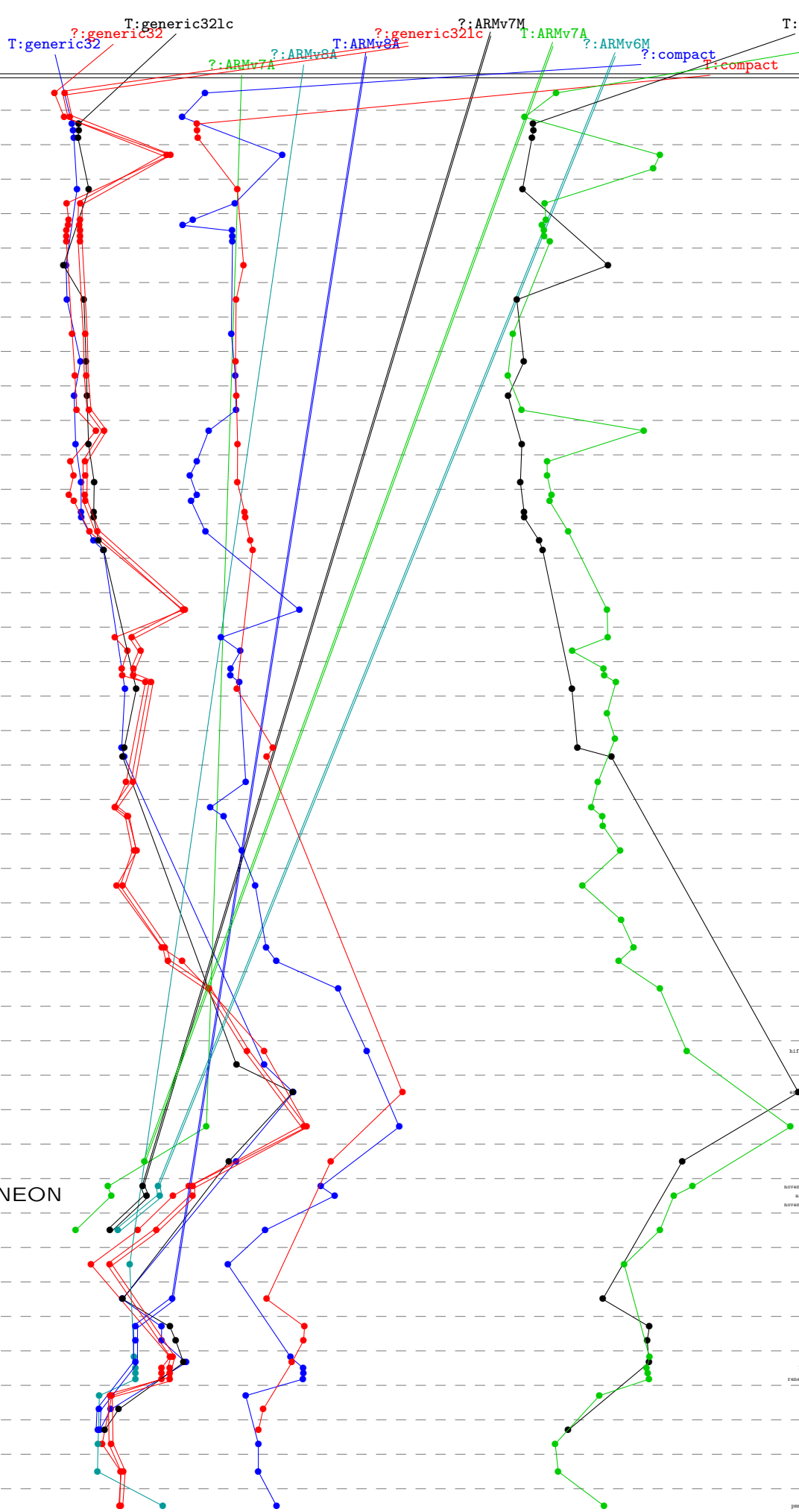


crypto_aead
ketjeminorv2
implementations

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 Goldmont
amd64 K8
amd64 Bobcat
amd64 Atom
ppc32 G3
riscv64 U54
mips32 Oocton II
armeabi Armada
armeabi Cortex-A7
armeabi Cortex-A9+NEON
armeabi Cortex-A15
aarch64 X-Gene
aarch64 Skylark
aarch64 A53
aarch64 A53+crypto
aarch64 A57+crypto
aarch64 A72
aarch64 A72+crypto
aarch64 ThunderX2



genj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830f10); supercop-20191017
ryzae: 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20170904
rubaat: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20191018
ruba6: 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); supercop-2011108
ruba3: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); supercop-20200908
genj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; KnLanding (50671); supercop-20180818
genj1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; KnLanding (50671); supercop-201910229
avx512iaah: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; CascadeLake (50657); supercop-20210126
pmsd076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); supercop-20191017
naany1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); supercop-20170904
u41: 6 x 3500MHz; 2017 Intel Core i7-7850X; amd64; SL+512x2 (50654); supercop-20181123
pms003: 20 x 2400MHz; 2016 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017
genj1158: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017
genj1239: 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; SL+512x2 (50654); supercop-20191017
leolake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (706e5); 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
r2400: 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-20190910
kizomba: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); supercop-20211108
intelasci: 4 x 3100MHz; 2018 Intel Xeon E3-1220 v5; amd64; KabyLake (906e9); supercop-20191017
sant: 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
genj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20180818
naany087: 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20190228
genj1122: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20171020
bakara: 8 x 1700MHz; 2016 Intel Xeon E5-2609 v5; amd64; BW+AES (406f1); supercop-20211108
genj1440: 20 x 2300MHz; 2016 Intel Xeon E5-2650 v4; amd64; HW+AES (306f2); supercop-20180818
genj1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v2; amd64; HW+AES (306f2); supercop-20171020
rifa204: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v2; amd64; HW+AES (306f2); supercop-20171020
bitpap: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; amd64; HW+AES (306c3); supercop-20211108
111aw: 4 x 3000MHz; 2013 Intel Xeon E3-1275 v2; amd64; HW+AES (306c3); supercop-20211108
naany113: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306f4); supercop-20180818
bakera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; IB+AES (306a9); supercop-20210326
hydra: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306a9); supercop-20211108
robis281: 8 x 2600MHz; 2012 Intel Xeon E5-4500L; amd64; SB+AES (206d7); supercop-20190228
h6aandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20200618
hydra: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); supercop-20171218
lbrxyati: 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
calvia: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
hydra: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20171218
saber214: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20211108
glyna: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20170105
katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20170105
nagasa: 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20211108
laxor: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20211108
hydra: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20191221
hydra: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f60); supercop-20171218
wenziger: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100f42); supercop-20170904
hbae: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20191005
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
naca: 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
hbatca: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (306e1); supercop-20200618
nintendovillainuzg: 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
riscvunleashed000: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20210326
tdsido: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); supercop-20170178
berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20210604
sorevaab1w: 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 (413f09c); supercop-20191221
sorevaiaa6: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221
jetsotat: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); supercop-20170725
gcc116: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500f000); supercop-20171218
gcc185: 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
jw8: 4 x 2000MHz; 2016 Amlogic S905; aarch64; A53+crypto (410f034); supercop-20170718
twaa8: 8 x 1600MHz; 2015 NXP QorIQ LS1088; aarch64; A53+crypto (410f034); supercop-20210604
1epstataa19fba: 4 x 1500MHz; 2016 Amlogic S905; aarch64; A53+crypto (410f034); supercop-20191221
geoplicoraidr: 4 x 1500MHz; 2018 NXP i.MX 8M; aarch64; A53+crypto (410f034); supercop-20191221
rmeagelcckk328cc: 4 x 1512MHz; 2017 Rockchip RK3328; aarch64; A53+crypto (410f034); supercop-20191221
jetsotaxi: 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
rpi4buntu64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20191221
a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); supercop-20170904
pmsd145: 64 x 2500MHz; 2018 Cavium ThunderX2 CN980; aarch64; ThunderX2 (431f0a1); supercop-20191017

Time 65536 262144 1048576 4194304 16777216