

crypto_core
invsntруп1277
implementations

avx

ref

https://bench.cr.y.p.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 Oceon 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

2097152

8388608

33554432

13421728

bbobcat: 2 x 1650MHz; 2011 AMD G-T56n; amd64; Bobcat (600F10); supercop-20230630																								
m4e50: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (600F20); supercop-20200618																								

naca: 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 (100fA0); supercop-20171218																								
sonnigstar: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100fA2); supercop-20170904																								
h3naw: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100fG3); supercop-20171218																								

hydra4: 4 x 2600MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); supercop-20230630																								
hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); supercop-20230630																								

bobcat: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercop-20171218																								
calista: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercop-20171218																								
hydra4: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600F12); supercop-20171218																								
saber216: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20); supercop-20230630																								

hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610F01); supercop-20171218																								
hptriatry: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610F01); supercop-20200618																								

reggie: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercop-20170865																								
rubias: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); supercop-20170865																								
rubias3: 4 x 3100MHz; 2017 AMD Ryzen 3 1300; amd64; Zen (800H11); supercop-20211232																								
dali: 2 x 1800MHz; 2017 AMD Ryzen 3 1300; amd64; Zen (800H11); supercop-20211232																								

rozeo: 64 x 2750MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830F10); supercop-20230630																								
rozeo1: 6 x 3000MHz; 2022 AMD Ryzen 5 4500U; amd64; Zen 2 (860H01); supercop-20230630																								
lactance: 4 x 2600MHz; 2020 AMD Ryzen 9 5900X; amd64; Zen 2 (830F10); supercop-20230630																								
gauj1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830F10); supercop-20191017																								

baseline: 6 x 4062MHz; 2021 AMD Ryzen 5 5600U; amd64; Zen 3 (a50F00); supercop-20211122																								
sash: 16 x 3400MHz; 2020 AMD Ryzen 9 5900X; amd64; Zen 3 (a50F10); supercop-20211122																								
cezanne: 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (a50F00); supercop-20230630																								

gauj1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); supercop-20180818																								
gauj1154: 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																								

avx121nath: 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; Cascade Lake (50657); supercop-20201126																								
pmc0076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); supercop-20191017																								

panther: 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); supercop-20230630																								

nany1004: 18 x 2700MHz; 2017 Intel Xeon Gold 6100; amd64; Skylake+512x2 (906A4); supercop-20170865																								
pmc0076: 8 x 2500MHz; 2017 Intel Core i9-7900; amd64; Skylake+512x2 (906A4); supercop-20181123																								
gauj1291: 16 x 2400MHz; 2017 Intel Xeon Gold 6110; amd64; Skylake+512x2 (906A4); supercop-20181123																								
gauj1291: 8 x 2400MHz; 2017 Intel Xeon Gold 6110; amd64; Skylake+512x2 (906A4); supercop-20191017																								
gauj1291: 8 x 2400MHz; 2017 Intel Xeon Gold 6110; amd64; Skylake+512x2 (906A4); 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																								

cusis: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230630																								
coset: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); supercop-20230630																								

cannon: 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 (906e4); supercop-20230630																								
nlvisia: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906e4); supercop-20190910																								

kabya: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); supercop-20230630																								
shourahar: 2 x 2400MHz; 2017 Intel Core i3-7102; amd64; Kaby Lake (906e9); supercop-20211122																								
istalucis1: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); supercop-20191017																								

sand: 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-20230630																								

gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20180818																								
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20180818																								
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20170228																								
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20170228																								
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20230630																								
gauj1441: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); supercop-20230630																								

gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20190910																								
gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20190910																								
gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20230630																								
gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20230630																								
gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20230630																								
gauj1441: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e4); supercop-20230630																								

nany613: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; Ivy Bridge+AES (306e4); supercop-20180818																								
nany613: 2 x 1800MHz; 2012 Intel Core i5-3427U; amd64; Ivy Bridge+AES (306e9); supercop-20230630																								
hydra4: 4 x 3000MHz; 2012 Intel Xeon E3-1275 V2; amd64; Ivy Bridge+AES (306e9); supercop-20230630																								
bedera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; Ivy Bridge+AES (306e9); supercop-20210326																								

robia281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; Sandy Bridge+AES (206d7); supercop-20170228																								
hydra7: 4 x 3100MHz; 2011 Intel Xeon E3-1225; amd64; Sandy Bridge+AES (206d7); supercop-20230630																								

h6sandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20221122																								

g1yso: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20170105																								

voifdale: 2 x 3060MHz; 2009 Intel Core 2 Duo E7600; amd64; Core 2 45nm (1067a); supercop-20230630																								

katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; Core 2 65nm (60f); supercop-20170105																								
trsdant: 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; Core 2 65nm (60f); supercop-20230630																								
naargat: 4 x 2004MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (60f); supercop-20230630																								
lalour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (60f); supercop-20201130																								

alder2.1f62690.3300000: 4 x 1600MHz; 2022 Intel Core i3-1215U efficiency cores; amd64; Gracemont (906A4-20); supercop-20230630																								

jasper2: 2 x 1100MHz; 2021 Intel Celeron N4500; amd64; Tremont (906c0); supercop-20230630																								
jasper3: 4 x 2000MHz; 2021 Intel Celeron N5105; amd64; Tremont (906c0); supercop-20230630																								
jasper: 4 x 1100MHz; 2021 Intel Pentium Silver N6000; amd64; Tremont (906c0); supercop-20230630																								

gemini: 2 x 1100MHz; 2019 Intel Celeron N4020; amd64; Goldmont Plus (706a8); supercop-20230630																								

wooden: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); supercop-20230630																								
scv1M8h1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017																								

muscc: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercop-20230630																								

cherry: 4 x 1440MHz; 2016 Intel Atom i5-28350; amd64; Silvermont (406c4); supercop-20230630																								

h8ato: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Bonnell (306f1); supercop-20230630																								

aintendovilliauzang: 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																								

gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnmps64v2); supercop-20230630																								
expofafz2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnmps64v2); supercop-20220213																								

teside: 1 x 1200MHz; 2010 Marvel Armada 310; armeabi; Armada (562f311); supercop-20170718																								

berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20230630																								

nblack: 1 x 1000MHz; 2012 TI Sitara XAM3359AZC2100; armeabi; Cortex-A8 (413f082); supercop-20230630																								

noaveblaw: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20200702																								
artix: 4 x 1200MHz; 2012 Samsung Exynos 44127; armeabi; Cortex-A9+NEON (413f090); supercop-20191221																								
noaveblaw: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221																								

jtsosati: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); supercop-20170728																								

gcc16: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500f000); supercop-20171218																								

pi3hplai: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410f034); supercop-20230630																								
pi3hplai: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; Cortex-A53 (410f034); supercop-20221122																								

leeds: 4 x 1600MHz; 2015 ARMv8-A Cortex-A53; aarch64; Cortex-A53+crypto (410f034); supercop-20170464																								
leptonarmv8a: 4 x 1600MHz; 2015 ARMv8-A Cortex-A53; aarch64; Cortex-A53+crypto (410f034); supercop-20170464	goglacraslav: 4 x 1500MHz; 2015 NXP i.MX 8M; aarch64; Cortex-A53+crypto (410f034); supercop-20191221		reegadecor8000c: 4 x 1600MHz; 2015 Rockchip RK3288; aarch64; Cortex-A53+crypto (410f034); supercop-20191221		-----		jtsosati: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; Cortex-A57+crypto (418f071); supercop-20191017		warbear: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (4116072); supercop-20200626		-----		pi4h: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20221122		rpi4bunbu64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20191221		-----		a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418f080); supercop-20190904		-----		pmc0445: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0a1); supercop-20191017	
goglacraslav: 4 x 1500MHz; 2015 NXP i.MX 8M; aarch64; Cortex-A53+crypto (410f034); supercop-20191221																								
reegadecor8000c: 4 x 1600MHz; 2015 Rockchip RK3288; aarch64; Cortex-A53+crypto (410f034); supercop-20191221																								

jtsosati: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; Cortex-A57+crypto (418f071); supercop-20191017																								
warbear: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (4116072); supercop-20200626																								

pi4h: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20221122																								
rpi4bunbu64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); supercop-20191221																								

a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418f080); supercop-20190904																								

pmc0445: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0a1); supercop-20191017																								