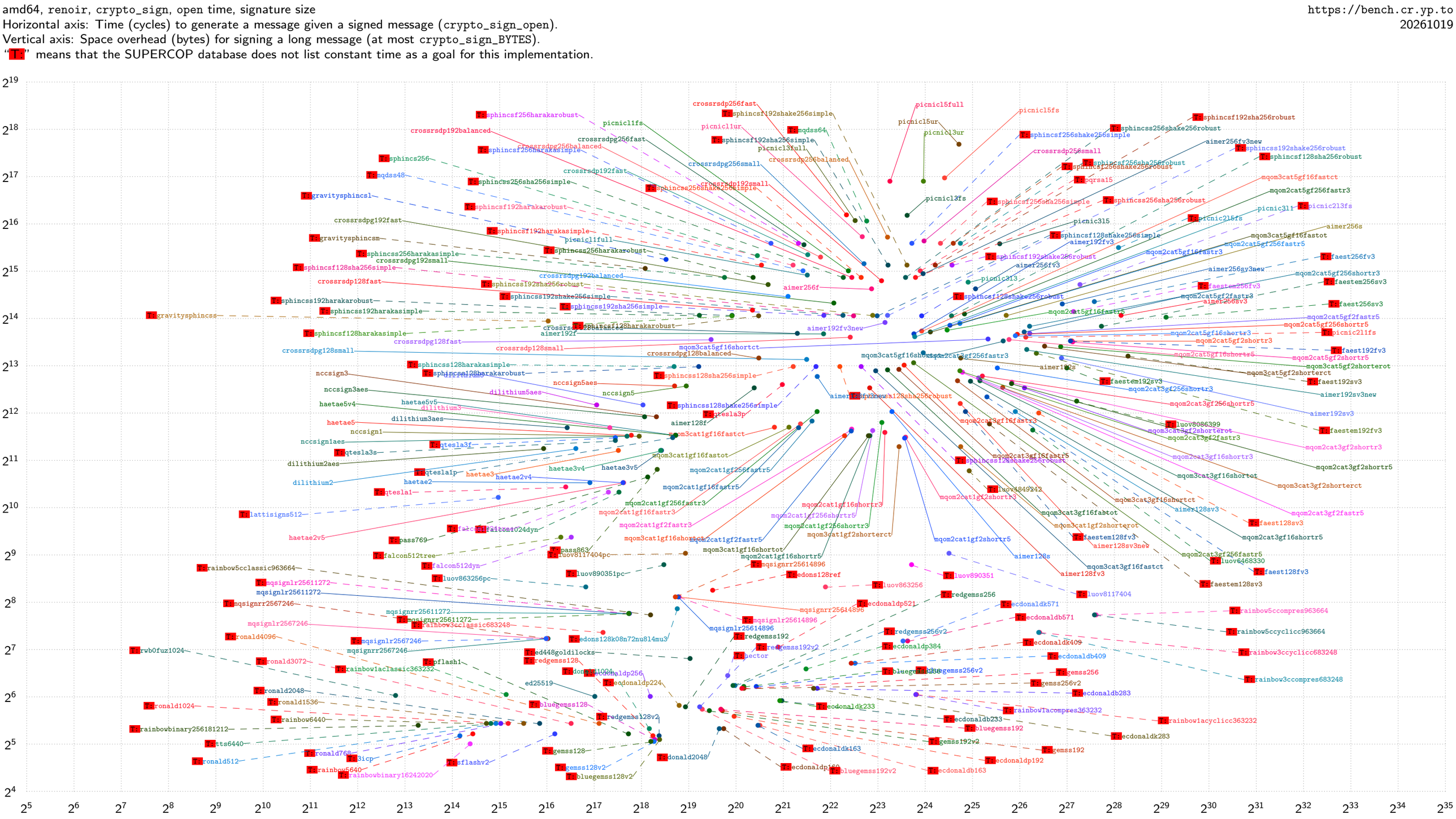
amd64, renoir, crypto_sign, open time, signature size
https://bench.cr.yp.to
20261019
Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open).
Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).
"T:" means that the SUPERCOP 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:sphincsf256harakarobust
T:sphincsf192shake256simple
picnicl15full
picnicl15fs
T:sphincsf192sha256robust
crossrsdp256fast
picnicl5ur
picnicl3ur
T:sphincsf256shake256simple
T:sphincss256shake256robust
picnicl1fs
T:mqdss64
picnicl1ur
T:sphincsf192sha256simple
crossrsdp192balanced
crossrsdpg256fast
picnicl3full
crossrsdp256small
aimer256fv3new
T:sphincss192shake256robust
T:sphincsf256harakasimple
crossrsdp256balanced
T:sphincsf128sha256robust
T:sphincsf256sha256robust
T:sphincs256
crossrsdpg256small
T:sphincsf256sha256robust
T:mqdss48
crossrsdp192fast
T:pqrsa15
T:sphincss256sha256simple
crossrsdp192small
mqom3cat5gf16fastct
T:sphincss256shake256simple
T:gravitysphincsl
picnicl3fs
mqom2cat5gf256fastr3
T:sphincsf256sha256simple
T:sphincss256sha256robust
T:sphincsf192harakarobust
picnic311
T:picnic213fs
picnic315
T:picnic215fs
crossrsdpg192fast
T:sphincsf192harakasimple
aimer256s
T:gravitysphincsm
picnicl1full
aimer192fv3
mqom3cat5gf16fastot
T:sphincsf128shake256simple
mqom2cat5gf256fastr5
T:sphincss256harakasimple
T:sphincss256harakarobust
mqom2cat5gf16fastr3
T:faest256fv3
crossrsdpg192small
T:sphincsf192shake256robust
aimer256fv3
T:sphincsf128sha256simple
aimer256sv3new
mqom2cat5gf256shortr3
crossrsdpg192balanced
picnic313
T:faestem256fv3
T:faestem256sv3
crossrsdp128fast
T:sphincsf128shake256robust
T:sphincss192sha256robust
mqom2cat5gf2fastr3
T:sphincss192harakarobust
T:sphincss192shake256simple
aimer256sv3
T:faest256sv3
T:sphincss192harakasimple
T:sphincss192sha256simple
mqom2cat5gf16fastr5
mqom2cat5gf2fastr5
T:gravitysphincss
mqom2cat5gf256shortr5
T:sphincsf128harakarobust
aimer192fv3new
mqom2cat5gf16shortr3
T:picnicl1fs
T:sphincsf128harakasimple
aimer192f
mqom2cat5gf2shortr3
crossrsdpg128fast
T:faest192fv3
crossrsdp128small
mqom3cat5gf16shortct
crossrsdpg128small
crossrsdp128balanced
mqom2cat5gf16shortr5
mqom2cat5gf2shortr5
T:sphincss128harakasimple
mqom3cat5gf2shorterot
T:sphincss128harakarobust
nccsign3
T:sphincss128sha256simple
nccsign5aes
aimer192s
mqom3cat5gf2shortercrt
T:faestem192sv3
nccsign3aes
dilithium5aes
nccsign5
T:faest192sv3
mqom2cat3gf256shortr3
haetae5v4
haetae5v5
dilithium3
T:sphincss128shake256simple
aimer192sv3new
mqom2cat3gf256shortr5
T:tesla3p
dilithium3aes
haetae5
aimer128f
T:luov8086399
aimer192sv3
nccsign1
mqom3cat1gf16fastct
mqom3cat3gf2shorterot
T:faestem192fv3
mqom2cat3gf2fastr3
nccsign1aes
T:tesla3f
mqom2cat3gf2shortr3
T:tesla3s
mqom3cat1gf16fastot
mqom2cat3gf16fastr5
mqom2cat3gf16shortr3
dilithium2aes
T:sphincss128shake256robust
haetae3v4
haetae3v5
mqom2cat3gf2shortr5
T:tesla1p
haetae3
haetae2v4
mqom2cat1gf256fastr5
mqom3cat3gf16shortot
dilithium2
haetae2
mqom2cat1gf16fastr5
T:luov8349242
mqom3cat3gf2shorterct
T:tesla1
mqom2cat1gf2shortr3
mqom2cat1gf256fastr3
mqom2cat1gf16shortr3
mqom3cat3gf16shortct
T:lattisigns512
mqom2cat1gf256shortr5
aimer128sv3
mqom2cat3gf2fastr5
mqom2cat1gf16fastr3
mqom2cat1gf256shortr3
mqom3cat3gf16fastot
mqom2cat1gf2fastr3
mqom3cat1gf2shorterot
T:faest128sv3
haetae2v5
T:falcon1024dyn
mqom2cat1gf2shortercrt
T:faestem128fv3
T:pass769
mqom3cat1gf16shortct
mqom2cat1gf2fastr5
mqom2cat1gf2shortr5
mqom2cat3gf16shortr5
T:pass863
aimer128sv3new
T:falcon512tree
T:luov8117404pc
mqom3cat1gf16shortot
mqom2cat1gf16shortr5
aimer128s
mqom2cat3gf256fastr5
T:mqsignrr25614896
T:luov6466330
T:falcon512dyn
mqom3cat3gf16fastct
T:edons128ref
T:faest128fv3
T:luov890351pc
T:luov890351
T:luov863256pc
aimer128fv3
T:faestem128sv3
T:rainbow5cclassic963664
T:luov863256
T:redgemss256
T:luov8117404
T:mqsignlr25611272
mqsignlr25611272
T:ecdonaldp521
T:ecdonaldk571
T:mqsignrr2567246
mqsignrr25614896
T:rainbow5ccompres963664
mqsignrr25611272
T:mqsignrr25611272
T:ecdonaldb571
mqsignlr25614896
T:rainbow3cclassic683248
T:redgemss256v2
T:rainbow5ccyclicc963664
T:ronald4096
T:redgemss192
T:ecdonaldk409
T:mqsignlr2567246
T:edons128k08n72nu814mu3
T:ecdonaldp384
T:rainbow3ccyclicc683248
mqsignrr2567246
T:redgemss192v2
T:ecdonaldb409
T:rwb0fuz1024
T:ed448goldilocks
T:hector
T:ronald3072
T:redgemss128
T:bluegemss256v2
T:gemss256
T:rainbow1aclassic363232
T:pflash1
T:edonaldp1024
T:gemss256v2
T:rainbow3ccompres683248
T:ecdonaldp256
T:ronald2048
ed25519
T:ecdonaldp224
T:ecdonaldb283
T:ronald1536
T:bluegemss128
T:ecdonaldk233
T:rainbow7acompres363232
T:ronald1024
T:redgemss128v2
T:rainbow1acyclicc363232
T:rainbow6440
T:ecdonaldb233
T:bluegemss192
T:rainbowbinary256181212
T:ecdonaldk283
T:gemss192v2
T:tts6440
T:gemss192
T:ecdonaldk163
T:ronald768
T:3icp
T:ecdonaldp192
T:ronald512
T:sflashv2
T:ecdonaldp160
T:bluegemss192v2
T:ecdonaldb163
T:rainbow5640
T:gemss128
T:donald2048
T:gemss128v2
T:rainbowbinary16242020
T:bluegemss128v2