amd64, renoir, crypto_sign, keypair time, key size

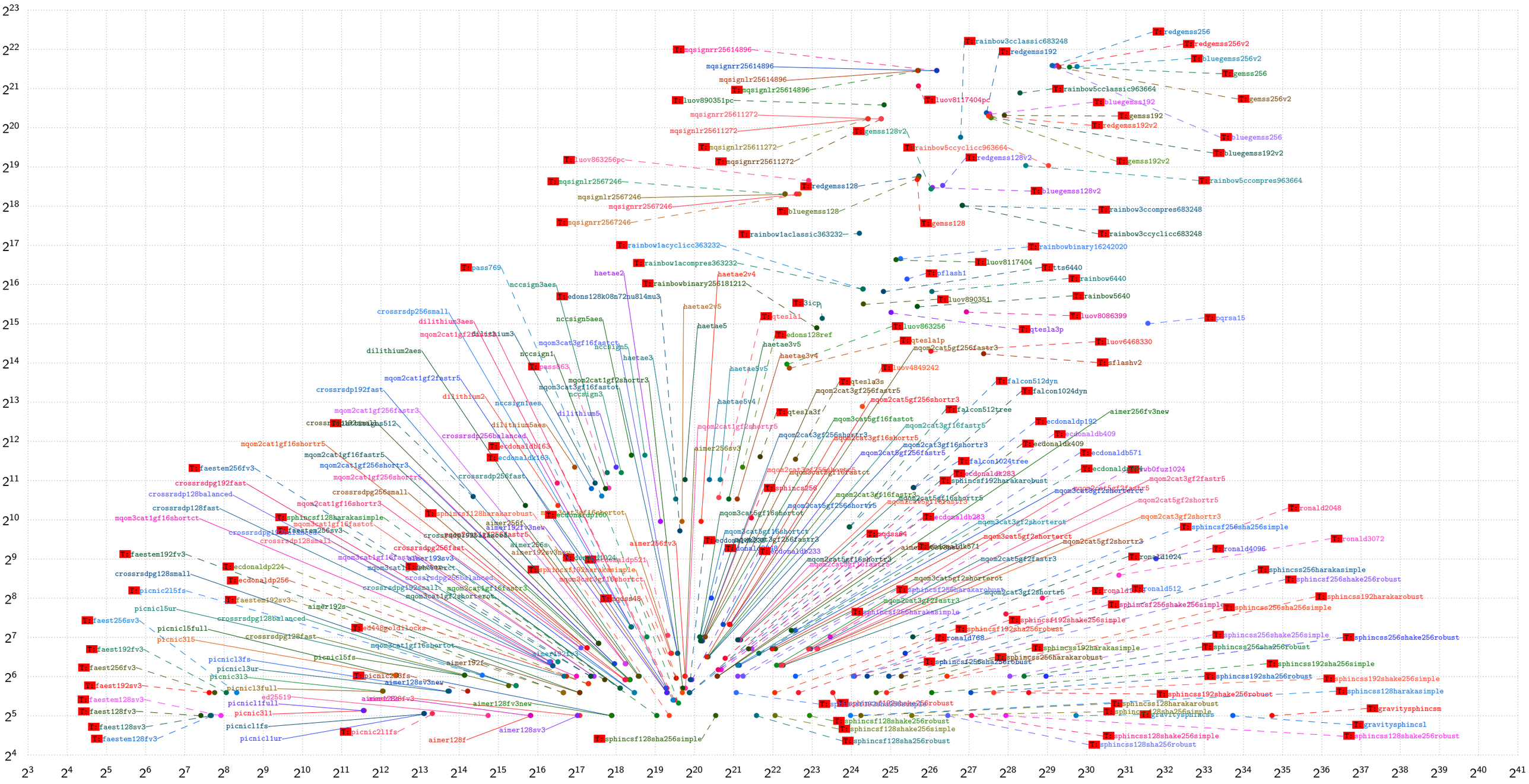
https://bench.cr.yp.to

20261019

Horizontal axis: Time (cycles) to generate a public key (crypto_sign_keypair).

Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).

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


2^23
2^22
2^21
2^20
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
2^3 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 2^36 2^37 2^38 2^39 2^40 2^41
T:redgemss256
T:redgemss256v2
T:bluegemss256v2
T:gemss256
T:gemss256v2
T:rainbow3cclassic683248
T:redgemss192
T:rainbow5cclassic963664
T:bluegemss192
T:gemss192
T:redgemss192v2
T:bluegemss256
T:bluegemss192v2
T:gemss192v2
T:rainbow5ccompres963664
T:mqsignrr25614896
mqsignrr25614896
mqsignlr25614896
T:mqsignlr25614896
T:luov890351pc
T:luov8117404pc
mqsignrr25611272
mqsignlr25611272
T:gemss128v2
T:mqsignlr25611272
T:mqsignrr25611272
T:rainbow5ccyclicc963664
T:redgemss128v2
T:luov863256pc
T:mqsignlr2567246
T:redgemss128
mqsignlr2567246
mqsignrr2567246
T:mqsignrr2567246
T:bluegemss128v2
T:bluegemss128
T:gemss128
T:rainbow3ccompres683248
T:rainbow3ccyclicc683248
T:rainbow1aclassic363232
T:rainbow1acyclicc363232
T:rainbowbinary16242020
T:rainbow1acompres363232
T:luov8117404
T:pass769
T:pflash1
T:tts6440
haetae2
haetae2v4
T:rainbowbinary256181212
T:rainbow6440
nccsign3aes
T:edons128k08n72nu814mu3
T:luov890351
T:rainbow5640
haetae2v5
T:3icp
T:luov8086399
T:pqrsa15
crossrsdp256small
dilithium3aes
nccsign5aes
T:qtesla1
T:qtesla3p
haetae5
T:luov863256
T:edons128ref
T:qtesla1p
T:luov6468330
haetae3v5
haetae3v4
T:sflashv2
T:luov4849242
T:qtesla3s
T:falcon512dyn
T:falcon1024dyn
T:qtesla3f
T:falcon512tree
T:falcon1024tree
T:ecdonaldp192
T:ecdonaldb409
T:ecdonaldk409
T:ecdonaldb571
T:ecdonaldk283
T:sphincsf192harakarobust
T:sphincs256
T:ecdonaldb283
T:mqdss64
T:mqdss48
T:ronald2048
T:ronald3072
T:ronald4096
T:ronald1024
T:ronald768
T:ronald512
T:sphincsf256sha256simple
T:sphincsf256shake256robust
T:sphincsf256harakarobust
T:sphincsf256shake256simple
T:sphincsf192sha256robust
T:sphincsf192shake256simple
T:sphincsf256sha256robust
T:sphincsf128harakarobust
T:sphincsf128shake256robust
T:sphincsf128shake256simple
T:sphincsf128sha256robust
T:sphincss256sha256simple
T:sphincss256shake256simple
T:sphincss256shake256robust
T:sphincss256sha256robust
T:sphincss256harakarobust
T:sphincss192harakarobust
T:sphincss192sha256simple
T:sphincss192shake256simple
T:sphincss192sha256robust
T:sphincss192shake256robust
T:sphincss128harakasimple
T:gravitysphincsm
T:gravitysphincsl
T:sphincss128shake256simple
T:sphincss128shake256robust
T:sphincss128sha256robust
T:faestem256fv3
T:faestem192fv3
T:faestem128fv3
T:faest256fv3
T:faest192fv3
T:faest128fv3
T:faest256sv3
T:faest192sv3
T:faest128sv3
T:ecdonaldp224
T:ecdonaldp256
T:ecdonaldp521
T:ecdonaldp160
T:ecdonaldb163
T:ecdonaldk163
T:ecdonaldb233
T:ecdonaldk233
T:ecdonaldb571
T:ecdonaldk571
T:ed448goldilocks
T:picnic2l5fs
T:picnicl5ur
T:picnicl5full
T:picnic315
T:picnicl3fs
T:picnicl3ur
T:picnic313
T:picnicl3full
T:picnic2l3fs
T:picnicl1full
T:picnic311
T:picnicl1fs
T:picnicl1ur
T:picnic2l1fs
T:sphincsf128harakarobust
T:sphincsf128sha256simple
T:sphincsf128sha256robust
T:sphincsf128shake256simple
T:sphincsf128shake256robust
T:sphincsf128harakasimple
T:sphincsf192harakasimple
T:sphincsf192shake256robust
T:sphincsf192shake256simple
T:sphincsf256harakasimple
T:sphincsf256shake256robust
T:sphincsf256shake256simple
T:sphincsf256sha256robust
T:sphincsf256sha256simple
T:sphincsf256harakarobust
T:sphincsf192sha256robust
T:sphincsf192sha256simple
T:sphincsf192harakarobust
T:sphincsf192shake256simple
T:sphincsf192shake256robust
T:sphincsf192sha256simple
T:sphincsf192harakarobust
T:sphincsf192shake256simple
T:sphincsf192shake256robust
T:sphincsf192sha