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: gemss256
• T: bluegemss256
• T: bluegemss256v2
• T: redgemss256v2
• T: redgemss256
• T: gemss256v2
• T: gemss192
• T: bluegemss192
• T: redgemss192
• T: bluegemss192v2
• T: gemss192v2
• T: redgemss192v2
• T: gemss128
• T: bluegemss128
• T: redgemss128
• T: bluegemss128v2
• T: redgemss128v2
• T: gemss128v2
• T: luov8117404
• T: luov8086399
• T: luov890351
• T: qtesla3p
• T: luov6468330
• T: luov863256
• T: luov4849242
• T: falcon1024dyn
• T: falcon512tree
• T: qtesla1p
• T: sphincss256harakarobust
• T: sphincss256shake256robust
• T: sphincss256harakasimple
• T: sphincss256shake256simple
• T: sphincss192harakarobust
• T: sphincss192shake256robust
• T: sphincss192harakasimple
• T: sphincss192shake256simple
• T: sphincss128harakarobust
• T: sphincss128shake256robust
• T: sphincss128harakasimple
• T: sphincss128shake256simple
• T: sphincsf256harakarobust
• T: sphincsf256shake256robust
• T: sphincsf256harakasimple
• T: sphincsf256shake256simple
• T: sphincsf192harakarobust
• T: sphincsf192shake256robust
• T: sphincsf192harakasimple
• T: sphincsf192shake256simple
• T: sphincsf128harakarobust
• T: sphincsf128shake256robust
• T: sphincsf128harakasimple
• T: sphincsf128shake256simple
• T: dilithium5aes
• T: dilithium3aes
• T: dilithium5
• T: dilithium3
• T: dilithium2aes
• T: dilithium2
• T: mqdss64
• T: mqdss48
• T: picnicl5ur
• T: picnicl5fs
• T: picnic2l5fs
• T: picnicl3fs
• T: picnicl3ur
• T: picnic3l5
• T: picnicl5full
• T: picnic2l1fs
• T: picnicl1ur
• T: picnicl1fs
• T: picnic3l3
• T: picnicl1full
• T: picnic3l1