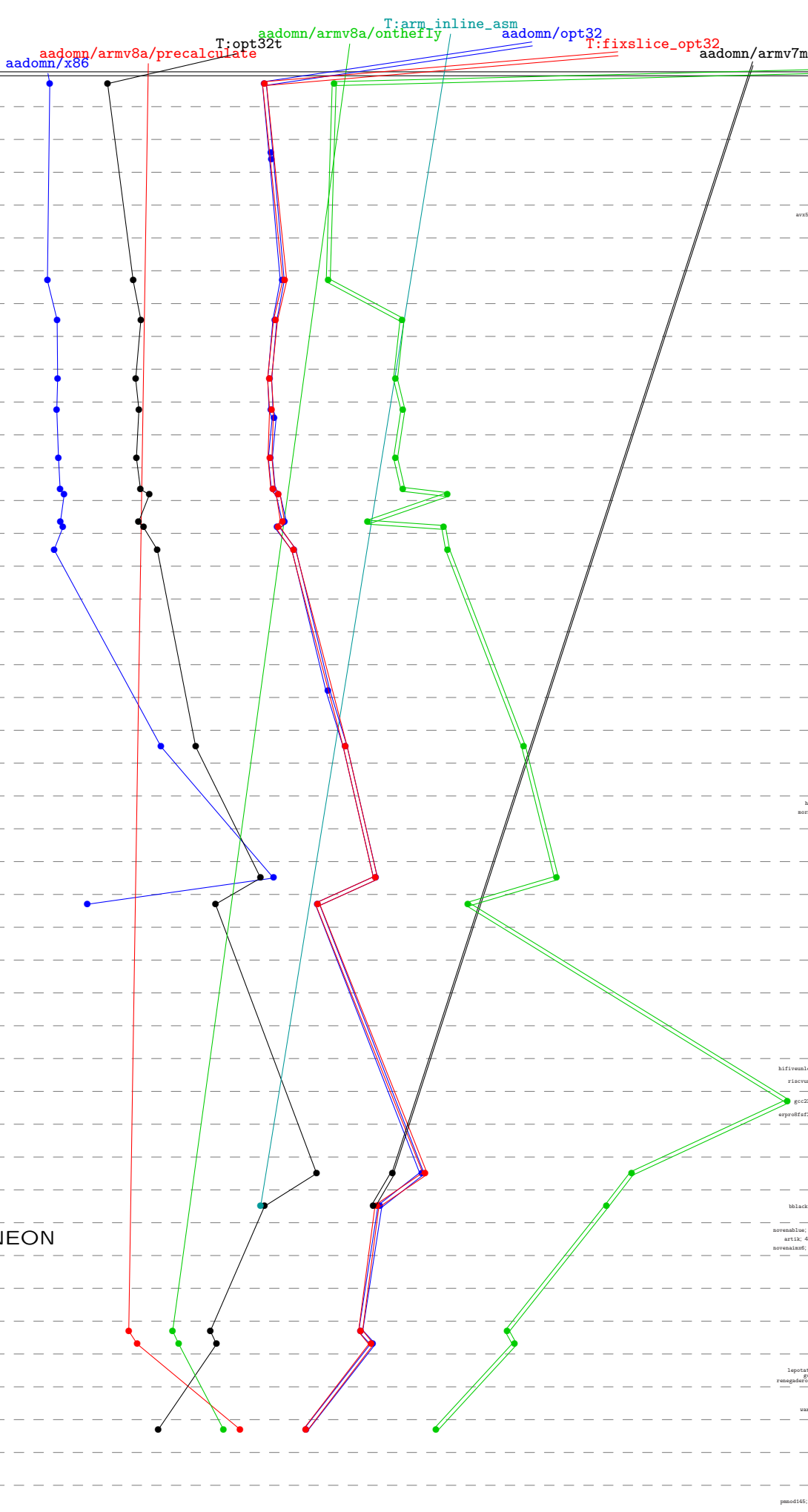


crypto_aead
romulusn
implementations

amd64 Zen3
amd64 Zen2
amd64 Zen
amd64 KnLanding
amd64 CascadeLake
amd64 SL+512x2
amd64 IceLake
amd64 CometLake
amd64 CannonLake
amd64 CoffeeLake
amd64 KabyLake
amd64 Skylake
amd64 BW+AES
amd64 HW+AES
amd64 IB+AES
amd64 SB+AES
amd64 Sandy Bridge
amd64 Piledriver
amd64 Bulldozer
amd64 Westmere
amd64 C2 65nm
amd64 K10 32nm
amd64 K10 45nm
amd64 K10 65nm
amd64 Airmont
amd64 Goldmont
amd64 K8
amd64 Bobcat
amd64 Atom
ppc32 G3
riscv64 U54
mips32 Oction II
armeabi Armada
armeabi Cortex-A7
armeabi Cortex-A8
armeabi Cortex-A9+NEON
armeabi Cortex-A15
aarch64 X-Gene
aarch64 A53
aarch64 A53+crypto
aarch64 A57+crypto
aarch64 A72
aarch64 A72+crypto
aarch64 ThunderX2



Time 262144 1048576 4194304

bealiak: 6 x 4062MHz; 2021 AMD Ryzen 5 5600U; amd64; Zen3 (a50f00); supercop-20221122

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

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

ryuab7: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20220606

ryuab6: 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); supercop-20220606

ryuab3: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); supercop-20200906

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

avx512aath: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; CascadeLake (50657); supercop-20210126

pmo0876: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); supercop-20191017

aanay1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654)

phl: 6 x 3500MHz; 2017 Intel Core i7-7800X; amd64; SL+512x2 (50654)

aanay003: 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; BW+AES (50654)

gej1158: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654)

gej1338: 32 x 2100MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654)

icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; IceLake (706e5); supercop-20221008

icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (706e5); supercop-20200626

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

cannon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; CannonLake (60663); supercop-20191010

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

bitvisie: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); supercop-20191010

shorthera: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; KabyLake (806ef); supercop-20221122

kiwoha: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906ef); supercop-20220606

intellanc8: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906ef); supercop-20191017

saat: 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

gej1441: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (40611); supercop-20180818

aanay007: 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (40611); supercop-20170228

gej1122: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (40611); supercop-20171020

bealiak8: 8 x 1500MHz; 2015 Intel Xeon E5-2680 v4; amd64; BW+AES (40611); supercop-20221122

bealiak9: 8 x 1100MHz; 2015 Intel Xeon E5-2680 v4; amd64; BW+AES (40611); supercop-20221122

gej1462: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v4; amd64; HW+AES (30627); supercop-20180818

gej1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v4; amd64; HW+AES (30627); supercop-20171020

rihazak4: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v4; amd64; HW+AES (30627); supercop-20171020

tiitaa4: 4 x 3500MHz; 2013 Intel Xeon E3-1275 V2; amd64; HW+AES (306c3); supercop-20221122

kiwoha2: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v5; amd64; HW+AES (306c3); supercop-20221122

aanay113: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306c4); supercop-20180818

hydra8: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306a9); supercop-20221122

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

robi281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; SB+AES (206d7); supercop-20170228

hfaandy: 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

btbristay2: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); supercop-20200618

bbobos: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218

calviss: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218

hydra5: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20171218

ab4r214: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20220606

glywa: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20171010

katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20171010

nargaus: 4 x 2404MHz; 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-20211018

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

hydra6: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f50); supercop-20171218

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

h3wo: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20171010

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

mucacc: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercop-20221122

voodea: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); supercop-20221122

scv1M3b1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017

sacc: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20171010

bBobcat: 2 x 1650MHz; 2011 AMD G-T56M; amd64; Bobcat (500f10); supercop-20171218

h4e40: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20200618

hlatas: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (306f1); supercop-20200618

nintendowilliamszgs: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221

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

riscvuaashad800: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20210326

gcc23: 2 x 2000MHz; 2011 Cavium Oction II CN6120; mips32; Oction II (cnmips64v2); supercop-20221122

eygroffafz2: 2 x 2000MHz; 2011 Cavium Oction II CN6120; mips32; Oction II (cnmips64v2); supercop-20220213

tonisdo: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); supercop-20170718

berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20221122

tblack: 1 x 1000MHz; 2012 TI Sitara XAM3359AZC2100; armeabi; Cortex-A8 (413f082); supercop-20221005

norveablus: 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

norveasaa5: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221

jetsonat1: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); supercop-20170725

gcc16: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500f000); supercop-20171218

pi3plus: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); supercop-20221122

pi3plus: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); supercop-20221122

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

tanu4: 8 x 1600MHz; 2015 NXP QorIQ LS1088; aarch64; A53+crypto (410f034); supercop-20190604

1epotatosu9f8cc: 4 x 1312MHz; 2016 Amlogic S905X; aarch64; A53+crypto (410f034); supercop-20191221

congaccara1aw: 4 x 1500MHz; 2018 NXP i.MX 8M; aarch64; A53+crypto (410f034); supercop-20191221

rengadesferc388cc: 4 x 1312MHz; 2017 Rockchip RK3288; aarch64; A53+crypto (410f034); supercop-20191221

jetsonat1: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; A57+crypto (418f071); supercop-20191017

warbaar0: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; A57+crypto (418f072); supercop-20200626

pi4b: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20221122

rp148butsu4: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20191221

a7: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); supercop-20170904

pmo4146: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9800; aarch64; ThunderX2 (431f0a1); supercop-20191017