

crypto_aead
aes128n8silcv1
implementations

T:ref

https://bench.cr.yp.to
20230702

amd64 Bobcat

amd64 K8

amd64 K10 65nm

amd64 K10 45nm

amd64 K10 32nm

amd64 Bulldozer

amd64 Piledriver

amd64 Zen

amd64 Zen 2

amd64 Zen 3

amd64 Knights Landing

amd64 Golden Cove

amd64 Cascade Lake

amd64 Tiger Lake

amd64 Skylake+512x2

amd64 Ice Lake

amd64 Comet Lake

amd64 Cannon Lake

amd64 Coffee Lake

amd64 Kaby Lake

amd64 Skylake

amd64 Broadwell+AES

amd64 Haswell+AES

amd64 Ivy Bridge+AES

amd64 Sandy Bridge+AES

amd64 Sandy Bridge

amd64 Westmere

amd64 Core 2 45nm

amd64 Core 2 65nm

amd64 Gracemont

amd64 Tremont

amd64 Goldmont Plus

amd64 Goldmont

amd64 Airmont

amd64 Silvermont

amd64 Bonnell

ppc32 G3

riscv64 U54

mipso32 Octeon II

armeabi Armada

armeabi Cortex-A7

armeabi Cortex-A8

armeabi Cortex-A9+NEON

armeabi Cortex-A15

aarch64 X-Gene

aarch64 Cortex-A53

aarch64 Cortex-A53+crypto

aarch64 Cortex-A57+crypto

aarch64 Cortex-A72

aarch64 Cortex-A72+crypto

aarch64 ThunderX2

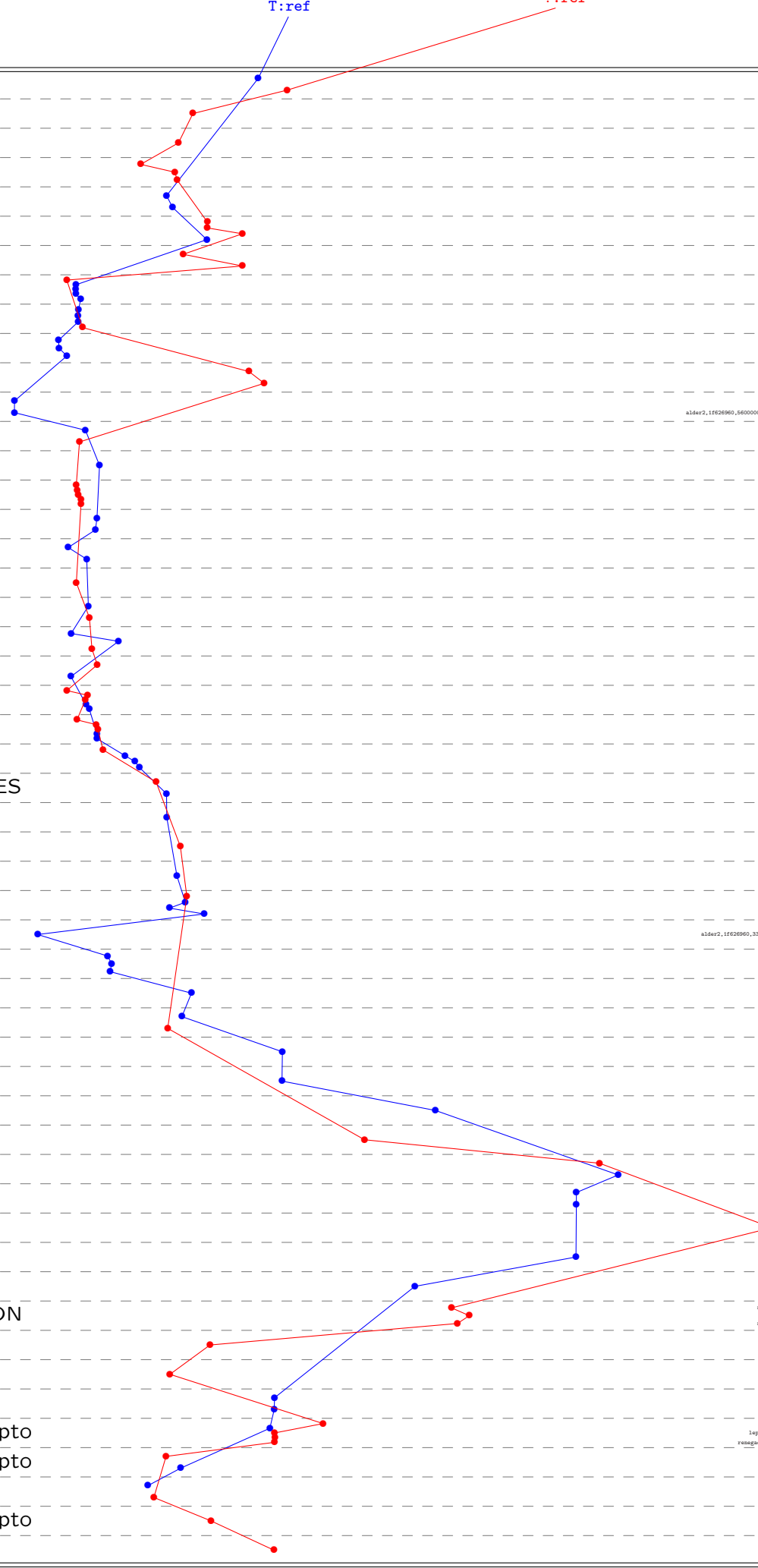
Time

131072

262144

524288

1048576



bbobcat: 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500F10); supercop-20230630
m4650: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500F20); supercop-20230618
naxc: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40f2); supercop-201710105
gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100F23); supercop-20171218
hydras3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100F40); supercop-20171218
sonnigstar: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100F42); supercop-20170904
h3max: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100F63); supercop-201710105
hydras4: 4 x 2600MHz; 2011 AMD A6-3650; amd64; K10 32nm (300F10); supercop-20230630
hydras5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); supercop-20230630
bobcat: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (500F20); supercop-20171218
calista: 4 x 4000MHz; 2012 AMD FX-8370; amd64; Bulldozer (500F20); supercop-20171218
hydras6: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (500F12); supercop-20171218
shaver215: 4 x 4000MHz; 2012 AMD FX-8360; amd64; Bulldozer (500F20); supercop-20230630
hydras7: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610F11); supercop-20171218
spriority: 2 x 2000MHz; 2012 AMD A10-6650M; amd64; Piledriver (610F11); supercop-20230618
regado: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800F11); supercop-20170865
regado: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800F11); supercop-20170865
regado: 4 x 3100MHz; 2017 AMD Ryzen 3 3100; amd64; Zen (800F11); supercop-20230630
regado: 4 x 3100MHz; 2017 AMD Ryzen 3 3100; amd64; Zen (800F11); supercop-20230630
dali: 2 x 1400MHz; 2019 AMD EPYC 7002; amd64; Zen 2 (830F10); supercop-20191017
regado: 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830F10); supercop-20230630
regado: 6 x 3000MHz; 2022 AMD Ryzen 5 8500U; amd64; Zen 2 (860F11); supercop-20230630
lacienne: 4 x 2600MHz; 2021 AMD Ryzen 5 5600G; amd64; Zen 2 (820F10); supercop-20230630
gwj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830F10); supercop-20191017
regado: 6 x 4062MHz; 2021 AMD Ryzen 5 5600G; amd64; Zen 3 (A50F00); supercop-20211122
swash: 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen 3 (A20F10); supercop-20220311
cezanne: 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (A50F00); supercop-20230630
gwj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); supercop-20180818
gwj1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; Knights Landing (50671); supercop-20170228
alder: 4 x 3300MHz; 2022 Intel Core i3-12100; amd64; Golden Cove (90673-00); supercop-20230630
alder1:1f62690,5600000; 2 x 1600MHz; 2022 Intel Core i3-1215U performance cores; amd64; Golden Cove (906A4-40); supercop-20230630
avx512mash: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; Cascade Lake (50657); supercop-20210126
penod076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); supercop-20191017
panther: 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercop-20230630
sanjay1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906A1); supercop-20170865
panther: 8 x 2500MHz; 2017 Intel Core i7-8750; amd64; Coffee Lake (906a4); supercop-201910105
sanjay1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906A1); supercop-20170865
sanjay1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906A1); supercop-20170865
sanjay1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906A1); supercop-20170865
sanjay1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906A1); supercop-20170865
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-20200626
cubio: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806c); supercop-20230630
cosat: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806c); supercop-20230630
cannon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; Cannon Lake (90663); supercop-20190910
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906a4); supercop-20230630
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906a4); supercop-20230630
r3000: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906a4); supercop-20190910
kozabwa: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); supercop-20230630
shoukhar: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; Kaby Lake (906e9); supercop-20211122
instalaur1: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); supercop-20191017
sanat: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); supercop-20171218
sanat: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); supercop-20230630
gem1461: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f); supercop-20180818
BanjoT72: 18 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f); supercop-20170228
BanjoT72: 18 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; Broadwell+AES (406f); supercop-20170228
bolshoi: 18 x 1700MHz; 2015 Intel Core i3-5005A; amd64; Broadwell+AES (506d4); supercop-20230630
bolshoi: 18 x 1700MHz; 2015 Intel Core i3-5005A; amd64; Broadwell+AES (506d4); supercop-20230630
gem1461: 20 x 2800MHz; 2014 Intel Xeon E5-2680 v3; amd64; Haswell+AES (306e2); supercop-20190910
Haswell: 12 x 2800MHz; 2012 Intel Xeon E5-2680 v2; amd64; Haswell+AES (306e2); supercop-20190910
Haswell: 12 x 2800MHz; 2012 Intel Xeon E5-2680 v2; amd64; Haswell+AES (306e2); supercop-20190910
Haswell: 4 x 3100MHz; 2013 Intel Xeon E3-1275 v2; amd64; Haswell+AES (306e2); supercop-20230630
Haswell: 4 x 3100MHz; 2013 Intel Xeon E3-1275 v2; amd64; Haswell+AES (306e2); supercop-20230630
Haswell: 4 x 3100MHz; 2013 Intel Xeon E3-1275 v2; amd64; Haswell+AES (306e2); supercop-20230630
Haswell: 4 x 3100MHz; 2013 Intel Xeon E3-1275 v2; amd64; Haswell+AES (306e2); supercop-20230630
Haswell: 4 x 3100MHz; 2013 Intel Xeon E3-1275 v2; amd64; Haswell+AES (306e2); supercop-20230630
Haswell: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; Ivy Bridge+AES (306e4); supercop-20180818
banjayv17: 2 x 1800MHz; 2012 Intel Core i5-3427U; amd64; Ivy Bridge+AES (306e4); supercop-20230630
hydras8: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; Ivy Bridge+AES (306e4); supercop-20230630
bedera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; Ivy Bridge+AES (306e4); supercop-20210326
robias281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; Sandy Bridge+AES (206d7); supercop-20170228
hydras7: 4 x 3100MHz; 2011 Intel Xeon E3-1225; amd64; Sandy Bridge+AES (206a7); supercop-20230630
hsandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20211122
glysw: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-201710105
voifdale: 2 x 3060MHz; 2009 Intel Core 2 Duo E7600; amd64; Core 2 45nm (1067a); supercop-20230630
katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; Core 2 65nm (6f6); supercop-201710105
teridan: 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; Core 2 65nm (6f6); supercop-20230630
nasgard: 4 x 2604MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); supercop-20230630
lalour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); supercop-20211030
alder1:1f62690,3300000; 4 x 1600MHz; 2022 Intel Core i3-1215U efficiency cores; amd64; Gracemont (906A4-20); supercop-20230630
jasper2: 2 x 1100MHz; 2021 Intel Celeron N4500; amd64; Tremont (906c0); supercop-20230630
jasper3: 4 x 2000MHz; 2021 Intel Celeron N5105; amd64; Tremont (906c0); supercop-20230630
jasper: 4 x 1100MHz; 2021 Intel Pentium Silver N6000; amd64; Tremont (906c0); supercop-20230630
gemiti: 2 x 1100MHz; 2019 Intel Celeron N4020; amd64; Goldmont Plus (706a8); supercop-20230630
wooden: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); supercop-20230630
soviM3h1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017
m3ccm: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercop-20230630
cherry: 4 x 1440MHz; 2016 Intel Atom i5-Z8350; amd64; Silvermont (406a4); supercop-20230630
bbaton: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Bonnell (306f1); supercop-20230630
alntendosilluzlang: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221
hifiveunleashedriscv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20191221
riscvunleashedmips0: 4 x 1000MHz; 2017 SiFive Freedom U540; mipso32; U54 (sifive,u54-mc); supercop-20210326
gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnips64v2); supercop-20230630
erpfroffaz2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnips64v2); supercop-20220213
tesdie: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); supercop-20170718
berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20230630
bnlack: 1 x 1000MHz; 2012 TI Sitara XAM3359A2CZ120; armeabi; Cortex-A8 (413fc082); supercop-20230630
novaelina: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20200702
artix: 4 x 1200MHz; 2012 Samsung Exynos 44127; armeabi; Cortex-A9+NEON (413f090); supercop-20191221
novaelina: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221
jatsosati: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); supercop-20170728
gcc16: 8 x 1600MHz; 2014 APM 883208-K1; aarch64; X-Gene (500F000); supercop-20171218
p3hapi4: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410f094); supercop-20230630
p3hapi4: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410f094); supercop-20211122
leeds: 4 x 1500MHz; 2015 ARMv8-A 5000; aarch64; Cortex-A53+crypto (410f094); supercop-201710105
leeds: 4 x 1500MHz; 2015 ARMv8-A 5000; aarch64; Cortex-A53+crypto (410f094); supercop-201710105
gogolacrasia: 4 x 1500MHz; 2016 NXP i.MX 8M; aarch64; Cortex-A53+crypto (410f094); supercop-20191221
reagadecheckidrac: 4 x 1820MHz; 2017 Rockchip RK3288; aarch64; Cortex-A53+crypto (410f094); supercop-20191221
jatsosati: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; Cortex-A57+crypto (418f071); supercop-20191017
varbear: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (411f072); supercop-20200626
pi4h: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20211122
rpi4batus64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20191221
a7: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418f080); supercop-20170904
jms0445: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0af1); supercop-20191017