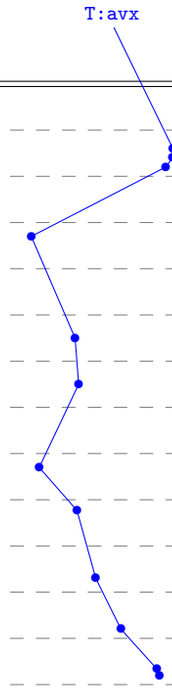
crypto_kem
hqcrmrs256
implementations

https://bench.cr.yp.to
20210605



amd64 Zen2

genji346; 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830f10); supercop-20191017

amd64 Zen

ryzen; 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20170904
rumba7; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800f11); supercop-20210604
rumba5; 6 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800f11); supercop-20210604
rumba3; 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800f11); supercop-20200906

amd64 KnLanding

genji291; 68 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; KnLanding (50671); supercop-20180818
genji154; 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; KnLanding (50671); supercop-20170228

amd64 CascadeLake

avx512math; 18 x 3000MHz; 2019 Intel Core i9-10980XE; amd64; CascadeLake (50657); supercop-20210125
pmod076; 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); supercop-20191017

amd64 SL+512x2

mamy1024; 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); supercop-20170904
oki; 6 x 3500MHz; 2017 Intel Core i7-7800X; amd64; SL+512x2 (50654); supercop-20181123
pmod003; 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20190910
genji548; 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017
genji239; 32 x 2100MHz; 2017 Intel Xeon Gold 6130; amd64; SL+512x2 (50654); supercop-20191017

amd64 IceLake

icelake; 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (706e5); supercop-20200826

amd64 CometLake

comet; 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; CometLake (806ec); supercop-20210604

amd64 CannonLake

cannon; 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; CannonLake (60663); supercop-20190910

amd64 CoffeeLake

r24000; 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; CoffeeLake (906ea); supercop-20210604
bitvise; 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); supercop-20190910

amd64 KabyLake

kizomba; 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); supercop-20210604
intelnuc8; 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906e9); supercop-20191017
intelnuc7; 2 x 3500MHz; 2017 Intel Core i7-7567U; amd64; KabyLake (806e9); supercop-20191017

amd64 Skylake

sand; 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); supercop-20171218
samba; 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); supercop-20210604

amd64 BW+AES

genji441; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20180818
mamy357; 14 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20170228
genji122; 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20171020
bolero; 8 x 1700MHz; 2016 Intel Xeon E5-2609 v4; amd64; BW+AES (406f1); supercop-20210604

amd64 HW+AES

genji460; 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; HW+AES (306f2); supercop-20180818
genji202; 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (306f2); supercop-20171020
robin204; 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (306f2); supercop-20170228
hiphop; 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; amd64; HW+AES (306c3); supercop-20210604
titan0; 4 x 3500MHz; 2013 Intel Xeon E3-1275 V3; amd64; HW+AES (306c3); supercop-20210604

amd64 IB+AES

mamy613; 12 x 2700MHz; 2013 Intel Xeon E5-2697 v2; amd64; IB+AES (306e4); supercop-20180818
hedera; 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; IB+AES (306a9); supercop-20210326
hydra8; 4 x 3500MHz; 2012 Intel Xeon E3-1275 V2; amd64; IB+AES (306a9); supercop-20210604

amd64 SB+AES

robin281; 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; SB+AES (206d7); supercop-20170228

amd64 Sandy Bridge

h6sandy; 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20200618

amd64 Piledriver

hydra9; 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); supercop-20171218
h9trinity; 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); supercop-20200618

amd64 Bulldozer

hobbes; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
calvin; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
hydra6; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20171218
samvar24; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20210423

amd64 Westmere

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

amd64 C2 65nm

katana; 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20170105
margaux; 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6fb); supercop-20210604
latour; 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6fb); supercop-20201130

amd64 K10 32nm

hydra5; 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20191221

amd64 K10 45nm

hydra3; 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100fa0); supercop-20171218
morningstar; 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100f42); supercop-20170904
h3sac; 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20170105

amd64 K10 65nm

gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20171218

amd64 Goldmont

scw1b63b1; 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017

amd64 K8

mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20170105

amd64 Bobcat

h8bobcat; 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500f10); supercop-20171218
h4e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20200618

amd64 Atom

h8atom; 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (30661); supercop-20200618

ppc32 G3

nintendovillinuxmgx; 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221

riscv64 U54

hifivesunleashedriscv; 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

mipso32 Octeon II

erpro8fsf2; 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnmips64v2); supercop-20210604

armeabi Armada

tonido; 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f1311); supercop-20170718

armeabi Cortex-A7

berry2; 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410fc075); supercop-20210604

armeabi Cortex-A9+NEON

novenablue; 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercop-20200702
artik; 4 x 1200MHz; 2012 Samsung Exynos 4412?; armeabi; Cortex-A9+NEON (413fc090); supercop-20191221
novenaimx6; 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); supercop-20191221

armeabi Cortex-A15

jetsontk1; 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); supercop-20170725

aarch64 X-Gene

gcc116; 8 x 1600MHz; 2014 APM 883208-X1; aarch64; X-Gene (500f0000); supercop-20171218

aarch64 A53

pi3bplus; 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410fd034); supercop-20210604

aarch64 A53+crypto

par3; 4 x 2000MHz; 2015 Amlogic S905; aarch64; A53+crypto (410fd034); supercop-20170718
lepotatoamls905xcc; 4 x 1512MHz; 2016 Amlogic S905X; aarch64; A53+crypto (410fd034); supercop-20191221
googlecoraldev; 4 x 1500MHz; 2018 NXP i.MX 8M; aarch64; A53+crypto (410fd034); supercop-20191221
renegaderocrk3328cc; 4 x 1512MHz; 2017 Rockchip RK3328; aarch64; A53+crypto (410fd034); supercop-20191221

aarch64 A57+crypto

jetsontx1; 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; A57+crypto (418fd071); supercop-20191017
warbear0; 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; A57+crypto (411fd072); supercop-20200826

aarch64 A72

rpi4ubuntu64; 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410fd083); supercop-20191221

aarch64 A72+crypto

a72; 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418fd080); supercop-20170904

aarch64 ThunderX2

pmod145; 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0af1); supercop-20191017

Time 2097152 4194304