

crypto\_aead  
shellaes128v2d6n80  
implementations

T:ref

? :ref

https://bench.cr.yp.to  
20230702

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

mipso32 Octeon II

armeabi Armada

armeabi Cortex-A7

armeabi Cortex-A8

armeabi Cortex-A9+NEON

armeabi Cortex-A15

aarch64 X-Gen

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

hbbocat: 2 x 1650MHz; 2011 AMD G-T56n; amd64; Bobcat (500F10); supercop-20230630
m4e50: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500F20); supercop-20200618
nae: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40f2b); supercop-20170105
gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20171218
hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f40); supercop-20171218
sonnigstar: 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-20171218
hydra4: 4 x 2600MHz; 2011 AMD A6-3850; amd64; K10 32nm (300F10); supercop-20230630
hydra5: 4 x 2900MHz; amd64; K10 32nm (300F10); supercop-20230630
bobcat: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); supercop-20171218
calvin: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); supercop-20171218
hydra6: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600P12); supercop-20171218
hawer216: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); supercop-20230630
hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610F11); supercop-20171218
hprariaty: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610F11); supercop-20200618
zeus8: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercop-20170805
zeus9: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercop-20170805
rubas3: 4 x 3100MHz; AV10; AMD; Ryzen 3 1300G; amd64; Zen (800H11); supercop-20221122
dali: 2 x 1800MHz; 2016 AMD Athlon Silver E2-9000; amd64; Zen (800H11); supercop-20221122
reno6: 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830F10); supercop-20230630
reno7: 6 x 3000MHz; 2022 AMD Ryzen 5 4500U; amd64; Zen 2 (860H01); supercop-20230630
lactance: 4 x 2600MHz; 2021 AMD Ryzen 3 3300U; amd64; Zen 2 (830F10); supercop-20191017
gwj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830F10); supercop-20191017
bealinx: 6 x 4062MHz; 2021 AMD Ryzen 5 5560U; amd64; Zen 3 (a50F00); supercop-20211122
swah: 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen 3 (a20F10); supercop-20220213
cezanne: 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (a50F00); supercop-20230630
gwj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); supercop-20180818
gwj1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; Knights Landing (50671); supercop-20170228
alder: 4 x 3300MHz; 2022 Intel Core i3-12100; amd64; Golden Cove (90673-00); supercop-20230630
alder2:1f62690,5600000; 2 x 1600MHz; 2022 Intel Core i3-1215U performance cores; amd64; Golden Cove (906A4-40); supercop-20230630
avx512iaah: 18 x 3000MHz; 2019 Intel Core i9-10980X; amd64; Cascade Lake (50657); supercop-20201126
penod076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); supercop-20191017
panthar: 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercop-20230630
sanmy1024: 18 x 2100MHz; 2017 Intel Xeon Core E3-1220 v5; amd64; Skylake (506c3); supercop-20170805
sanmy0070: 8 x 2500MHz; 2017 Intel Core i7-6700; amd64; Skylake (506c3); supercop-20171121
sanmy0071: 8 x 2500MHz; 2017 Intel Core i7-6700; amd64; Skylake (506c3); supercop-20171121
gwj1298: 20 x 2100MHz; 2017 Intel Xeon Gold 6135; amd64; Skylake (506c3); supercop-20191017
gwj1299: 20 x 2100MHz; 2017 Intel Xeon Gold 6135; amd64; Skylake (506c3); supercop-20191017
icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; Ice Lake (706e5); supercop-20221005
icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; Ice Lake (706e5); supercop-20200626
cubis10: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230630
cosat: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230630
canon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; Cannon Lake (90663); supercop-20190910
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906a3); supercop-20230630
blitvix: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906a3); supercop-20190910
kizamba: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); supercop-20230630
shouhara: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; Kaby Lake (906e9); supercop-20211122
intalanci: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); supercop-20191017
saad: 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-20230630
gwj1461: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20180818
sanmy1271: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20170228
sanmy1272: 18 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20170228
bolax: 18 x 1700MHz; 2015 Intel Core i3-5005G1; amd64; Broadwell+AES (506d4); supercop-20230630
alder: 4 x 1900MHz; 2019 Intel Core i3-1005G1; amd64; Broadwell+AES (506d4); supercop-20230630
gwj1465: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306d7); supercop-20190910
hsw1024: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1025: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1026: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1027: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1028: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1029: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1030: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1031: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1032: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1033: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1034: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1035: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1036: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1037: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1038: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1039: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1040: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1041: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1042: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1043: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1044: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1045: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1046: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1047: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1048: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1049: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1050: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1051: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1052: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1053: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1054: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1055: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1056: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1057: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1058: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1059: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1060: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1061: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1062: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1063: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1064: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1065: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1066: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1067: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1068: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1069: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1070: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1071: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1072: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1073: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1074: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1075: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1076: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1077: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1078: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1079: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1080: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1081: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1082: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1083: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1084: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1085: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1086: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1087: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1088: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1089: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1090: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1091: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1092: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1093: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1094: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1095: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1096: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1097: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1098: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1099: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1100: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1101: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1102: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1103: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1104: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1105: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1106: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1107: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1108: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1109: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1110: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1111: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1112: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1113: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-20171121
hsw1114: 18 x 2400MHz; 2012 Intel Xeon E5-2650 v2; amd64; Haswell+AES (306d7); supercop-