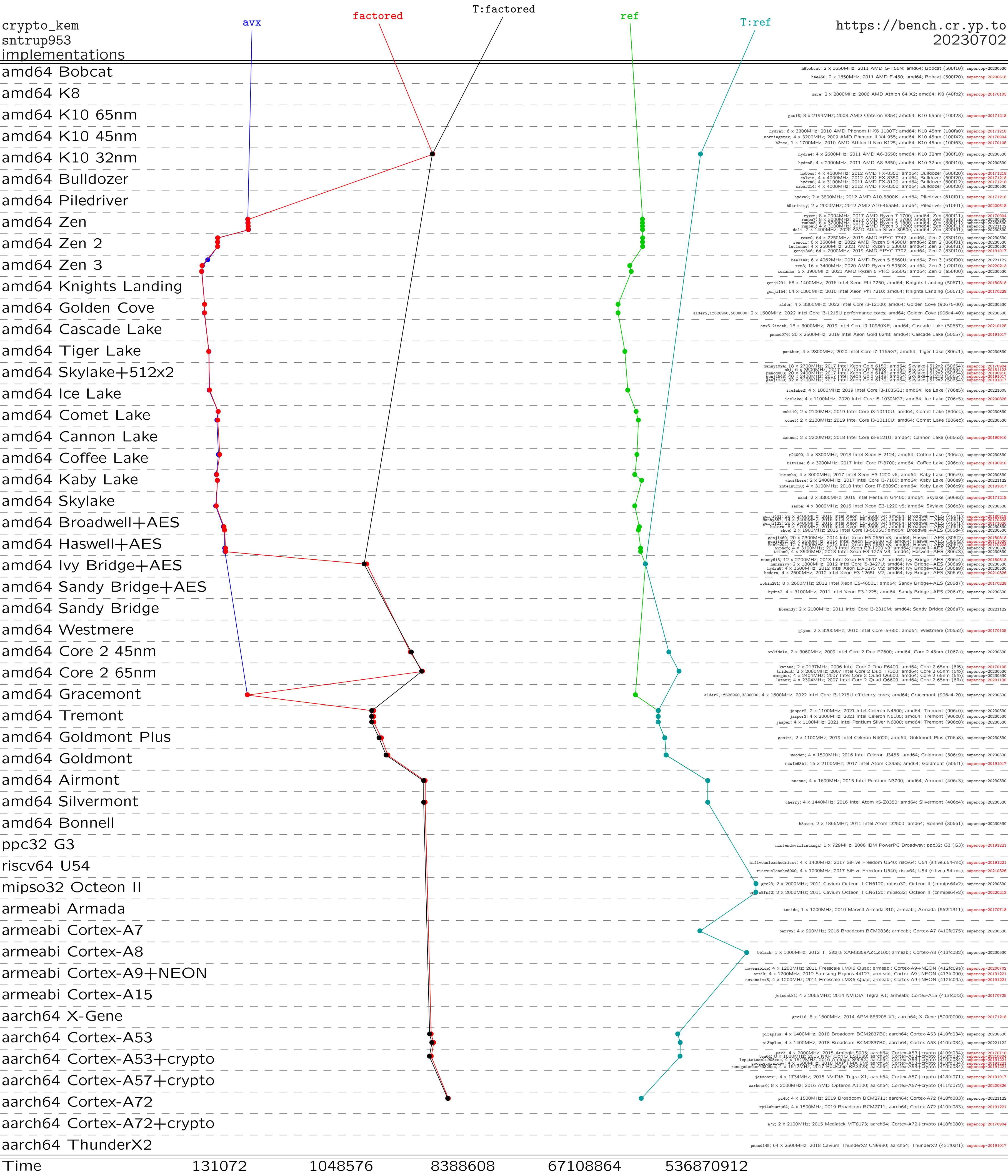
crypto_kem
sntrup953
implementations
https://bench.cr.yp.to
20230702
avx
factored
T:factored
ref
T:ref
amd64 Bobcat
h8bobcat; 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500f10); supercop-20230530
h4e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20200618
amd64 K8
mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20170105
amd64 K10 65nm
gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20171218
amd64 K10 45nm
hydra3; 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100fa0); supercop-20171218
morningstar; 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100f42); supercop-20170904
h3neo; 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20170105
amd64 K10 32nm
hydra4; 4 x 2600MHz; 2011 AMD A6-3650; amd64; K10 32nm (300f10); supercop-20230530
hydra5; 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20230530
amd64 Bulldozer
hobbes; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
calvin; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
hydra6; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20171218
saber214; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20230530
amd64 Piledriver
hydra9; 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); supercop-20171218
h9trinity; 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); supercop-20200618
amd64 Zen
ryzen; 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20170904
rumba7; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20230530
rumba5; 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); supercop-20230530
rumba3; 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); supercop-20221122
dali; 2 x 1400MHz; 2020 AMD Athlon Silver 3050e; amd64; Zen (820f01); supercop-20230530
amd64 Zen 2
rome0; 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830f10); supercop-20230530
renoir; 6 x 3600MHz; 2022 AMD Ryzen 5 4500U; amd64; Zen 2 (860f01); supercop-20230530
lucienne; 4 x 2600MHz; 2021 AMD Ryzen 3 5300U; amd64; Zen 2 (860f81); supercop-20230530
genji346; 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830f10); supercop-20191017
amd64 Zen 3
beelink; 6 x 4062MHz; 2021 AMD Ryzen 5 5560U; amd64; Zen 3 (a50f00); supercop-20221122
zen3; 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen 3 (a20f10); supercop-20220213
cezanne; 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (a50f00); supercop-20230530
amd64 Knights Landing
genji291; 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); supercop-20180818
genji154; 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; Knights Landing (50671); supercop-20170228
amd64 Golden Cove
alder; 4 x 3300MHz; 2022 Intel Core i3-12100; amd64; Golden Cove (90675-00); supercop-20230530
alder2,1f626960,5600000; 2 x 1600MHz; 2022 Intel Core i3-1215U performance cores; amd64; Golden Cove (906a4-40); supercop-20230530
amd64 Cascade Lake
avx512imath; 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; Cascade Lake (50657); supercop-20210125
pmnod076; 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); supercop-20191017
amd64 Tiger Lake
panther; 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercop-20230530
amd64 Skylake+512x2
manny1024; 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (50654); supercop-20170904
oki; 6 x 3500MHz; 2017 Intel Core i7-7800X; amd64; Skylake+512x2 (50654); supercop-20181123
pmnod003; 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; Skylake+512x2 (50654); supercop-20190910
genji548; 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; Skylake+512x2 (50654); supercop-20191017
genji239; 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; Skylake+512x2 (50654); supercop-20191017
amd64 Ice Lake
icelake2; 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; Ice Lake (706e5); supercop-20221005
icelake; 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; Ice Lake (706e5); supercop-20200826
amd64 Comet Lake
cubi10; 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230530
comet; 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230530
amd64 Cannon Lake
cannon; 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; Cannon Lake (60663); supercop-20190910
amd64 Coffee Lake
r24000; 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906ea); supercop-20230530
bitvise; 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906ea); supercop-20190910
amd64 Kaby Lake
kizomba; 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); supercop-20230530
whosthere; 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; Kaby Lake (806e9); supercop-20221122
intelnuci8; 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); supercop-20191017
amd64 Skylake
sand; 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); supercop-20171218
samba; 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); supercop-20230530
amd64 Broadwell+AES
genji441; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f1); supercop-20180818
manny357; 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f1); supercop-20170228
genji122; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f1); supercop-20171020
bolero; 8 x 1700MHz; 2016 Intel Xeon E5-2609 v4; amd64; Broadwell+AES (406f1); supercop-20230530
shoe; 2 x 1900MHz; 2015 Intel Core i3-5005U; amd64; Broadwell+AES (306d4); supercop-20230530
amd64 Haswell+AES
genji460; 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306f2); supercop-20180818
genji202; 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; Haswell+AES (306f2); supercop-20171020
robin204; 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; Haswell+AES (306f2); supercop-20170228
hiphop; 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; amd64; Haswell+AES (306c3); supercop-20230530
titan0; 4 x 3500MHz; 2013 Intel Xeon E3-1275 V3; amd64; Haswell+AES (306c3); supercop-20230530
amd64 Ivy Bridge+AES
manny613; 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; Ivy Bridge+AES (306e4); supercop-20180818
hunsnivy; 2 x 1800MHz; 2012 Intel Core i5-3427U; amd64; Ivy Bridge+AES (306a9); supercop-20230530
hydra8; 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; Ivy Bridge+AES (306a9); supercop-20230530
hedera; 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; Ivy Bridge+AES (306a9); supercop-20210326
amd64 Sandy Bridge+AES
robin281; 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; Sandy Bridge+AES (206d7); supercop-20170228
hydra7; 4 x 3100MHz; 2011 Intel Xeon E3-1225; amd64; Sandy Bridge+AES (206a7); supercop-20230530
amd64 Sandy Bridge
h6sandy; 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20221122
amd64 Westmere
glyme; 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20170105
amd64 Core 2 45nm
wolfdale; 2 x 3060MHz; 2009 Intel Core 2 Duo E7600; amd64; Core 2 45nm (1067a); supercop-20230530
amd64 Core 2 65nm
katana; 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; Core 2 65nm (6f6); supercop-20170105
trident; 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; Core 2 65nm (6fb); supercop-20230530
margaux; 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6fb); supercop-20230530
latour; 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6fb); supercop-20201130
amd64 Gracemont
alder2,1f626960,3300000; 4 x 1600MHz; 2022 Intel Core i3-1215U efficiency cores; amd64; Gracemont (906a4-20); supercop-20230530
amd64 Tremont
jasper2; 2 x 1100MHz; 2021 Intel Celeron N4500; amd64; Tremont (906c0); supercop-20230530
jasper3; 4 x 2000MHz; 2021 Intel Celeron N5105; amd64; Tremont (906c0); supercop-20230530
jasper; 4 x 1100MHz; 2021 Intel Pentium Silver N6000; amd64; Tremont (906c0); supercop-20230530
amd64 Goldmont Plus
gemini; 2 x 1100MHz; 2019 Intel Celeron N4020; amd64; Goldmont Plus (706a8); supercop-20230530
amd64 Goldmont
wooden; 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); supercop-20230530
scw1b63b1; 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017
amd64 Airmont
nucnuc; 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercop-20230530
amd64 Silvermont
cherry; 4 x 1440MHz; 2016 Intel Atom x5-Z8350; amd64; Silvermont (406c4); supercop-20230530
amd64 Bonnell
h8atom; 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Bonnell (30661); supercop-20230530
ppc32 G3
nintendowiilinuxngx; 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221
riscv64 U54
hifiveunleashedriscv; 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20191221
riscvunleashed000; 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20210326
mipso32 Octeon II
gcc23; 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnmips64v2); supercop-20230530
o8fsf2; 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnmips64v2); supercop-20220213
armeabi Armada
tonido; 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); supercop-20170718
armeabi Cortex-A7
berry2; 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410fc075); supercop-20230530
armeabi Cortex-A8
bblack; 1 x 1000MHz; 2012 TI Sitara XAM3359AZCZ100; armeabi; Cortex-A8 (413fc082); supercop-20230530
armeabi Cortex-A9+NEON
novenablue; 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercop-20200702
artik; 4 x 1200MHz; 2012 Samsung Exynos 4412?; armeabi; Cortex-A9+NEON (413fc090); supercop-20191221
novenaimx6; 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercop-20191221
armeabi Cortex-A15
jetsontk1; 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); supercop-20170725
aarch64 X-Gene
gcc116; 8 x 1600MHz; 2014 APM 883208-X1; aarch64; X-Gene (500f0000); supercop-20171218
aarch64 Cortex-A53
pi3aplus; 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410fd034); supercop-20230530
pi3bplus; 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410fd034); supercop-20221122
aarch64 Cortex-A53+crypto
par3; 4 x 2000MHz; 2015 Amlogic S905; aarch64; Cortex-A53+crypto (410fd034); supercop-20170718
ten64; 8 x 1600MHz; 2015 NXP QorIQ LS1088; aarch64; Cortex-A53+crypto (410fd034); supercop-20210604
lepotatoamls905xcc; 4 x 1512MHz; 2016 Amlogic S905X; aarch64; Cortex-A53+crypto (410fd034); supercop-20191221
googlecoraldev; 4 x 1500MHz; 2018 NXP i.MX 8M; aarch64; Cortex-A53+crypto (410fd034); supercop-20191221
renegaderocrk3328cc; 4 x 1512MHz; 2017 Rockchip RK3328; aarch64; Cortex-A53+crypto (410fd034); supercop-20191221
aarch64 Cortex-A57+crypto
jetsontx1; 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; Cortex-A57+crypto (418fd071); supercop-20191017
warbear0; 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (411fd072); supercop-20200826
aarch64 Cortex-A72
pi4b; 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410fd083); supercop-20221122
rpi4ubuntu64; 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410fd083); supercop-20191221
aarch64 Cortex-A72+crypto
a72; 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418fd080); supercop-20170904
aarch64 ThunderX2
pmnod145; 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0af1); supercop-20191017
Time
131072
1048576
8388608
67108864
536870912