amd64, shoe, crypto_sign, sign time, signature size

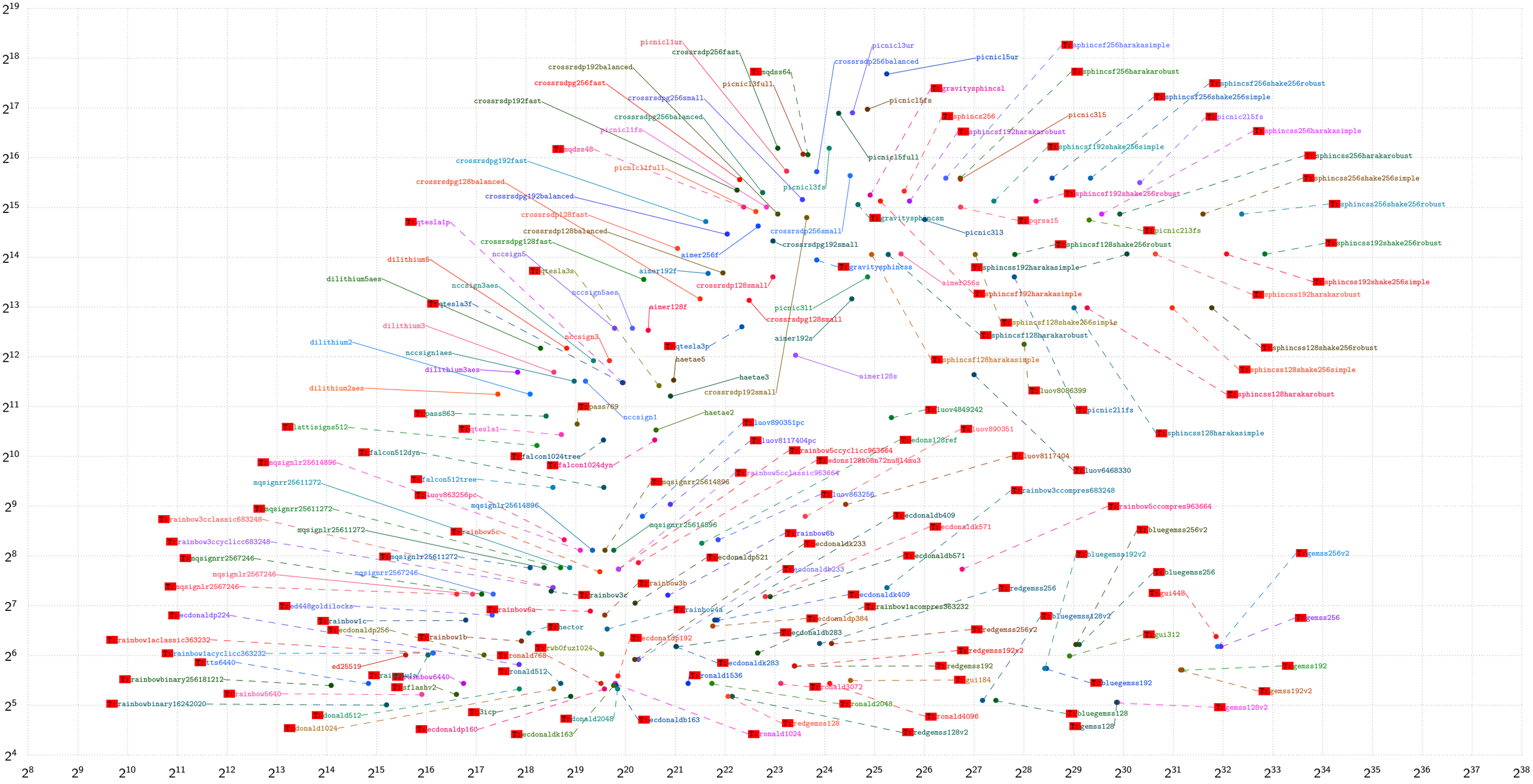
https://bench.cr.yp.to

20250412

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

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.


2^19
2^18
2^17
2^16
2^15
2^14
2^13
2^12
2^11
2^10
2^9
2^8
2^7
2^6
2^5
2^4
2^8 2^9 2^10 2^11 2^12 2^13 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 2^33 2^34 2^35 2^36 2^37 2^38
picnicl1ur
crossrsdp256fast
crossrsdp192balanced
crossrsdp256fast
crossrsdpg256small
crossrsdp192fast
crossrsdpg256balanced
picnicl1fs
T:mqdss48
picnicl1full
crossrsdpg192fast
crossrsdpg128balanced
crossrsdpg192balanced
crossrsdp128fast
crossrsdp128balanced
crossrsdpg128fast
nccsign5
dilithium5
T:qtesla1p
dilithium5aes
nccsign3aes
T:qtesla3f
dilithium3
dilithium2
nccsign1aes
dilithium3aes
dilithium2aes
T:lattisigns512
T:falcon512dyn
T:mqsignlr25614896
mqsignrr25611272
T:falcon512tree
T:luov863256pc
T:mqsignrr25611272
T:rainbow3cclassic683248
mqsignlr25611272
T:rainbow3ccyclicc683248
T:mqsignrr2567246
mqsignlr2567246
T:mqsignlr2567246
T:ed448goldilocks
T:ecdonaldp224
T:rainbow1c
T:ecdonaldp256
T:rainbow1aclassic363232
T:rainbow1acyclicc363232
T:tts6440
T:rainbowbinary256181212
T:rainbow5640
T:rainbowbinary16242020
T:donald512
T:donald1024
T:3icp
T:ecdonaldp160
T:ecdonaldk163
T:donald2048
T:ecdonaldb163
T:ronald1024
T:redgemss128
T:ronald2048
T:ronald4096
T:redgemss128v2
T:bluegemss128
T:gemss128
T:gemss128v2
T:bluegemss192
T:gemss192v2
T:gemss192
T:ronald3072
T:gui184
T:redgemss192
T:ronald1536
T:ronald512
T:ronald768
ed25519
T:sflashv2
T:rainbow6440
T:rainbow1b
T:rwb0fuz1024
T:hector
T:rainbow6a
T:rainbow3c
T:rainbow5c
T:rainbow3b
T:rainbow4a
T:ecdonaldp192
T:ecdonaldk283
T:ecdonaldp384
T:ecdonaldb283
T:redgemss256v2
T:redgemss192v2
T:rainbow1acompres363232
T:redgemss256
T:ecdonaldk409
T:ecdonaldb409
T:rainbow6b
T:ecdonaldk233
T:ecdonaldp521
T:ecdonaldb233
T:ecdonaldk571
T:ecdonaldb571
T:rainbow3ccompres683248
T:rainbow5ccompres963664
T:bluegemss256v2
T:bluegemss192v2
T:bluegemss256
T:gui448
T:gui312
T:bluegemss128v2
T:gemss256v2
T:gemss256
T:luov6468330
T:luov8117404
T:luov890351
T:redons128
T:redons128k08n72nu814mu3
T:rainbow5ccyclicc963664
T:rainbow5cclassic963664
T:luov8117404pc
T:luov890351pc
T:luov4849242
T:luov8086399
T:picnic211fs
T:sphincss128harakasimple
T:sphincss128harakarobust
T:sphincss128shake256simple
T:sphincss128shake256robust
T:sphincsf128harakasimple
T:sphincsf128harakarobust
T:sphincsf128shake256simple
T:sphincsf128shake256robust
T:sphincss192harakasimple
T:sphincss192harakarobust
T:sphincss192shake256simple
T:sphincss192shake256robust
T:sphincsf192harakasimple
T:sphincsf192harakarobust
T:sphincsf192shake256simple
T:sphincsf192shake256robust
T:sphincs256
T:gravitysphincsl
T:sphincsf256harakasimple
T:sphincsf256harakarobust
T:sphincsf256shake256simple
T:sphincsf256shake256robust
T:sphincss256harakasimple
T:sphincss256harakarobust
T:sphincss256shake256simple
T:sphincss256shake256robust
T:picnic215fs
T:picnic213fs
T:picnic315
T:pqrsa15
T:gravitysphincsm
T:gravitysphincss
T:qtesla3s
T:qtesla3p
T:qtesla1
T:pass863
T:pass769
T:falcon1024tree
T:falcon1024dyn
T:mqsignrr25614896
T:mqsignlr25614896
T:rainbow5c
T:rainbow3c
T:rainbow3b
T:rainbow6a
T:rainbow4a
T:rainbow1c
T:rainbow1b
T:hector
T:rwb0fuz1024
T:ecdonaldp256
T:ecdonaldp224
T:ecdonaldp192
T:ecdonaldp521
T:ecdonaldp384
T:ecdonaldk283
T:ecdonaldb283
T:ecdonaldk409
T:ecdonaldb409
T:ecdonaldk233
T:ecdonaldb233
T:ecdonaldk571
T:ecdonaldb571
T:redgemss256
T:redgemss192
T:redgemss128
T:gui184
T:gui312
T:gui448
T:bluegemss256
T:bluegemss192
T:bluegemss128
T:gemss256
T:gemss192
T:gemss128
T:luov663256
T:luov8117404pc
T:luov890351pc
T:luov4849242
T:luov8086399
T:picnic211fs
T:sphincss128harakasimple
T:sphincss128harakarobust
T:sphincss128shake256simple
T:sphincss128shake256robust
T:sphincsf128harakasimple
T:sphincsf128harakarobust
T:sphincsf128shake256simple
T:sphincsf128shake256robust
T:sphincss192harakasimple
T:sphincss192harakarobust
T:sphincss192shake256simple
T:sphincss192shake256robust
T:sphincsf192harakasimple
T:sphincsf192harakarobust
T:sphincsf192shake256simple
T:sphincsf192shake256robust
T:sphincs256
T:gravitysphincsl
T:sphincsf256harakasimple
T:sphincsf256harakarobust
T:sphincsf256shake256simple
T:sphincsf256shake256robust
T:sphincss256harakasimple
T:sphincss256harakarobust
T:sphincss256shake256simple
T:sphincss256shake256robust
T:picnic215fs
T:picnic213fs
T:picnic315
T:pqrsa15
T:gravitysphincsm
T:gravitysphincss
T:qtesla3s
T:qtesla3p
T:qtesla1
T:pass863
T:pass769
T:falcon1024tree
T:falcon1024dyn
T:mqsignrr25614896
T:mqsignlr25614896
T:rainbow5c
T:rainbow3c
T:rainbow3b
T:rainbow6a
T:rainbow4a
T:rainbow1c
T:rainbow1b
T:hector
T:rwb0fuz1024
T:ecdonaldp256
T:ecdonaldp224
T:ecdonaldp192
T:ecdonaldp521
T:ecdonaldp384
T:ecdonaldk283
T:ecdonaldb283
T:ecdonaldk409
T:ecdonaldb409
T:ecdonaldk233
T:ecdonaldb233
T:ecdonaldk571
T:ecdonaldb571
T:redgemss256
T:redgemss192
T:redgemss128
T:gui184
T:gui312
T:gui448
T:bluegemss256
T:bluegemss192
T:bluegemss128
T:gemss256
T:gemss192
T:gemss128
T:luov663256
T:luov8117404
T:luov890351
T:luov6468330
T:rainbow3ccompres683248
T:rainbow5ccompres963664
T:bluegemss256v2
T:bluegemss192v2
T:gemss256v2
T:gemss192v2
T:gemss128v2
T:bluegemss128v2
T:redgemss256v2
T:redgemss192v2
T:rainbow1acompres363232
T:redons128
T:redons128k08n72nu814mu3
T:rainbow5ccyclicc963664
T:rainbow5cclassic963664