amd64, freshwrap,little, crypto_sign, open time, signature size

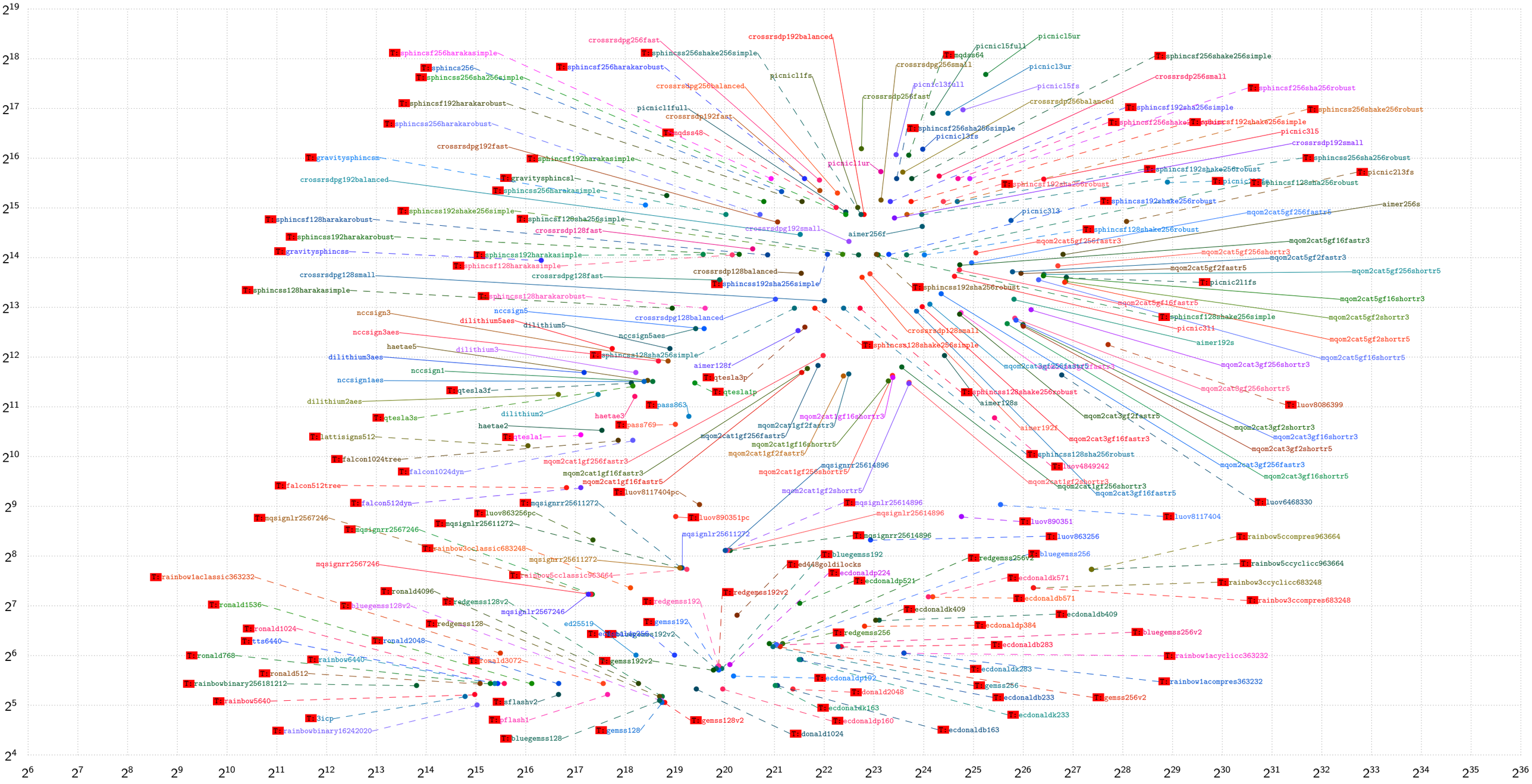
https://bench.cr.yp.to

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

20260422

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
2^6 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 2^36
T:sphincsf256harakasimple
T:sphincs256
T:sphincs256sha256simple
T:sphincsf192harakarobust
T:sphincss256harakarobust
T:gravitysphincsm
T:gravitysphincsl
T:sphincs256harakasimple
T:sphincsf192harakasimple
T:sphincss192shake256simple
T:sphincsf128harakarobust
T:sphincsf128sha256simple
T:sphincss192harakarobust
T:gravitysphincss
T:sphincs192harakasimple
T:sphincsf128harakasimple
T:sphincss128harakasimple
T:sphincss128harakarobust
T:sphincss128sha256simple
T:qtesla3f
T:qtesla3s
T:lattisigns512
T:falcon1024tree
T:falcon1024dyn
T:falcon512tree
T:falcon512dyn
T:mqsignr2567246
T:mqsignlr2567246
T:rainbow3cclassic683248
T:rainbow1aclassic363232
T:ronald4096
T:ronald1536
T:bluegemss128v2
T:redgemss128v2
T:ronald1024
T:tts6440
T:ronald2048
T:ronald768
T:rainbow6440
T:ronald3072
T:ronald512
T:rainbowbinary256181212
T:rainbow5640
T:sflashv2
T:3icp
T:oflash1
T:rainbowbinary16242020
T:bluegemss128
T:gemss128
T:gemss128v2
T:redgemss128
T:gemss192
T:redgemss192
T:redgemss192v2
T:gemss192v2
T:bluegemss192v2
T:bluegemss192
T:redgemss192v2
T:ed448goldilocks
T:ecdonaldp224
T:ecdonaldp521
T:ecdonaldp192
T:donald2048
T:ecdonaldk163
T:ecdonaldp160
T:donald1024
T:ecdonaldb163
T:ecdonaldk233
T:ecdonaldb233
T:gemss256
T:ecdonaldk283
T:ecdonaldb283
T:ecdonaldp384
T:redgemss256
T:ecdonaldk409
T:ecdonaldb409
T:ecdonaldb571
T:ecdonaldk571
T:redgemss256v2
T:bluegemss256
T:gemss256v2
T:bluegemss256v2
T:rainbow1acompres363232
T:rainbow1acyclicc363232
T:rainbow3ccompres683248
T:rainbow3ccyclicc683248
T:rainbow5ccyclicc963664
T:rainbow5ccompres963664
T:luov8117404
T:luov6468330
T:luov8086399
T:luov863256
T:luov890351
T:luov4849242
T:luov8117404pc
T:luov863256pc
T:luov890351pc
T:mqsignr25611272
T:mqsignlr25611272
T:mqsignr25614896
T:mqsignlr25614896
T:pass863
T:pass769
T:qtesla1
T:qtesla1p
T:qtesla3p
T:mqdss64
T:mqdss48
T:sphincs256sha256simple
T:sphincs256shake256simple
T:sphincsf256shake256simple
T:sphincsf192sha256simple
T:sphincsf256shake256robust
T:sphincsf192shake256simple
T:sphincsf192shake256robust
T:sphincsf192sha256robust
T:sphincsf128sha256robust
T:sphincsf128shake256robust
T:sphincsf128shake256simple
T:sphincsf256sha256robust
T:sphincss256shake256robust
T:sphincss256sha256robust
T:sphincss192shake256robust
T:sphincss192sha256robust
T:sphincss128shake256simple
T:sphincss128shake256robust
T:sphincss128sha256robust
picnicl1fs
picnicl1full
picnicl1ur
picnicl3full
picnicl3ur
picnicl3fs
picnicl5full
picnicl5ur
picnicl5fs
picnicl3fs
picnic313
picnic211fs
picnic311
picnic315
picnic213fs
crossrsdp256fast
crossrsdp256balanced
crossrsdp256small
crossrsdp192balanced
crossrsdp192fast
crossrsdp192small
crossrsdp128fast
crossrsdp128balanced
crossrsdp128small
crossrsdpg256fast
crossrsdpg256balanced
crossrsdpg256small
crossrsdpg192balanced
crossrsdpg192small
crossrsdpg128small
crossrsdpg128balanced
aimer256f
aimer128f
aimer192s
aimer128s
aimer192f
aimer256s
mqom2cat5gf256fastr5
mqom2cat5gf256fastr3
mqom2cat5gf256shortr3
mqom2cat5gf2fastr3
mqom2cat5gf2fastr5
mqom2cat5gf256shortr5
mqom2cat5gf16fastr3
mqom2cat5gf16fastr5
mqom2cat5gf16shortr3
mqom2cat5gf2shortr3
mqom2cat5gf2shortr5
mqom2cat5gf16shortr5
mqom2cat3gf256fastr5fastr3
mqom2cat3gf256shortr3
mqom2cat3gf256shortr5
mqom2cat3gf2fastr5
mqom2cat3gf16fastr3
mqom2cat3gf2shortr3
mqom2cat3gf16shortr3
mqom2cat3gf2shortr5
mqom2cat3gf256fastr3
mqom2cat3gf16shortr5
mqom2cat3gf16fastr5
mqom2cat1gf2fastr3
mqom2cat1gf256fastr5
mqom2cat1gf16shortr5
mqom2cat1gf2fastr5
mqom2cat1gf256fastr3
mqom2cat1gf16fastr3
mqom2cat1gf16fastr5
mqom2cat1gf16shortr3
mqom2cat1gf256shortr5
mqom2cat1gf2shortr5
mqom2cat1gf2shortr2
mqom2cat1gf256shortr3
mqom2cat3gf16fastr5
mqsignr25614896
mqsignlr25614896
mqsignr25611272
mqsignlr25611272
mqsignr2567246
mqsignlr2567246
ed25519
ed448
dilithium5aes
dilithium5
dilithium3
dilithium3aes
dilithium2aes
dilithium2
nccsign3
nccsign3aes
nccsign5
nccsign5aes
nccsign1
nccsign1aes
haetae5
haetae3
haetae2
haetae1
mqdss
gravitysphincs
sphincs192
sphincs128
sphincs256
sphincs192shake256robust
sphincs128sha256robust
sphincs128shake256robust
sphincs192sha256robust
sphincs128shake256simple
sphincs128sha256simple
sphincs192sha256simple
sphincs192shake256simple
sphincs128harakasimple
sphincs128harakarobust
sphincs192harakasimple
sphincs192harakarobust
sphincs256harakasimple
sphincs256harakarobust
sphincs256sha256simple
sphincs256shake256simple
sphincs256sha256robust
sphincs256shake256robust
sphincs192shake256robust
sphincs192sha256robust
sphincs128shake256robust
sphincs128sha256robust
sphincs128shake256simple
sphincs128sha256simple
sphincs192shake256simple
sphincs192sha