amd64, lucienne, crypto_sign, open time, signature size

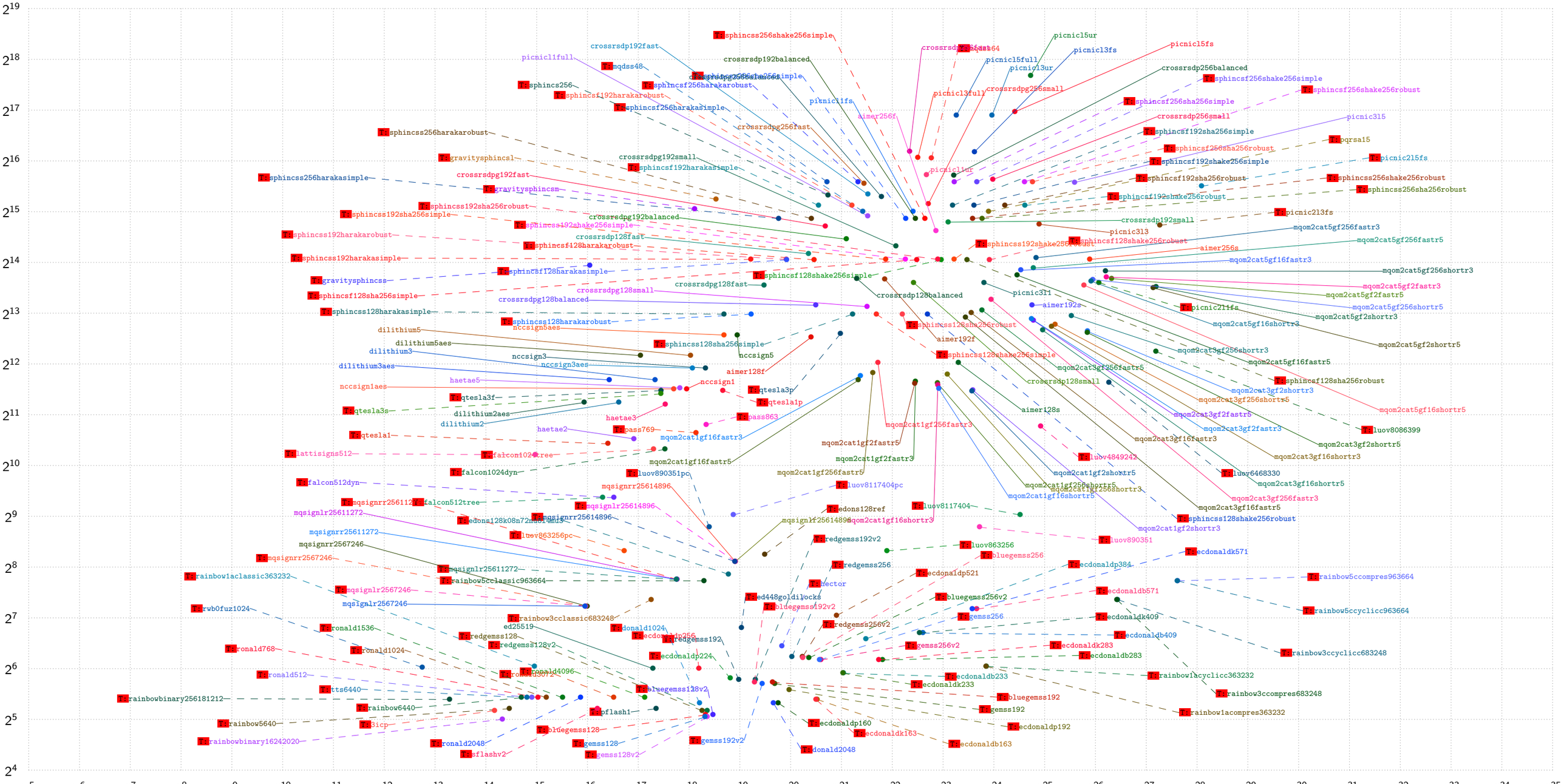
https://bench.cr.yp.to

20260402

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.


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
2^5 2^6 2^7 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
T:sphincss256shake256simple
crossrsdp192fast
picnicl1full
T:mqdss48
crossrsdp192balanced
T:sphincs256
T:sphincsf192harakarobust
T:sphincsf256harakarobust
T:sphincsf256harakasimple
picnicl1fs
aimer256f
crossrsdpg256fast
crossrsdp256small
picnicl3full
picnicl5ur
picnicl3fs
picnicl5full
picnicl3ur
picnicl5fs
crossrsdp256balanced
T:sphincsf256shake256simple
T:sphincsf256shake256robust
T:sphincsf256sha256simple
crossrsdp256small
picnic315
T:sphincsf192sha256simple
T:sphincsf256sha256robust
T:pqrsa15
T:sphincsf192shake256simple
T:picnic215fs
T:sphincsf192sha256robust
T:sphincss256shake256robust
T:sphincss256sha256robust
T:sphincsf192shake256robust
T:picnic213fs
crossrsdp192small
picnic313
T:sphincsf128shake256robust
aimer256s
mqom2cat5gf256fastr3
mqom2cat5gf256fastr5
mqom2cat5gf16fastr3
mqom2cat5gf256shortr3
mqom2cat5gf2fastr3
mqom2cat5gf2fastr5
mqom2cat5gf256shortr5
mqom2cat5gf2shortr3
mqom2cat5gf2shortr5
mqom2cat3gf256shortr3
mqom2cat5gf16fastr5
T:sphincsf128sha256robust
mqom2cat3gf2shortr3
mqom2cat3gf256shortr5
mqom2cat5gf16shortr5
mqom2cat3gf2fastr5
mqom2cat3gf2fastr3
T:luov8086399
mqom2cat3gf16fastr3
mqom2cat3gf2shortr5
mqom2cat3gf16shortr3
T:luov4849242
T:luov6468330
mqom2cat3gf16shortr5
mqom2cat3gf256fastr3
mqom2cat3gf16fastr5
T:sphincss128shake256robust
mqom2cat1gf2shortr3
T:luov890351
T:ecdonaldk571
T:ecdonaldp384
T:rainbow5ccompres963664
T:ecdonaldb571
T:ecdonaldk409
T:ecdonaldb409
T:ecdonaldk283
T:ecdonaldb283
T:rainbow5ccyclicc963664
T:rainbow3ccyclicc683248
T:rainbow1acyclicc363232
T:rainbow3ccompres683248
T:rainbow1acompres363232
T:ecdonaldp192
T:ecdonaldb163
T:ecdonaldk163
T:ecdonaldp160
T:ecdonaldb233
T:ecdonaldk233
T:bluegemss192
T:gemss192
T:bluegemss256v2
T:gemss256
T:gemss256v2
T:ecdonaldp521
T:bluegemss256
T:luov863256
T:redgemss192v2
T:redgemss256
T:rector
T:ed448goldilocks
T:bluegemss192v2
T:redgemss256v2
T:donald2048
T:gemss192v2
T:gemss128
T:gemss128v2
T:bluegemss128
T:pflash1
T:bluegemss128v2
T:ecdonaldp224
T:redgemss192
T:donald1024
T:rainbow3cclassic683248
ed25519
T:redgemss128
T:redgemss128v2
T:ronald1024
T:ronald4096
T:ronald5072
T:ronald2048
T:sflashv2
T:3icp
T:rainbow5640
T:rainbowbinary16242020
T:rainbowbinary256181212
T:rainbow6440
T:tts6440
T:ronald512
T:ronald768
T:ronald1536
T:rwb0fuz1024
T:rainbow1aclassic363232
T:mqsignrr2567246
mqsignrr2567246
mqslgnlr2567246
T:mqsignlr25611272
T:rainbow5cclassic963664
mqsignlr25611272
mqsignrr25611272
T:falcon512dyn
T:falcon512tree
T:edons128k08n72m0r4mu5
T:luov863256pc
T:falcon1024dyn
T:falcon1024tree
T:lattisigns512
T:qtesla1
T:qtesla3s
T:qtesla3f
T:qtesla3p
T:qtesla1p
T:pass863
T:pass769
haetae5
haetae3
haetae2
dilithium5aes
dilithium5
dilithium3
dilithium3aes
dilithium2aes
dilithium2
nccsign1aes
nccsign3aes
nccsign3
nccsign5aes
nccsign5
nccsign1
aimer128f
aimer192f
aimer192s
aimer128s
T:sphincss128sha256simple
T:sphincss128sha256robust
T:sphincss128shake256simple
T:sphincsf128harakasimple
T:sphincsf128harakarobust
T:sphincsf128shake256simple
T:sphincsf128sha256simple
T:sphincss128harakasimple
T:sphincss128harakarobust
T:gravitysphincss
crossrsdpg128small
crossrsdpg128balanced
crossrsdp128balanced
crossrsdp128fast
crossrsdp128small
T:sphincss192harakarobust
T:sphincss192harakasimple
T:sphincss192sha256simple
T:sphincss192sha256robust
T:sphincss192shake256simple
crossrsdpg192balanced
crossrsdpg192fast
T:gravitysphincsl
T:gravitysphincsm
crossrsdpg192small
T:sphincsf192harakasimple
T:sphincss256harakasimple
T:sphincss256harakarobust
picnic311
picnic211fs
T:luov8117404pc
T:luov8117404
T:edons128ref
mqsignrr25614896
mqsignlr25614896
mqsignlr25614896
mqsignrr256112
mqsignrr25614896
mqom2cat1gf256fastr3
mqom2cat1gf2fastr5
mqom2cat1gf2fastr3
mqom2cat1gf256fastr5
mqom2cat1gf16fastr3
mqom2cat1gf16fastr5
mqom2cat1gf16shortr3
mqom2cat1gf16shortr5
mqom2cat1gf256shortr3
mqom2cat1gf256shortr5
mqom2cat1gf2shortr5
T:pass769
T:qtesla1p
T:qtesla3p
T:luov890351pc
T:luov863256
T:bluegemss256
T:redgemss192v2
T:redgemss256
T:rector
T:ed448goldilocks
T:bluegemss192v2
T:redgemss256v2
T:gemss256
T:gemss256v2
T:ecdonaldp521
T:ecdonaldp384
T:ecdonaldb571
T:ecdonaldk409
T:ecdonaldb409
T:ecdonaldk283
T:ecdonaldb283
T:ecdonaldk571
T:ecdonaldb233
T:ecdonaldk233
T:bluegemss192
T:gemss192
T:ecdonaldp192
T:ecdonaldb163
T:ecdonaldk163
T:ecdonaldp160