



Time 16384 32768 65536 131072

crypto_aead	hs1sivlov1	implementations	
amd64 Zen3			bealiak: 6 x 4062MHz; 2021 AMD Ryzen 5 5600U; amd64; Zen3 (a50f00); supercop-20221122
amd64 Zen2			zen3: 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen3 (a20f10); supercop-20220213
amd64 Zen			gej1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830f10); supercop-20191017
amd64 KnLanding			ryzen: 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20170904 rubb7: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20220606 rubb6: 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); supercop-20220606 rubb3: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); supercop-20200906
amd64 CascadeLake			gej1291: 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; KnLanding (50671); supercop-20180818 gej1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; KnLanding (50671); supercop-20170228
amd64 SL+512x2			avx512aath: 18 x 3000MHz; 2019 Intel Core i9-10900XE; amd64; CascadeLake (50657); supercop-20210126 pnoo876: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); supercop-20191017
amd64 IceLake			aaay1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); supercop-20170904 pnl: 6 x 3500MHz; 2017 Intel Core i7-8800X; amd64; SL+512x2 (50654); supercop-20211123 pnoo903: 20 x 2400MHz; 2018 Intel Xeon Gold 6148; amd64; BW+AES (50654); supercop-20191017 gej1548: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017 gej1338: 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; BW+AES (50654); supercop-20211122
amd64 CometLake			icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; icelake (706e5); supercop-20221008 icelake; 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; icelake (706e5); supercop-20200826
amd64 CannonLake			comet: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; CometLake (806e); supercop-20221026
amd64 CoffeeLake			caano: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; CannonLake (60663); supercop-20190910
amd64 KabyLake			r2400: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; CoffeeLake (906ea); supercop-20221019 bitvisy: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); supercop-20190910
amd64 Skylake			shorthera: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; KabyLake (806e9); supercop-20221122 kisooba: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); supercop-20220606 intelasc18: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906e9); supercop-20191017
amd64 BW+AES			saad: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); supercop-20171218 raaba: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); supercop-20221122
amd64 HW+AES			gej1441: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20180818 aaay087: 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20170228 gej1122: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20171020 beaef8: 8 x 1300MHz; 2015 Intel Core i5-5200U; amd64; BW+AES (406f1); supercop-20221122
amd64 IB+AES			gej1462: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; HW+AES (30627); supercop-20180818 gej1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (30627); supercop-20171020 rubb204: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (30627); supercop-20170228 titand: 4 x 3500MHz; 2013 Intel Xeon E5-1275 V2; amd64; HW+AES (306c3); supercop-20221122 lubb9: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v5; amd64; HW+AES (306c3); supercop-20221122
amd64 SB+AES			maayg13: 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306e4); supercop-20180818 hydra8: 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306e9); supercop-20221122 bedera: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; IB+AES (306e9); supercop-20210326
amd64 Sandy Bridge			robia281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; SB+AES (206d7); supercop-20170228
amd64 Piledriver			hfaandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20200618
amd64 Bulldozer			hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); supercop-20171218 lbtirsty: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); supercop-20200618
amd64 Westmere			bbaba: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218 calvia: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218 hydra7: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f20); supercop-20171120 aaba216: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20220606
amd64 C2 65nm			glywa: 2 x 3300MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20170105
amd64 K10 32nm			katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20170105 nargusa: 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20221122 latour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20211018
amd64 K10 45nm			hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20191221
amd64 K10 65nm			hydra6: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f50); supercop-20171218 worsigast: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100f42); supercop-20170904 h3ao: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20170105
amd64 Airmont			gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20171218
amd64 Goldmont			mucaac: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); supercop-20221122
amd64 K8			voodea: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506e9); supercop-20221122 scv163b1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017
amd64 Bobcat			saac: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20170105
amd64 Atom			bBboca: 2 x 1650MHz; 2011 AMD G-T56M; amd64; Bobcat (500f10); supercop-20171218 h4e80: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20200618
ppc32 G3			hlatca: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (306f1); supercop-20200618
riscv64 U54			nintendovillainuzg: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221
mipso32 Oocteon II			hifiveuaashadricv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20191221 riscvuaashad800: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20210326
armeabi Armada			gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnips64v2); supercop-20221122 eyroffarf2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnnips64v2); supercop-20220213
armeabi Cortex-A7			tonido: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f311); supercop-20170718
armeabi Cortex-A8			berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20221122
armeabi Cortex-A9+NEON			tblad: 1 x 1000MHz; 2012 TI Sitara XAM3359AZCZ100; armeabi; Cortex-A8 (413f082); supercop-20221005
armeabi Cortex-A15			noveabla: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20200702 artik: 4 x 1200MHz; 2012 Samsung Exynos 4412; armeabi; Cortex-A9+NEON (413f090); supercop-20191221 noveasiaa: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221
aarch64 X-Gene			jetsontat: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); supercop-20170726
aarch64 A53			gcc116: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500f000); supercop-20171218
aarch64 A53+crypto			pi3aplu: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); supercop-20221122 pi3aplu: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); supercop-20221122
aarch64 A57+crypto			par3: 4 x 2000MHz; 2015 Amlogic S905; aarch64; A53+crypto (410f034); supercop-20170718 aaad4: 8 x 1600MHz; 2015 NXP QorIQ LS1088; aarch64; A53+crypto (410f034); supercop-20190904 1epotatouap80cc: 4 x 1312MHz; 2016 Amlogic S905X; aarch64; A53+crypto (410f034); supercop-20191221 rengadefec838cc: 4 x 1312MHz; 2017 Rockchip RK3288; aarch64; A53+crypto (410f034); supercop-20191221
aarch64 A72			jetsontat: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; A57+crypto (418f071); supercop-20191017
aarch64 A72+crypto			warbaar: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; A57+crypto (411f072); supercop-20200826
aarch64 ThunderX2			pi4b: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20221122 rpi4batsua4: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20191221
			a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); supercop-20170904
			pnoo146: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0f1); supercop-20191017