

crypto_aead
elmd600v2
implementations
amd64 Bobcat
amd64 K8
amd64 K10 65nm
amd64 K10 45nm
amd64 K10 32nm
amd64 Bulldozer
amd64 Piledriver
amd64 Zen
amd64 Zen 2
amd64 Zen 3
amd64 Knights Landing
amd64 Golden Cove
amd64 Cascade Lake
amd64 Tiger Lake
amd64 Skylake+512x2
amd64 Ice Lake
amd64 Comet Lake
amd64 Cannon Lake
amd64 Coffee Lake
amd64 Kaby Lake
amd64 Skylake
amd64 Broadwell+AES
amd64 Haswell+AES
amd64 Ivy Bridge+AES
amd64 Sandy Bridge+AES
amd64 Sandy Bridge
amd64 Westmere
amd64 Core 2 45nm
amd64 Core 2 65nm
amd64 Gracemont
amd64 Tremont
amd64 Goldmont Plus
amd64 Goldmont
amd64 Airmont
amd64 Silvermont
amd64 Bonnell
ppc32 G3
riscv64 U54
mips32 Octeon II
armeabi Armada
armeabi Cortex-A7
armeabi Cortex-A8
armeabi Cortex-A9+NEON
armeabi Cortex-A15
aarch64 X-Gene
aarch64 Cortex-A53
aarch64 Cortex-A53+crypto
aarch64 Cortex-A57+crypto
aarch64 Cortex-A72
aarch64 Cortex-A72+crypto
aarch64 ThunderX2
Time

131072

262144

524288

1048576

T:ref

? :ref

bhbcata: 2 x 1650MHz; 2011 AMD G-T56n; amd64; Bobcat (500F10); supercep-20230630
m4e50: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500F20); supercep-20200618
naaa: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40f82); supercep-20170105
gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercep-20171218
hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100fa0); supercep-20171218
sonniagtar: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100fa2); supercep-20170904
hbaaw: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f83); supercep-20171005
hydra4: 4 x 2600MHz; 2011 AMD A6-3850; amd64; K10 32nm (300F10); supercep-20230630
hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); supercep-20230630
bobcat: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercep-20171218
calista: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercep-20171218
hydra6: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600F12); supercep-20171218
nauer210: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercep-20230630
hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610F01); supercep-20171218
fpriority: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610F01); supercep-20200618
ryzen: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercep-20230630
ryzen2: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercep-20230630
ryzen3: 4 x 3300MHz; 2017 AMD Ryzen 3 3300U; amd64; Zen (800H11); supercep-20230630
ryzen4: 6 x 3300MHz; 2017 AMD Ryzen 3 3300U; amd64; Zen (800H11); supercep-20230630
dali: 2 x 1400MHz; 2020 AMD Athlon Silver E3000; amd64; Zen (800H11); supercep-20211212
ryzen7: 8 x 3800MHz; 2017 AMD Ryzen 7 3800X; amd64; Zen (800H11); supercep-20230630
ryzen9: 8 x 3800MHz; 2017 AMD Ryzen 9 3900X; amd64; Zen (800H11); supercep-20230630
ryzen9: 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830F10); supercep-20230630
ryzen9: 6 x 3000MHz; 2022 AMD Ryzen 5 8500U; amd64; Zen 2 (860H01); supercep-20230630
lacienne: 4 x 2000MHz; 2021 AMD Ryzen 3 3300U; amd64; Zen 3 (820F10); supercep-20230630
gauj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830F10); supercep-20191017
beavink: 6 x 4062MHz; 2021 AMD Ryzen 5 5560U; amd64; Zen 3 (a50F00); supercep-20211221
saah: 16 x 3400MHz; 2020 AMD Ryzen 9 3900X; amd64; Zen 3 (820F10); supercep-20230630
cezanne: 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (a50F00); supercep-20230630
gauj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); supercep-20180818
gauj1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; Knights Landing (50671); supercep-20170228
alder: 4 x 3300MHz; 2022 Intel Core i3-12100; amd64; Golden Cove (90673-00); supercep-20230630
alder1:1f26290,560000; 2 x 1600MHz; 2022 Intel Core i3-1215U performance cores; amd64; Golden Cove (9064A-40); supercep-20230630
avx512maxh: 18 x 3000MHz; 2019 Intel Core i9-10900K; amd64; Cascade Lake (50657); supercep-20210126
pmo4076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); supercep-20191017
panther: 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercep-20230630
saavy1024: 18 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake (50641); supercep-20170804
panther: 8 x 2500MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercep-20230630
gauj1230: 18 x 2400MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake (50641); supercep-20191017
gauj1230: 18 x 2400MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake (50641); supercep-20191017
gauj1230: 18 x 2400MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake (50641); supercep-20191017
icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; Ice Lake (706e5); supercep-20221005
icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; Ice Lake (706e5); supercep-20200626
cus10: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercep-20230630
cosat: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercep-20230630
canon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; Cannon Lake (90663); supercep-20190910
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906a3); supercep-20230630
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906a3); supercep-20230630
bitvix: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906a3); supercep-20190910
kabyaa: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); supercep-20230630
skovshare: 2 x 2400MHz; 2017 Intel Core i7-8700; amd64; Kaby Lake (906e9); supercep-20211212
istalaucl: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); supercep-20191017
saah: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506c3); supercep-20171218
saaha: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506c3); supercep-20230630
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20180818
Banj1757: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
RW11: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
bolan: 18 x 1700MHz; 2015 Intel Core i3-5005A1; amd64; Broadwell+AES (506d4); supercep-20230630
saah: 4 x 1900MHz; 2010 Intel Core i3-530; amd64; Broadwell+AES (506d4); supercep-20230630
gauj1465: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306f2); supercep-20190818
Intel i704: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
Intel i704: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
Intel i704: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
Intel i704: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
Intel i704: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f3); supercep-20171028
gauj1613: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; Ivy Bridge+AES (306e4); supercep-20180818
transiv: 2 x 1800MHz; 2012 Intel Core i5-3427U; amd64; Ivy Bridge+AES (306e9); supercep-20230630
hydra8: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; Ivy Bridge+AES (306e9); supercep-20230630
hedera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; Ivy Bridge+AES (306e9); supercep-20210326
robia281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; Sandy Bridge+AES (206d7); supercep-20170228
hydra7: 4 x 3100MHz; 2011 Intel Xeon E3-1225; amd64; Sandy Bridge+AES (206a7); supercep-20230630
hbsandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercep-20221122
g3ysw: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercep-20170105
voirdale: 2 x 3060MHz; 2009 Intel Core 2 Duo E7600; amd64; Core 2 45nm (1067a); supercep-20230630
katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; Core 2 65nm (6f6); supercep-20170105
trdsant: 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; Core 2 65nm (6f6); supercep-20230630
nasraaj: 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); supercep-20230630
lathour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); supercep-20201130
alder2:1f26290,330000; 4 x 1600MHz; 2022 Intel Core i3-1215U efficiency cores; amd64; Gracemont (9064A-20); supercep-20230630
jasper2: 2 x 1100MHz; 2021 Intel Celeron N4500; amd64; Tremont (906c0); supercep-20230630
jasper3: 4 x 2000MHz; 2021 Intel Celeron N5105; amd64; Tremont (906c0); supercep-20230630
jasper: 4 x 1100MHz; 2021 Intel Pentium Silver N6000; amd64; Tremont (906c0); supercep-20230630
gemini: 2 x 1100MHz; 2019 Intel Celeron N4020; amd64; Goldmont Plus (706a8); supercep-20230630
wooden: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); supercep-20230630
scvil63h: 16 x 2100MHz; 2017 Intel Atom C395G; amd64; Goldmont (506f1); supercep-20191017
mcmcc: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercep-20230630
cherry: 4 x 1440MHz; 2016 Intel Atom i5-Z8350; amd64; Silvermont (406a4); supercep-20230630
bbaton: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Bonnell (306e1); supercep-20230630
alntendosillluing: 1 x 720MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercep-20191221
hifiveunleashedriscv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercep-20191221
riscvunleashedriscv: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercep-20210326
gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips32; Octeon II (cmnips64v2); supercep-20230630
erpfloatz: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips32; Octeon II (cmnips64v2); supercep-20220213
teside: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f311); supercep-20170718
berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410fc075); supercep-20230630
black: 1 x 1000MHz; 2012 TI Sitara XAM3359AZC12100; armeabi; Cortex-A8 (413fc082); supercep-20230630
norveallio: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercep-20200702
artix: 4 x 1200MHz; 2012 Samsung Exynos 44127; armeabi; Cortex-A9+NEON (413fc090); supercep-20191221
norveallio: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercep-20191221
jetsotti: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); supercep-20170728
gcc16: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500F000); supercep-20171218
pi3aplu: 4 x 1400MHz; 2018 Broadcom BCM28370; aarch64; Cortex-A53 (410f034); supercep-20230630
pi3aplu: 4 x 1400MHz; 2018 Broadcom BCM28370; aarch64; Cortex-A53 (410f034); supercep-20221122
leuf: 4 x 1400MHz; 2018 APM 88320B-X1; aarch64; Cortex-A53+crypto (410f034); supercep-20170728
leuf: 4 x 1400MHz; 2018 APM 88320B-X1; aarch64; Cortex-A53+crypto (410f034); supercep-20170728
goglaocrasin: 4 x 1500MHz; 2011 NXP iMX 6M; aarch64; Cortex-A53+crypto (410f034); supercep-20191221
rnsagdelockdriscv: 4 x 1800MHz; 2017 Rockchip RK3288; aarch64; Cortex-A53+crypto (410f034); supercep-20230630
jetsotti: 4 x 1734MHz; 2015 NVIDIA Tegra K1; aarch64; Cortex-A57+crypto (418f071); supercep-20191017
varbear: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (411f072); supercep-20200626
pi4h: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercep-20221122
rpi4bunleashed: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercep-20191221
a7: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418f080); supercep-20190904
pmo445: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431fa0f1); supercep-20191017