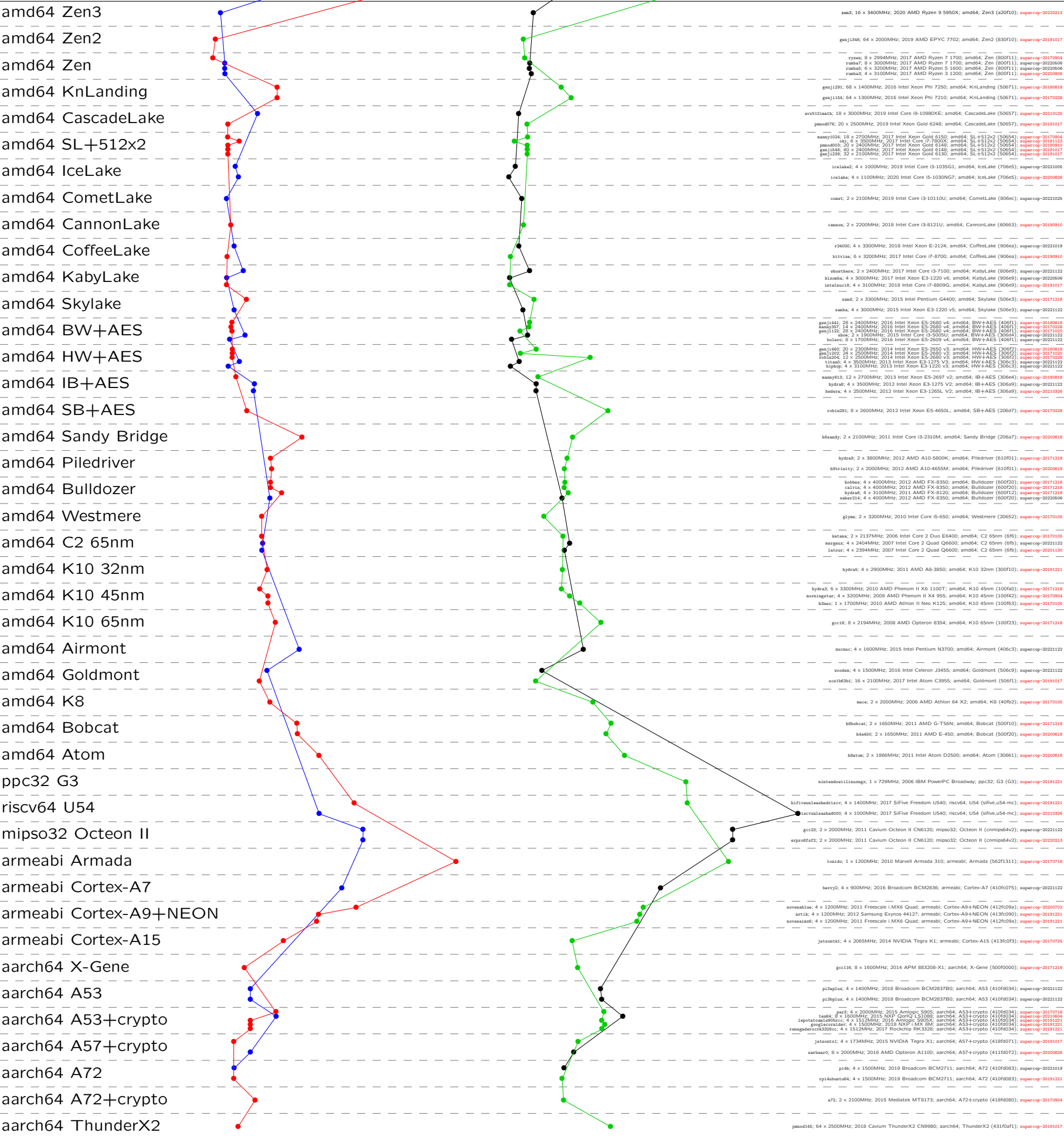


crypto_aead
acorn128v2
implementations



Time 65536 524288 4194304 33554432

zen3: 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen3 (a20f10); [supercop-20220213](#)

genj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830f10); [supercop-20191017](#)

ryzen: 8 x 3994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); [supercop-20170904](#)

ruab7: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); [supercop-20220606](#)

ruab8: 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); [supercop-20220808](#)

ruab9: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); [supercop-2021122](#)

genj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; KnLanding (50671); [supercop-20180818](#)

genj1184: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; KnLanding (50671); [supercop-20170228](#)

vr512naht: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; CascadeLake (50657); [supercop-20210126](#)

pm6d76: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); [supercop-20191017](#)

maany1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); [supercop-20170904](#)

ma4: 6 x 3500MHz; 2017 Intel Core i7-7600U; amd64; SL+512x2 (50654); [supercop-20181123](#)

pm6a003: 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); [supercop-20190910](#)

genj1858: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); [supercop-20190910](#)

genj1239: 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; SL+512x2 (50654); [supercop-20191017](#)

icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; IceLake (706e5); [supercop-20221005](#)

icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (706e5); [supercop-20220826](#)

comet: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; CometLake (806ec); [supercop-20221025](#)

canon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; CannonLake (50663); [supercop-20190910](#)

r2400: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; CoffeeLake (906ea); [supercop-20221019](#)

btv156: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); [supercop-20190910](#)

whothere: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; KabyLake (806e9); [supercop-20221122](#)

kiabaa: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); [supercop-20220606](#)

inteluc18: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906e9); [supercop-20191017](#)

saad: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506c3); [supercop-20171218](#)

saaba: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506c3); [supercop-20221122](#)

genj1441: 28 x 2400MHz; 2018 Intel Xeon E3-2880 v4; amd64; HW+AES (406f1); [supercop-20180818](#)

ma4027: 14 x 2400MHz; 2016 Intel Xeon E3-2880 v4; amd64; HW+AES (406f1); [supercop-20171027](#)

genj1122: 24 x 2400MHz; 2015 Intel Xeon E3-2880 v4; amd64; HW+AES (406f1); [supercop-20171027](#)

saab: 2 x 1900MHz; 2015 Intel Core i5-5050U; amd64; HW+AES (306c4); [supercop-20221122](#)

belara: 8 x 1700MHz; 2016 Intel Xeon E3-2659 v4; amd64; HW+AES (406f1); [supercop-20221122](#)

genj1462: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v2; amd64; HW+AES (306f2); [supercop-20180818](#)

genj1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (306f2); [supercop-20171020](#)

rob3348: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (306f2); [supercop-20171020](#)

ttiaad: 4 x 3500MHz; 2013 Intel Xeon E3-1220 v5; amd64; HW+AES (306c3); [supercop-20221122](#)

hisp6: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v5; amd64; HW+AES (306c3); [supercop-20221122](#)

maany151: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306c4); [supercop-20180818](#)

hydra4: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306a9); [supercop-20221122](#)

belara: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; IB+AES (306a9); [supercop-20210326](#)

rob1281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; SB+AES (206d7); [supercop-20170228](#)

hfsaandy: 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](#)

h3trinity: 2 x 3000MHz; 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](#)

hydra6: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); [supercop-20171218](#)

hawz16: 4 x 4000MHz; 2012 AMD FX-8360; amd64; Bulldozer (600f20); [supercop-20220606](#)

gl5w: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); [supercop-20171016](#)

katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); [supercop-20171016](#)

nargas: 4 x 2040MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); [supercop-20221122](#)

latour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); [supercop-20201130](#)

hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); [supercop-20141221](#)

hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100fa0); [supercop-20171218](#)

sonnigstar: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100fa2); [supercop-20170904](#)

h3aa: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); [supercop-20171016](#)

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

maacu: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); [supercop-20221122](#)

voodon: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); [supercop-20221122](#)

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

nac: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); [supercop-20171016](#)

hbobcat: 2 x 1650MHz; 2011 AMD G-T56n; amd64; Bobcat (500f10); [supercop-20171218](#)

h4450: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); [supercop-20200618](#)

hlaton: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (30661); [supercop-20200618](#)

nintendov111aunag: 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](#)

scv16aahad000: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); [supercop-20210326](#)

gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips64; Octeon II (cmnrips64v2); [supercop-20221122](#)

egrf0afz2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips64; Octeon II (cmnrips64v2); [supercop-20220213](#)

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

berry2: 4 x 900MHz; 2016 Broadcom BCM2835; armeabi; Cortex-A7 (410f075); [supercop-20221122](#)

soveeah1w: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); [supercop-20200702](#)

ar1x: 4 x 1200MHz; 2012 Samsung Exynos 4412; armeabi; Cortex-A9+NEON (413f090); [supercop-20191221](#)

soveeah2w: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); [supercop-20191221](#)

jtsaontz1: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); [supercop-20170725](#)

gcc114: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gen (500f000); [supercop-20171218](#)

pi36plu: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); [supercop-20221122](#)

pi36plu: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); [supercop-20221122](#)

par3: 4 x 2000MHz; 2015 Amlogic S905; aarch64; A53+crypto (410f034); [supercop-20170718](#)

teuf4: 8 x 1400MHz; 2015 Amlogic S905; aarch64; A53+crypto (410f034); [supercop-20170718](#)

lepotasoa19Risc: 4 x 1121MHz; 2016 Amlogic S905X; aarch64; A53+crypto (410f034); [supercop-20191221](#)

gongkacra1w: 4 x 1500MHz; 2017 Rockchip RK3328; aarch64; A53+crypto (410f034); [supercop-20191221](#)

rengadecrc8328c: 4 x 1512MHz; 2017 Rockchip RK3328; aarch64; A53+crypto (410f034); [supercop-20191221](#)

jtsaontz1: 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-20200626](#)

pi4b: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); [supercop-20221019](#)

rpi4buntu64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); [supercop-20191221](#)

ar2: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); [supercop-20170904](#)

pm6d145: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431fa1f1); [supercop-20191017](#)