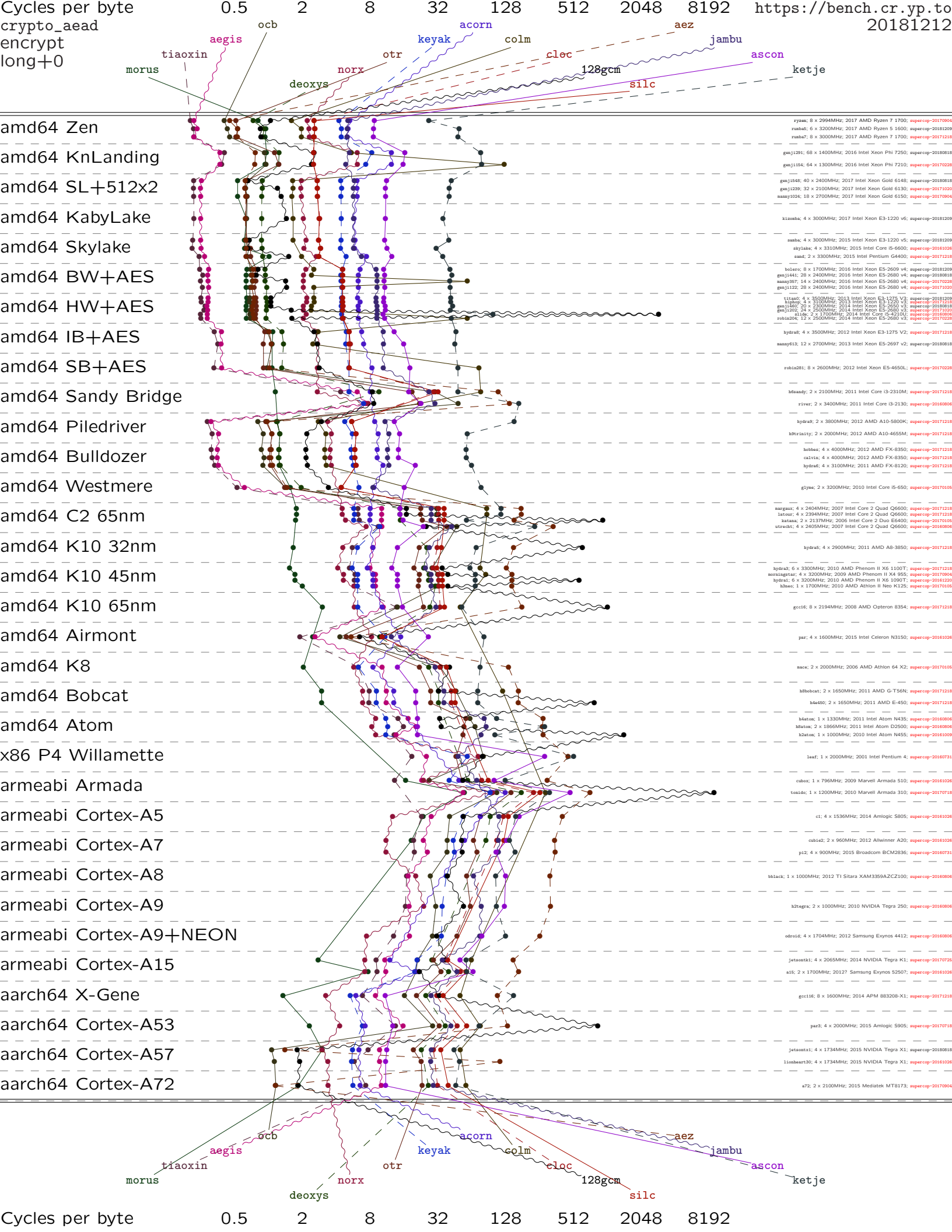
Cycles per byte
0.5
2
8
32
128
512
2048
8192
https://bench.cr.yp.to
20181212
crypto_aead
encrypt
long+0
ocb
acorn
aez
aegis
keyak
colm
jambu
tiaoxin
otr
cloc
ascon
morus
norx
128gcm
ketje
deoxys
silc
amd64 Zen
amd64 KnLanding
amd64 SL+512x2
amd64 KabyLake
amd64 Skylake
amd64 BW+AES
amd64 HW+AES
amd64 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 K8
amd64 Bobcat
amd64 Atom
x86 P4 Willamette
armeabi Armada
armeabi Cortex-A5
armeabi Cortex-A7
armeabi Cortex-A8
armeabi Cortex-A9
armeabi Cortex-A9+NEON
armeabi Cortex-A15
aarch64 X-Gene
aarch64 Cortex-A53
aarch64 Cortex-A57
aarch64 Cortex-A72
ryzen; 8 x 2994MHz; 2017 AMD Ryzen 7 1700; supercop-20170904
rumba5; 6 x 3200MHz; 2017 AMD Ryzen 5 1600; supercop-20181209
rumba7; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; supercop-20171218
genji291; 68 x 1400MHz; 2016 Intel Xeon Phi 7250; supercop-20180818
genji154; 64 x 1300MHz; 2016 Intel Xeon Phi 7210; supercop-20170228
genji548; 40 x 2400MHz; 2017 Intel Xeon Gold 6148; supercop-20180818
genji239; 32 x 2100MHz; 2017 Intel Xeon Gold 6130; supercop-20171020
manny1024; 18 x 2700MHz; 2017 Intel Xeon Gold 6150; supercop-20170904
kizomba; 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; supercop-20181209
samba; 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; supercop-20181209
skylake; 4 x 3310MHz; 2015 Intel Core i5-6600; supercop-20161026
saad; 2 x 3300MHz; 2015 Intel Pentium G4400; supercop-20171218
belzero; 8 x 1700MHz; 2016 Intel Xeon E5-2609 v4; supercop-20181209
genji441; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; supercop-20180818
manny357; 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; supercop-20170228
genji122; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; supercop-20171020
titan0; 4 x 3500MHz; 2013 Intel Xeon E3-1275 V3; supercop-20181209
kinkop; 4 x 3100MHz; 2013 Intel Xeon E3-1225 v3; supercop-20171218
genji460; 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; supercop-20180818
genji202; 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; supercop-20171020
alide; 2 x 1700MHz; 2014 Intel Core i5-4210U; supercop-20160806
robin204; 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; supercop-20170228
hydra8; 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; supercop-20171218
manny613; 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; supercop-20180818
robin281; 8 x 2600MHz; 2012 Intel Xeon E5-4650L; supercop-20170228
h6sandy; 2 x 2100MHz; 2011 Intel Core i3-2310M; supercop-20171218
river; 2 x 3400MHz; 2011 Intel Core i3-2130; supercop-20160806
hydra9; 2 x 3800MHz; 2012 AMD A10-5800K; supercop-20171218
h9trinity; 2 x 2000MHz; 2012 AMD A10-4655M; supercop-20171218
hobbes; 4 x 4000MHz; 2012 AMD FX-8350; supercop-20171218
calvin; 4 x 4000MHz; 2012 AMD FX-8350; supercop-20171218
hydra6; 4 x 3100MHz; 2011 AMD FX-8120; supercop-20171218
glyme; 2 x 3200MHz; 2010 Intel Core i5-650; supercop-20170105
margaux; 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; supercop-20171218
latour; 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; supercop-20171218
katana; 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; supercop-20170105
utrecht; 4 x 2405MHz; 2007 Intel Core 2 Quad Q6600; supercop-20160806
hydra5; 4 x 2900MHz; 2011 AMD A8-3850; supercop-20171218
hydra3; 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; supercop-20171218
morningstar; 4 x 3200MHz; 2009 AMD Phenom II X4 955; supercop-20170904
hydra1; 6 x 3200MHz; 2010 AMD Phenom II X6 1090T; supercop-20161220
h3sac; 1 x 1700MHz; 2010 AMD Athlon II Neo K125; supercop-20170105
gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; supercop-20171218
par; 4 x 1600MHz; 2015 Intel Celeron N3150; supercop-20161026
mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; supercop-20170105
h8bobcat; 2 x 1650MHz; 2011 AMD G-T56N; supercop-20171218
h4e450; 2 x 1650MHz; 2011 AMD E-450; supercop-20171218
h4atom; 1 x 1330MHz; 2011 Intel Atom N435; supercop-20160806
h8atom; 2 x 1866MHz; 2011 Intel Atom D2500; supercop-20160806
h2atom; 1 x 1000MHz; 2010 Intel Atom N455; supercop-20161009
leaf; 1 x 2000MHz; 2001 Intel Pentium 4; supercop-20160731
cubox; 1 x 796MHz; 2009 Marvell Armada 510; supercop-20161026
tonido; 1 x 1200MHz; 2010 Marvell Armada 310; supercop-20170718
c1; 4 x 1536MHz; 2014 Amlogic S805; supercop-20161026
cubie2; 2 x 960MHz; 2012 Allwinner A20; supercop-20161026
pi2; 4 x 900MHz; 2015 Broadcom BCM2836; supercop-20160731
bblack; 1 x 1000MHz; 2012 TI Sitara XAM3359AZCZ100; supercop-20160806
h2tegra; 2 x 1000MHz; 2010 NVIDIA Tegra 250; supercop-20160806
odroid; 4 x 1704MHz; 2012 Samsung Exynos 4412; supercop-20160806
jetsontk1; 4 x 2065MHz; 2014 NVIDIA Tegra K1; supercop-20170725
a15; 2 x 1700MHz; 2012? Samsung Exynos 5250?; supercop-20161026
gcc116; 8 x 1600MHz; 2014 APM 883208-X1; supercop-20171218
par3; 4 x 2000MHz; 2015 Amlogic S905; supercop-20170718
jetsontx1; 4 x 1734MHz; 2015 NVIDIA Tegra X1; supercop-20180818
lionheart30; 4 x 1734MHz; 2015 NVIDIA Tegra X1; supercop-20161026
a72; 2 x 2100MHz; 2015 Mediatek MT8173; supercop-20170904