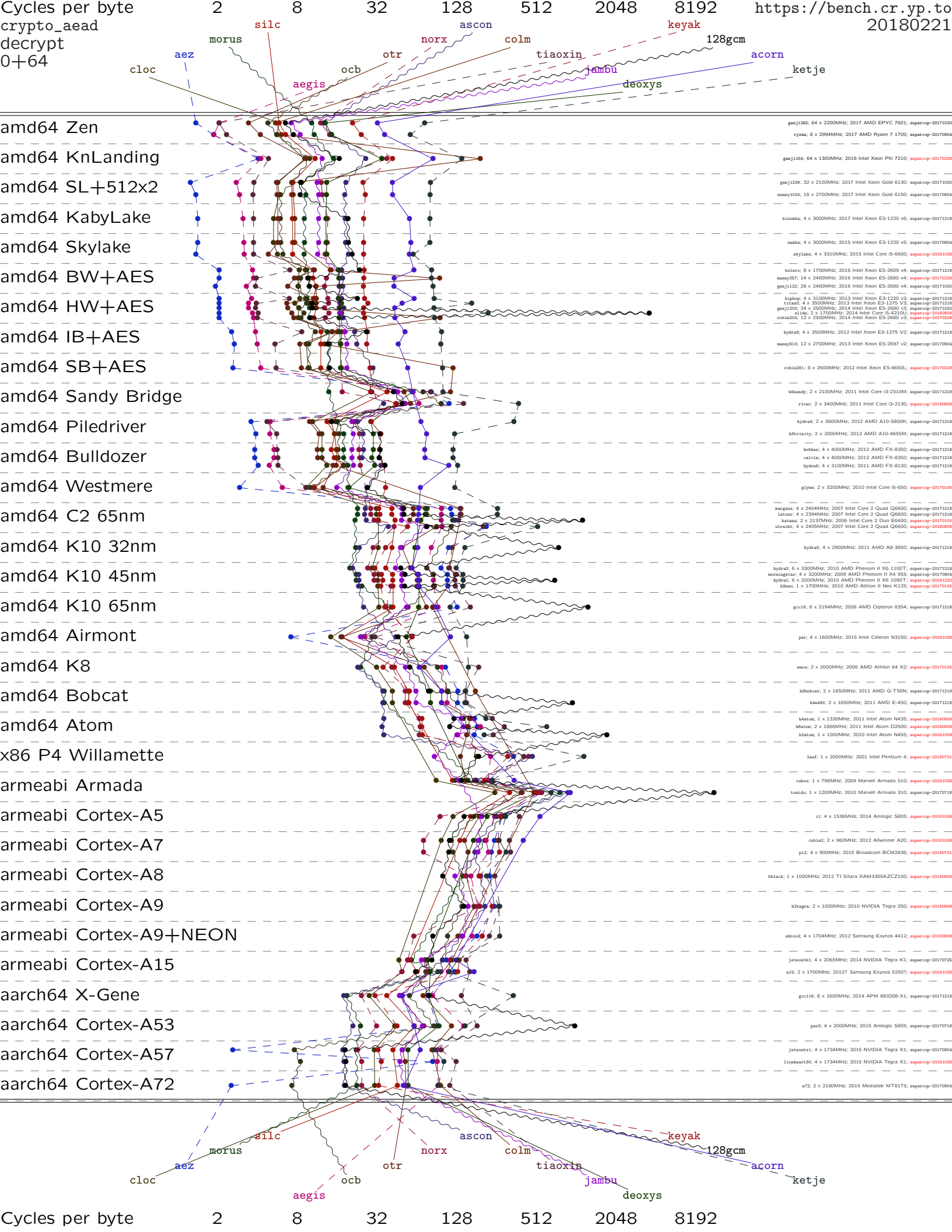
Cycles per byte
2
8
32
128
512
2048
8192
https://bench.cr.yp.to
20180221
crypto_aead
decrypt
0+64
silc
ascon
keyak
morus
norx
colm
128gcm
aez
otr
tiaoxin
acorn
cloc
ocb
jambu
ketje
aegis
deoxys
amd64 Zen
genji262; 64 x 2200MHz; 2017 AMD EPYC 7601; supercop-20171020
ryzen; 8 x 2994MHz; 2017 AMD Ryzen 7 1700; supercop-20170904
amd64 KnLanding
genji154; 64 x 1300MHz; 2016 Intel Xeon Phi 7210; supercop-20170228
amd64 SL+512x2
genji239; 32 x 2100MHz; 2017 Intel Xeon Gold 6130; supercop-20171020
manny1024; 18 x 2700MHz; 2017 Intel Xeon Gold 6150; supercop-20170904
amd64 KabyLake
kizomba; 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; supercop-20171218
amd64 Skylake
samba; 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; supercop-20170904
skylake; 4 x 3310MHz; 2015 Intel Core i5-6600; supercop-20161026
amd64 BW+AES
bolero; 8 x 1700MHz; 2016 Intel Xeon E5-2609 v4; supercop-20171218
manny357; 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; supercop-20170228
genji122; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; supercop-20171020
amd64 HW+AES
hiphop; 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; supercop-20171218
titan0; 4 x 3500MHz; 2013 Intel Xeon E3-1275 V3; supercop-20171218
genji202; 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; supercop-20171020
slide; 2 x 1700MHz; 2014 Intel Core i5-4210U; supercop-20160806
robin204; 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; supercop-20170228
amd64 IB+AES
hydra8; 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; supercop-20171218
manny613; 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; supercop-20170904
amd64 SB+AES
robin281; 8 x 2600MHz; 2012 Intel Xeon E5-4650L; supercop-20170228
amd64 Sandy Bridge
h6sandy; 2 x 2100MHz; 2011 Intel Core i3-2310M; supercop-20171218
river; 2 x 3400MHz; 2011 Intel Core i3-2130; supercop-20160806
amd64 Piledriver
hydra9; 2 x 3800MHz; 2012 AMD A10-5800K; supercop-20171218
h9trinity; 2 x 2000MHz; 2012 AMD A10-4655M; supercop-20171218
amd64 Bulldozer
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
amd64 Westmere
glyme; 2 x 3200MHz; 2010 Intel Core i5-650; supercop-20170105
amd64 C2 65nm
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
amd64 K10 32nm
hydra5; 4 x 2900MHz; 2011 AMD A8-3850; supercop-20171218
amd64 K10 45nm
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
amd64 K10 65nm
gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; supercop-20171218
amd64 Airmont
par; 4 x 1600MHz; 2015 Intel Celeron N3150; supercop-20161026
amd64 K8
mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; supercop-20170105
amd64 Bobcat
h8bobcat; 2 x 1650MHz; 2011 AMD G-T56N; supercop-20171218
h4e450; 2 x 1650MHz; 2011 AMD E-450; supercop-20171218
amd64 Atom
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
x86 P4 Willamette
leaf; 1 x 2000MHz; 2001 Intel Pentium 4; supercop-20160731
armeabi Armada
cubox; 1 x 796MHz; 2009 Marvell Armada 510; supercop-20161026
tonido; 1 x 1200MHz; 2010 Marvell Armada 310; supercop-20170718
armeabi Cortex-A5
c1; 4 x 1536MHz; 2014 Amlogic S805; supercop-20161026
armeabi Cortex-A7
cubie2; 2 x 960MHz; 2012 Allwinner A20; supercop-20161026
pi2; 4 x 900MHz; 2015 Broadcom BCM2836; supercop-20160731
armeabi Cortex-A8
bblack; 1 x 1000MHz; 2012 TI Sitara XAM3359AZCZ100; supercop-20160806
armeabi Cortex-A9
h2tegra; 2 x 1000MHz; 2010 NVIDIA Tegra 250; supercop-20160806
armeabi Cortex-A9+NEON
odroid; 4 x 1704MHz; 2012 Samsung Exynos 4412; supercop-20160806
armeabi Cortex-A15
jetsontk1; 4 x 2065MHz; 2014 NVIDIA Tegra K1; supercop-20170725
a15; 2 x 1700MHz; 2012? Samsung Exynos 5250?; supercop-20161026
aarch64 X-Gene
gcc116; 8 x 1600MHz; 2014 APM 883208-X1; supercop-20171218
aarch64 Cortex-A53
par3; 4 x 2000MHz; 2015 Amlogic S905; supercop-20170718
aarch64 Cortex-A57
jetsontx1; 4 x 1734MHz; 2015 NVIDIA Tegra X1; supercop-20170904
lionheart30; 4 x 1734MHz; 2015 NVIDIA Tegra X1; supercop-20161026
aarch64 Cortex-A72
a72; 2 x 2100MHz; 2015 Mediatek MT8173; supercop-20170904
silc
ascon
keyak
morus
norx
colm
128gcm
aez
otr
tiaoxin
acorn
cloc
ocb
jambu
ketje
aegis
deoxys
Cycles per byte
2
8
32
128
512
2048
8192