amd64, dali, crypto_sign, open time, signature size

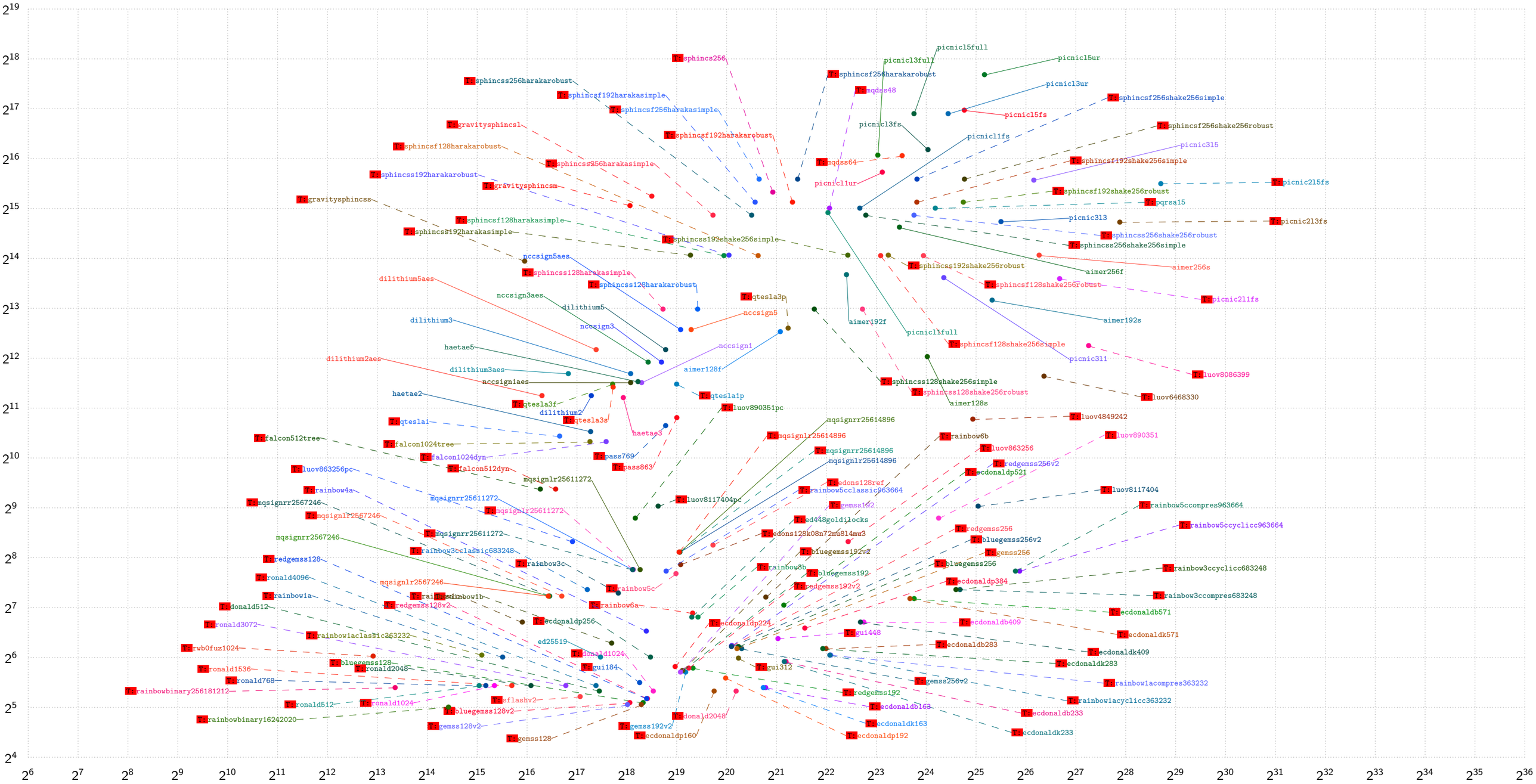
https://bench.cr.yp.to

20240912

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open).

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

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


T:sphincs256
T:sphincs256harakarobust
T:sphincsf192harakasimple
T:sphincsf256harakasimple
T:gravitysphincsl
T:sphincsf192harakarobust
T:sphincsf128harakarobust
T:sphincss256harakasimple
T:sphincss192harakarobust
T:gravitysphincsm
T:gravitysphincss
T:sphincsf128harakasimple
T:sphincss192harakasimple
T:sphincss192shake256simple
T:sphincsf256harakarobust
T:mqdss48
picnicl3full
picnicl5full
picnicl5ur
picnicl3ur
T:sphincsf256shake256simple
picnicl5fs
picnicl3fs
picnicl1fs
T:sphincsf256shake256robust
picnic315
T:sphincsf192shake256simple
T:mqdss64
picnicl1ur
T:picnic215fs
T:sphincsf192shake256robust
T:pqrsa15
picnic313
T:picnic213fs
T:sphincss256shake256robust
T:sphincss256shake256simple
T:sphincss192shake256robust
aimer256f
aimer256s
T:sphincsf128shake256robust
T:picnic211fs
aimer192s
aimer192f
picnicl1full
T:sphincsf128shake256simple
picnic311
T:luov8086399
T:luov6468330
T:sphincss128shake256simple
T:sphincss128shake256robust
aimer128s
T:luov4849242
T:luov890351
T:rainbow6b
T:luov863256
T:redgemss256v2
T:ecdonaldp521
T:luov8117404
T:rainbow5ccompres963664
T:rainbow5ccyclicc963664
T:redgemss256
T:bluegemss256v2
T:gemss256
T:bluegemss256
T:ecdonaldp384
T:rainbow3ccyclicc683248
T:rainbow3ccompres683248
T:ecdonaldb571
T:ecdonaldb409
T:ecdonaldk571
T:ecdonaldk409
T:ecdonaldb283
T:ecdonaldk283
T:rainbow1acompres363232
T:rainbow1acyclicc363232
T:ecdonaldb233
T:ecdonaldk233
T:ecdonaldp192
T:ecdonaldp163
T:ecdonaldk163
T:redgemss192
T:gemss256v2
T:gui312
T:gui448
T:ecdonaldp224
T:ed448goldilocks
T:edons128ref
T:rainbow5cclassic963664
T:gemss192
T:luov8117404pc
T:edons128k08n72mu814mu3
T:bluegemss192v2
T:rainbow3b
T:bluegemss192
T:redgemss192v2
T:mqsignrr25614896
T:mqsignlr25614896
mqsignrr25614896
mqsignlr25614896
T:rainbow5c
T:rainbow6a
T:ecdonaldp256
T:donald2048
T:ecdonaldp160
T:gemss192v2
T:gemss128
T:gemss128v2
T:bluegemss128v2
T:sflashv2
T:donald1024
T:gui184
T:ecdonaldp521
T:qtesla3p
nccsign5
nccsign1
aimer128f
T:qtesla1p
T:luov890351pc
haetae3
T:qtesla3s
T:qtesla3f
dilithium2
T:qtesla1
T:pass769
T:pass863
T:falcon1024dyn
T:falcon512dyn
T:falcon1024tree
T:falcon512tree
T:luov863256pc
T:rainbow4a
T:mqsignrr2567246
T:mqsignlr2567246
mqsignrr2567246
T:mqsignrr25611272
T:mqsignlr25611272
mqsignrr25611272
mqsignlr25611272
T:rainbow3cclassic683248
T:rainbow3c
T:redgemss128
T:ronald4096
mqsignlr2567246
T:rainbow1a
T:rainbow1b
T:donald512
T:redgemss128v2
T:ronald3072
T:rainbow1aclassic363232
T:rwb0fuz1024
T:bluegemss128
T:ronald1536
T:ronald2048
T:ronald768
T:rainbowbinary256181212
T:ronald512
T:ronald1024
T:rainbowbinary16242020
ed25519
dilithium5aes
nccsign5aes
nccsign3aes
dilithium5
dilithium3
nccsign3
haetae5
dilithium2aes
dilithium3aes
nccsign1aes
haetae2
T:sphincs128harakasimple
T:sphincs128harakarobust
T:sphincs192shake256simple
T:sphincs256shake256robust
T:sphincs256shake256simple
T:sphincs192shake256robust
T:sphincsf128shake256robust
T:sphincsf128shake256simple
T:sphincss128shake256simple
T:sphincss128shake256robust
T:luov8117404pc
T:luov890351pc
T:luov4849242
T:luov6468330
T:luov8086399
T:redgemss256v2
T:ecdonaldp521
T:ecdonaldp384
T:ecdonaldb571
T:ecdonaldb409
T:ecdonaldk571
T:ecdonaldk409
T:ecdonaldb283
T:ecdonaldk283
T:ecdonaldb233
T:ecdonaldk233
T:ecdonaldp163
T:ecdonaldk163
T:ecdonaldp192
T:ecdonaldp160
T:ecdonaldp224
T:ecdonaldp256
T:ecdonaldp521
T:ecdonaldp384
T:ecdonaldb571
T:ecdonaldb409
T:ecdonaldk571
T:ecdonaldk409
T:ecdonaldb283
T:ecdonaldk283
T:ecdonaldb233
T:ecdonaldk233
T:ecdonaldp192
T:ecdonaldp160
T:ecdonaldp163
T:ecdonaldk163