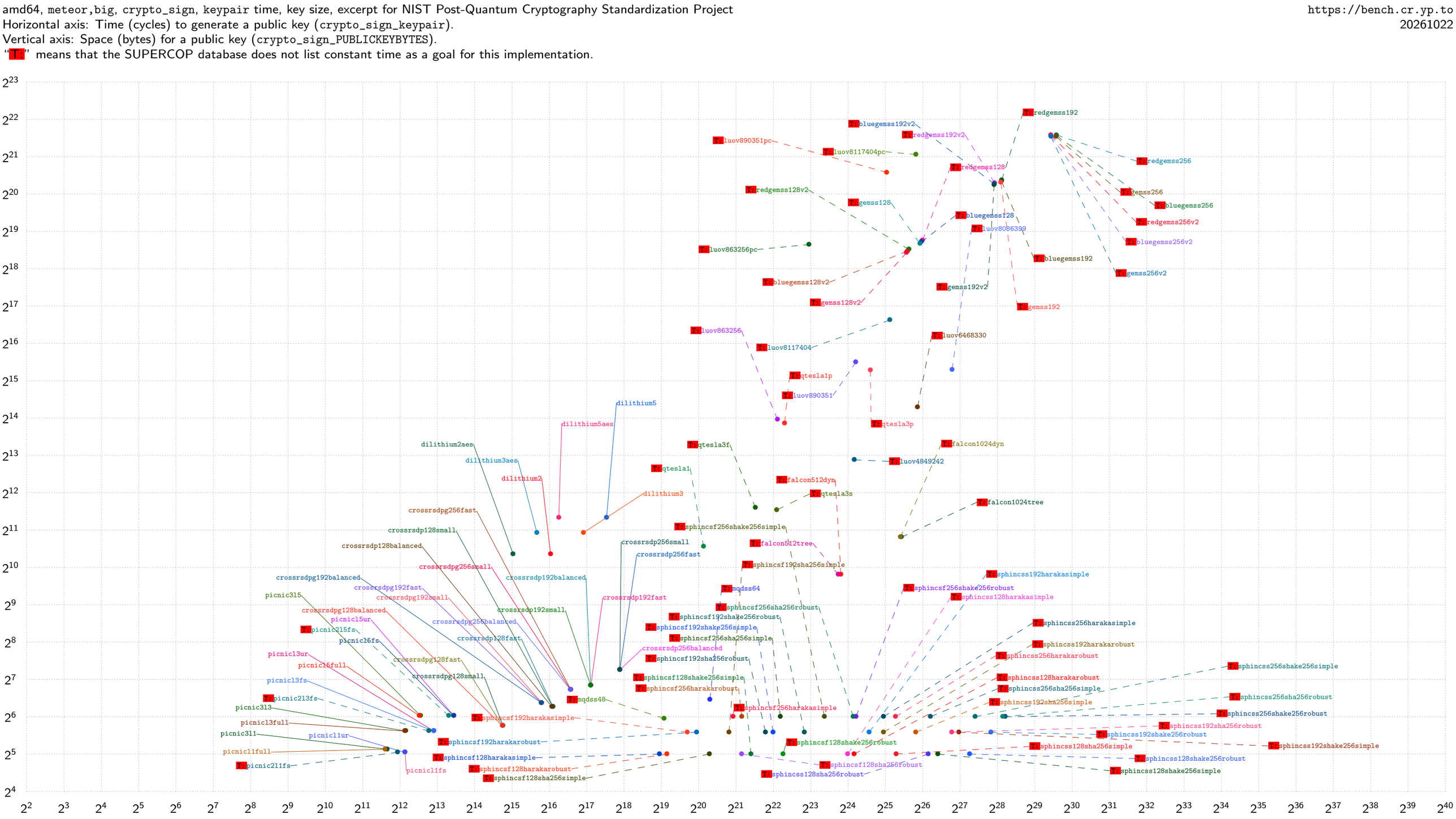

amd64, meteor,big, crypto_sign, keypair time, key size, excerpt for NIST Post-Quantum Cryptography Standardization Project
https://bench.cr.yp.to
20261022
Horizontal axis: Time (cycles) to generate a public key (crypto_sign_keypair).
Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).
"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.
T:redgemss192
T:bluegemss192v2
T:redgemss192v2
T:luov890351pc
T:luov8117404pc
T:redgemss256
T:redgemes128
T:redgemss128v2
T:gemss128
T:gemss256
T:bluegemss256
T:bluegemss128
T:redgemss256v2
T:luov8086399
T:luov863256pc
T:bluegemss256v2
T:bluegemss192
T:bluegemss128v2
T:gemss256v2
T:gemss192v2
T:gemss128v2
T:gemss192
T:luov863256
T:luov6468330
T:luov8117404
T:qtesla1p
T:luov890351
T:qtesla3p
dilithium5
dilithium5aes
dilithium2aes
T:qtesla3f
T:falcon1024dyn
dilithium3aes
T:luov4849242
T:qtesla1
dilithium2
T:falcon512dyn
dilithium3
T:qtesla3s
T:falcon1024tree
crossrsdpg256fast
T:sphincsf256shake256simple
crossrsdp128small
crossrsdp256small
T:falcon512tree
crossrsdp128balanced
crossrsdp256fast
T:sphincsf192sha256simple
crossrsdpg256small
crossrsdp192balanced
T:sphincss192harakasimple
crossrsdpg192balanced
crossrsdpg192fast
T:mqdss64
T:sphincsf256shake256robust
picnic315
crossrsdp192small
T:sphincss128harakasimple
crossrsdp192fast
T:sphincsf256sha256robust
crossrsdpg128balanced
crossrsdp192small
T:sphincsf192shake256robust
picnicl5ur
T:sphincss256harakasimple
crossrsdpg256balanced
T:picnic215fs
T:sphincsf192shake256simple
T:sphincsf256sha256simple
picnicl6fs
crossrsdp128fast
T:sphincss192harakarobust
crossrsdp256balanced
picnicl3ur
T:sphincsf192sha256robust
T:sphincss256harakarobust
picnicl5full
crossrsdpg128fast
T:sphincss256shake256simple
T:sphincsf128shake256simple
crossrsdpg128small
picnicl3fs
T:sphincsf256harakarobust
T:sphincss128harakarobust
T:picnic213fs
T:sphincss256sha256simple
T:sphincss256sha256robust
T:sphincsf256harakasimple
picnic313
T:sphincss192sha256simple
T:sphincss256shake256robust
T:mqdss48
T:sphincsf192harakasimple
picnicl3full
T:sphincss192sha256robust
T:sphincss192shake256robust
picnic311
picnicl1ur
T:sphincsf192harakarobust
T:sphincsf128shake256robust
T:sphincss192shake256simple
picnicl1full
T:sphincsf128sha256simple
T:sphincss128shake256robust
T:sphincsf128harakasimple
T:picnic211fs
T:sphincsf128sha256robust
picnicl1fs
T:sphincsf128harakarobust
T:sphincss128shake256simple
T:sphincsf128sha256simple
T:sphincss128sha256robust