears624r2cca
3bears624r2ccax
T: lac128
T: sntrup761
T: newhope512cca
kyber768
3bears936r2ccax
3bears936r2cca
T: C: rollOi256
C: 3bears936r2cpa
sntrup761
C: 3bears936r2cpax
ntruhrss701
kyber90s768
T: C: bike11
3bears1248r2ccax
T: sntrup857
C: 3bears1248r2cpax
3bears1248r2cca
C: 3bears1248r2cpa
sntrup857
T: newhope1024cca
T: sntrup953
T: C: hila5
sntrup1013
T: ledakem1464
T: C: ledakemcpa12
T: rollOii128
T: sntrup1013
T: sntrup1277
sntrup953
kyber1024
T: ledakem1364
T: rollOii192
T: rollOii256
kyber90s1024
T: ntruhps2048509
sntrup653
T: sntrup653
T: C: lake1
ntruhps2048509
T: ntrukem743
T: C: r5nd3kem0d
T: ntskem13136
T: C: r5nd5kem5d
mceliece8192128pc
T: C: lake2
T: C: lake4
T: ledakem14s1
T: ledakem1364
T: ledakem3464
T: ledakem5364
T: ledakem1264
T: ledakem12s1
T: ledakem3264
T: ledakem32s1
T: ledakem5264
T: ledakem53s1
T: ledakem54s1
T: ledakem33s1
T: ledakem5464
T: ledakem34s1
T: ledakem3364
T: locker9
T: locker8
T: locker7
T: locker6
T: locker5
T: locker3
T: locker4
T: locker2
T: locker1
T: sikep751
T: C: ledakemcpa34
T: ntrulpr4591761
T: sntrup4591761
T: sikep610
T: sikep503
T: sikep751comp
T: sikep434
T: sikep610comp
T: sikep434comp
T: sikep503comp
T: C: r5nd5kem0d
T: C: lake3
T: ntruhps2048677
T: ntrulpr653
T: C: ledakemcpa13
T: C: ledakemcpa14
T: ntruhps4096821
T: ntrulpr761
T: ntrulpr857
T: C: r5nd5kem5d
T: ntskem13136
T: ntrukem743
T: C: r5nd3kem0d
T: ntruhps2048509
T: C: lake1
T: sntrup653
sntrup653
T: C: rollOi128
T: C: r5nd1kem0d
T: C: r5nd1kem4longkey
T: C: r5nd1kem5d
T: C: r5nd3kem5d
C: 3bears624r2cpa
C: 3bears624r2cpax
T: C: rollOi192