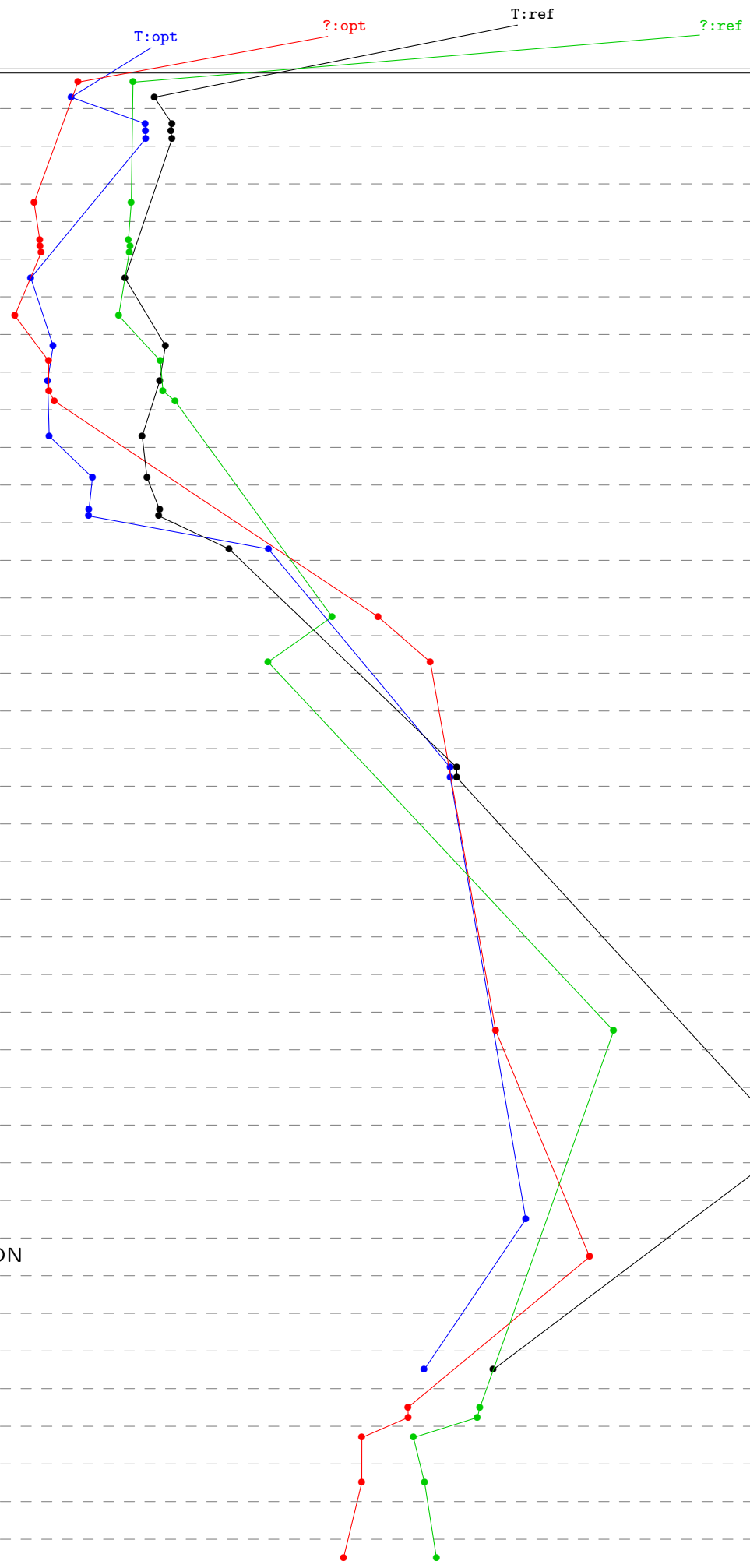


crypto_kem
hqc2563
implementations

https://bench.cr.yp.to
20210115

amd64 Zen2
amd64 Zen
amd64 KnLanding
amd64 CascadeLake
amd64 SL+512x2
amd64 IceLake
amd64 CannonLake
amd64 CoffeeLake
amd64 KabyLake
amd64 Skylake
amd64 BW+AES
amd64 HW+AES
amd64 IB+AES
amd64 SB+AES
amd64 Sandy Bridge
amd64 Piledriver
amd64 Bulldozer
amd64 Westmere
amd64 C2 65nm
amd64 K10 32nm
amd64 K10 45nm
amd64 K10 65nm
amd64 Goldmont
amd64 K8
amd64 Bobcat
amd64 Atom
ppc32 G3
riscv64 U54
mipso32 Octeon II
armeabi Armada
armeabi Cortex-A7
armeabi Cortex-A9+NEON
armeabi Cortex-A15
aarch64 X-Gene
aarch64 A53
aarch64 A53+crypto
aarch64 A57+crypto
aarch64 A72
aarch64 A72+crypto
aarch64 ThunderX2



gej1346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen2 (830F10); supercop-20191017
colossus6: 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen2 (830F10); supercop-20200118
ryzen: 8 x 2994MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800F11); supercop-20170904
ruba7: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800F11); supercop-20201130
ruba8: 8 x 3200MHz; 2017 AMD Ryzen 5 1600; amd64; Zen (800F11); supercop-20201130
ruba3: 4 x 3100MHz; 2017 AMD Ryzen 3 1200; amd64; Zen (800F11); supercop-20200906
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
pno0076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; CascadeLake (50657); supercop-20191017
naany1024: 18 x 2700MHz; 2017 Intel Xeon Gold 6150; amd64; SL+512x2 (50654); supercop-20170904
sk1: 6 x 3500MHz; 2017 Intel Core i7-7800X; amd64; SL+512x2 (50654); supercop-20181123
pno0003: 20 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017
gej1548: 40 x 2400MHz; 2017 Intel Xeon Gold 6148; amd64; SL+512x2 (50654); supercop-20191017
gej1235: 32 x 2100MHz; 2017 Intel Xeon Gold 6140; amd64; SL+512x2 (50654); supercop-20191017
icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; IceLake (706e5); supercop-20200826
cannon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; CannonLake (50663); supercop-20190910
r2600: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; CoffeeLake (906ea); supercop-20201018
bitvisie: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; CoffeeLake (906ea); supercop-20190910
ziasha: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; KabyLake (906e9); supercop-20201014
intelnuc18: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; KabyLake (906e9); supercop-20191017
intelnuc17: 2 x 3500MHz; 2017 Intel Core i7-7567U; amd64; KabyLake (806e9); supercop-20191017
sand: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506c3); supercop-20171218
saba: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506c3); supercop-20201130
gej1441: 28 x 2400MHz; 2016 Intel Xeon E5-2680 v4; amd64; BW+AES (406f1); supercop-20180818
naany387: 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
bkara: 8 x 1700MHz; 2016 Intel Xeon E5-2629 v4; amd64; BW+AES (406f1); supercop-20201014
gej1460: 20 x 2300MHz; 2014 Intel Xeon E5-2650 v3; amd64; HW+AES (3062f); supercop-20180818
gej1202: 24 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (3062f); supercop-20171020
rob004: 12 x 2500MHz; 2014 Intel Xeon E5-2680 v3; amd64; HW+AES (3062f); supercop-20170228
ttsad: 4 x 3500MHz; 2013 Intel Xeon E3-1275 v3; amd64; HW+AES (306c3); supercop-20201130
hlp06: 4 x 3100MHz; 2013 Intel Xeon E3-1220 v3; amd64; HW+AES (306c3); supercop-20201130
naany613: 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 (306a9); supercop-20201130
rakia281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; SB+AES (20647); supercop-20170228
h6eandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20200618
hydra9: 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610f01); supercop-20171218
h6r1asty: 2 x 2000MHz; 2012 AMD A10-4655M; amd64; Piledriver (610f01); supercop-20200618
bobba: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600f20); supercop-20171218
calvis: 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
glyw: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); supercop-20171016
latana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20171016
nargas: 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20201130
latour: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6f6); supercop-20201130
hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20191221
hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100f00); supercop-20171218
amniagar: 4 x 3200MHz; 2009 AMD Phenom II X6 955; amd64; K10 45nm (100f42); supercop-20170904
lbaoc: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100f63); supercop-20171016
gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20171218
scv1863n1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); supercop-20191017
sasc: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40f02); supercop-20171016
hbboccat: 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500f10); supercop-20171218
h4450: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20200618
hba2es: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Atom (30661); supercop-20200618
sinteadovilliauzag: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); supercop-20191221
hifivuuuashedricv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); supercop-20191221
hbfzf2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mipso32; Octeon II (cnmips64v2); supercop-20201014
tsoid: 1 x 1200MHz; 2010 Marvel Armada 310; armeabi; Armada (562f311); supercop-20170718
berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); supercop-20201018
sveeahlu: 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
sveeahaas: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412f09a); supercop-20191221
jetsontst: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413f0f3); supercop-20170725
gcc16: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500f000); supercop-20171218
pi3pplu: 4 x 1400MHz; 2018 Broadcom BCM2837B0; aarch64; A53 (410f034); supercop-20201014
par3: 4 x 2000MHz; 2015 Amlogic S905; aarch64; A53+crypto (410f034); supercop-20170718
jepotatoais908cc: 4 x 1512MHz; 2016 Amlogic S905X; aarch64; A53+crypto (410f034); supercop-20191221
geogacacraiev: 4 x 1500MHz; 2018 RKP i.MX 8M; aarch64; A53+crypto (410f034); supercop-20191221
jetsontz1: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; A57+crypto (418f071); supercop-20191017
varbear0: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; A57+crypto (411f072); supercop-20200826
rpi4ubuntu6: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; A72 (410f083); supercop-20191221
a72: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; A72+crypto (418f080); supercop-20170904
pno0146: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0f1); supercop-20191017

Time 4194304 16777216 67108864 268435456