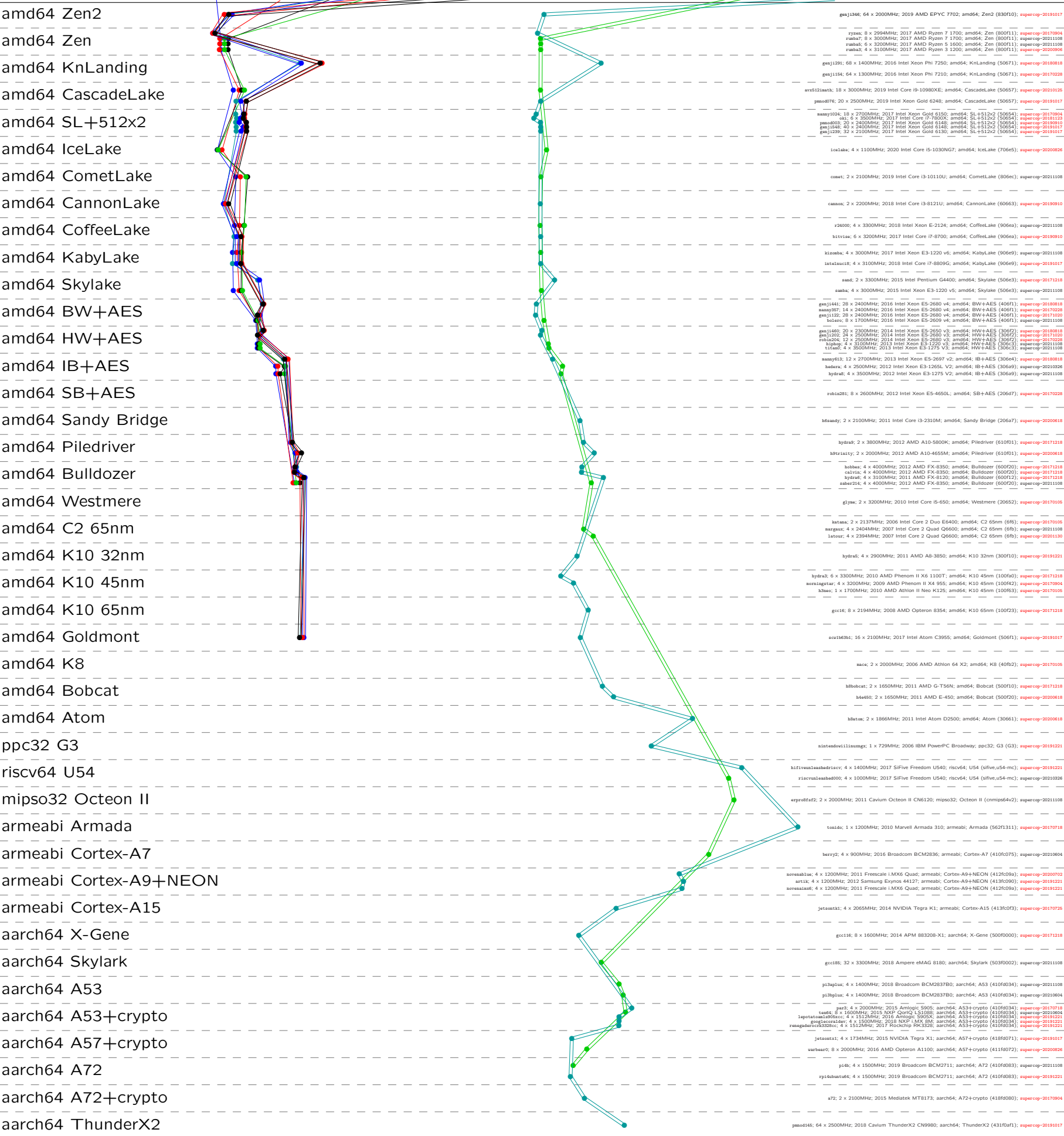


crypto_aead
aes128otrcv3
implementations



Time 8192 32768 131072 524288

gej1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830f10); [supercop-20191017](#)

ryzen: 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); [supercop-20170904](#)

ryabaf: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); [supercop-20211108](#)

ryabaf: 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); [supercop-20211108](#)

ryabaf: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); [supercop-20200908](#)

gej1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; KnLanding (50671); [supercop-20180818](#)

gej1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; KnLanding (50671); [supercop-20170228](#)

avx512iaatb: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; CascadeLake (50657); [supercop-20210126](#)

pmo0d76: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); [supercop-20191017](#)

aaay1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); [supercop-20170904](#)

aa1: 6 x 3500MHz; 2017 Intel Core i7-7800X; amd64; SL+512x2 (50654); [supercop-20181123](#)

pmo0p03: 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); [supercop-20190210](#)

gej11548: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); [supercop-20191017](#)

gej12919: 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; SL+512x2 (50654); [supercop-20211108](#)

iceLake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (70e05); [supercop-20200826](#)

comet: 2 x 2100MHz; 2019 Intel Core i9-10110U; amd64; CometLake (806ec); [supercop-20211108](#)

cannon: 2 x 2200MHz; 2018 Intel Core i9-8121U; amd64; CannonLake (60663); [supercop-20190910](#)

r2000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; CoffeeLake (906ea); [supercop-20211108](#)

bitvise: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); [supercop-20190101](#)

kiombo: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); [supercop-20211108](#)

intalcacii: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906e9); [supercop-20191017](#)

saad: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); [supercop-20171218](#)

saaba: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); [supercop-20211108](#)

gej1444: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); [supercop-20180818](#)

aaay087: 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); [supercop-20170228](#)

gej1122: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); [supercop-20171020](#)

bokaro: 8 x 1700MHz; 2016 Intel Xeon E5-2609 v5; amd64; BW+AES (406f1); [supercop-20211108](#)

gej1440: 20 x 2700MHz; 2014 Intel Xeon E5-2650 v3; amd64; HW+AES (306f2); [supercop-20180818](#)

gej1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (306f2); [supercop-20171020](#)

rihaz04: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v2; amd64; HW+AES (306f2); [supercop-20170228](#)

tipapq: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; amd64; HW+AES (306c3); [supercop-20211108](#)

11lavf: 4 x 3000MHz; 2013 Intel Xeon E3-1275 v3; amd64; HW+AES (306c3); [supercop-20211108](#)

aaay013: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306e4); [supercop-20180818](#)

bakera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; IB+AES (306e9); [supercop-20210326](#)

hydra8: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306e9); [supercop-20211108](#)

robis281: 8 x 2600MHz; 2012 Intel Xeon E5-4550L; amd64; SB+AES (206d7); [supercop-20170228](#)

h6aandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); [supercop-20200618](#)

hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); [supercop-20171218](#)

ibxriaty: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); [supercop-20200618](#)

bobba: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); [supercop-20171218](#)

calvix: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); [supercop-20171218](#)

hydra4: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); [supercop-20171218](#)

saber216: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); [supercop-20211108](#)

glywa: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); [supercop-20170105](#)

kataaa: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); [supercop-20170105](#)

naqaaa: 4 x 2940MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); [supercop-20211108](#)

laxou: 4 x 2940MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); [supercop-20211108](#)

hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); [supercop-20191221](#)

hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f60); [supercop-20171218](#)

wonjager: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100f42); [supercop-20170904](#)

hbaaa: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); [supercop-20170105](#)

gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); [supercop-20171218](#)

scv163b1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); [supercop-20191017](#)

naaa: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); [supercop-20170105](#)

hbobcat: 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500f10); [supercop-20171218](#)

h4e50: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); [supercop-20200618](#)

h8aaa: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (306e1); [supercop-20200618](#)

nintendowilliauzag: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); [supercop-20191221](#)

hifiveuaeasdrscv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); [supercop-20191221](#)

riscvuaaah8000: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); [supercop-20210326](#)

eprofzsf2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips32; Octeon II (cnnip64v2); [supercop-20211108](#)

tasido: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); [supercop-20170718](#)

berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); [supercop-20210604](#)

soveaa1w: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); [supercop-20200702](#)

artik: 4 x 1200MHz; 2012 Samsung Exynos 4412?; armeabi; Cortex-A9+NEON (413f090); [supercop-20191221](#)

soveaa1a6: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); [supercop-20191221](#)

jetsotst1: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); [supercop-20170725](#)

gcc116: 8 x 1600MHz; 2014 APM 883208-X1; aarch64; X-Gene (500f000); [supercop-20171218](#)

gcc118: 32 x 3300MHz; 2018 Ampere eMAG 8180; aarch64; Skylark (503f002); [supercop-20211108](#)

pi3aplus: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); [supercop-20211108](#)

pi3plus: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); [supercop-20210604](#)

pi4b: 4 x 2000MHz; 2016 Amlogic S905; aarch64; A53+crypto (410f034); [supercop-20170718](#)

twaa8: 8 x 1200MHz; 2015 NXP QorIQ LS1088; aarch64; A53+crypto (410f034); [supercop-20210604](#)

1egottaa19f8aa: 4 x 1512MHz; 2016 Amlogic S905; aarch64; A53+crypto (410f034); [supercop-20191221](#)

geopicoa1a0v: 4 x 1500MHz; 2018 NXP i.MX 8M; aarch64; A53+crypto (410f034); [supercop-20191221](#)

renegea1cck328cc: 4 x 1512MHz; 2017 Rockchip RK3328; aarch64; A53+crypto (410f034); [supercop-20191221](#)

jetsotxt1: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; A57+crypto (418f071); [supercop-20191017](#)

varbear0: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; A57+crypto (411f072); [supercop-20200826](#)

pi4b: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); [supercop-20211108](#)

rpi4babaatua6: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); [supercop-20191221](#)

a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); [supercop-20170904](#)

pmo0145: 64 x 2500MHz; 2018 Cavium ThunderX2 CN980; aarch64; ThunderX2 (431f0f1); [supercop-20191017](#)