

crypto\_kem  
ledakem32s1  
implementations

T:portableopt

?:portableopt

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

mips32 Octeon 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

Time

8388608

16777216

33554432

67108864

hBobcat: 2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (600F10); <a href="#">supercep-20230630</a>
m4450: 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (600F20); <a href="#">supercep-20200618</a>
naac: 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); <a href="#">supercep-20170105</a>
gcc16: 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100F23); <a href="#">supercep-20171218</a>
hydra3: 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100F40); <a href="#">supercep-20171218</a>
sonnigstar: 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100F42); <a href="#">supercep-20170904</a>
hNao: 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100F63); <a href="#">supercep-20170105</a>
hydra4: 4 x 2600MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); <a href="#">supercep-20230630</a>
hydra5: 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10); <a href="#">supercep-20230630</a>
bobcat: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); <a href="#">supercep-20171218</a>
calista: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); <a href="#">supercep-20171218</a>
hydra4: 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600P12); <a href="#">supercep-20171218</a>
shawr216: 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600P20); <a href="#">supercep-20230630</a>
hydra9: 2 x 3800MHz; 2012 AMD A10-6800K; amd64; Piledriver (610F01); <a href="#">supercep-20171218</a>
hPatrioty: 2 x 2000MHz; 2012 AMD A10-6650M; amd64; Piledriver (610F01); <a href="#">supercep-20200618</a>
zebra: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); <a href="#">supercep-20170825</a>
zebra: 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11); <a href="#">supercep-20230630</a>
rubus3: 4 x 3100MHz; 2011 AMD Ryzen 3 1300; amd64; Zen (800H11); <a href="#">supercep-20211232</a>
rubus3: 4 x 3100MHz; 2011 AMD Ryzen 3 1300; amd64; Zen (800H11); <a href="#">supercep-20230630</a>
dali: 2 x 1800MHz; 2017 AMD Athlon Silver E2-9000; amd64; Zen (800H11); <a href="#">supercep-20211232</a>
roseta: 64 x 2250MHz; 2019 AMD EPYC 7742; amd64; Zen 2 (830F10); <a href="#">supercep-20230630</a>
roseta: 6 x 3000MHz; 2022 AMD Ryzen 5 4500U; amd64; Zen 2 (860H01); <a href="#">supercep-20230630</a>
lactuca: 4 x 2600MHz; 2021 AMD Ryzen 3 3300U; amd64; Zen 2 (830F10); <a href="#">supercep-20230630</a>
gawj346: 64 x 2000MHz; 2019 AMD EPYC 7702; amd64; Zen 2 (830F10); <a href="#">supercep-20191017</a>
baseline: 6 x 4062MHz; 2021 AMD Ryzen 5 5600G; amd64; Zen 3 (a50F00); <a href="#">supercep-20211221</a>
sanu: 16 x 3400MHz; 2020 AMD Ryzen 9 5950X; amd64; Zen 3 (a50F10); <a href="#">supercep-20230630</a>
cezanne: 6 x 3900MHz; 2021 AMD Ryzen 5 PRO 5650G; amd64; Zen 3 (a50F00); <a href="#">supercep-20230630</a>
gawj129: 16 x 1400MHz; 2016 Intel Xeon Phi 7250; amd64; Knights Landing (50671); <a href="#">supercep-20180818</a>
gawj1154: 64 x 1300MHz; 2016 Intel Xeon Phi 7210; amd64; Knights Landing (50671); <a href="#">supercep-20170228</a>
alder: 4 x 3300MHz; 2022 Intel Core i3-12100; amd64; Golden Cove (90673-00); <a href="#">supercep-20230630</a>
alder2.1f62690.5600000: 2 x 1600MHz; 2022 Intel Core i3-1215U performance cores; amd64; Golden Cove (906A4-40); <a href="#">supercep-20230630</a>
avx512maah: 18 x 3000MHz; 2019 Intel Core i9-10900XE; amd64; Cascade Lake (50657); <a href="#">supercep-20210126</a>
penod076: 20 x 2500MHz; 2019 Intel Xeon Gold 6248; amd64; Cascade Lake (50657); <a href="#">supercep-20191017</a>
panthar: 4 x 2800MHz; 2020 Intel Core i7-1165G7; amd64; Tiger Lake (806c1); <a href="#">supercep-20230630</a>
sanu1024: 16 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906E4); <a href="#">supercep-20170804</a>
sanu1024: 16 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906E4); <a href="#">supercep-20230630</a>
sanu1024: 16 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906E4); <a href="#">supercep-20211232</a>
sanu1024: 16 x 2100MHz; 2017 Intel Xeon Gold 6150; amd64; Skylake+512x2 (906E4); <a href="#">supercep-20230630</a>
icelake2: 4 x 1000MHz; 2019 Intel Core i3-1035G1; amd64; Ice Lake (706e5); <a href="#">supercep-20221005</a>
icelake: 4 x 1100MHz; 2020 Intel Core i5-1030NG7; amd64; Ice Lake (706e5); <a href="#">supercep-20200626</a>
cubis10: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); <a href="#">supercep-20230630</a>
cosat: 2 x 2100MHz; 2019 Intel Core i3-10110U; amd64; Comet Lake (806ec); <a href="#">supercep-20230630</a>
canon: 2 x 2200MHz; 2018 Intel Core i3-8121U; amd64; Cannon Lake (90663); <a href="#">supercep-20190910</a>
r3000: 4 x 3300MHz; 2018 Intel Xeon E-2124; amd64; Coffee Lake (906e4); <a href="#">supercep-20230630</a>
blvsia: 6 x 3200MHz; 2017 Intel Core i7-8700; amd64; Coffee Lake (906e4); <a href="#">supercep-20190910</a>
kizama: 4 x 3000MHz; 2017 Intel Xeon E3-1220 v6; amd64; Kaby Lake (906e9); <a href="#">supercep-20230630</a>
shoubara: 2 x 2400MHz; 2017 Intel Core i3-7100; amd64; Kaby Lake (906e9); <a href="#">supercep-20211232</a>
istalauc1: 4 x 3100MHz; 2018 Intel Core i7-8809G; amd64; Kaby Lake (906e9); <a href="#">supercep-20191017</a>
sanu: 2 x 3300MHz; 2015 Intel Pentium G4400; amd64; Skylake (506e3); <a href="#">supercep-20171218</a>
sanu: 4 x 3000MHz; 2015 Intel Xeon E3-1220 v5; amd64; Skylake (506e3); <a href="#">supercep-20230630</a>
gawj1461: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); <a href="#">supercep-20180818</a>
gawj1461: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); <a href="#">supercep-20230630</a>
gawj1461: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); <a href="#">supercep-20170228</a>
gawj1461: 28 x 2400MHz; 2016 Intel Xeon E5-2650 v4; amd64; Broadwell+AES (406f1); <a href="#">supercep-20230630</a>
bolsh: 18 x 1700MHz; 2015 Intel Xeon E3-1225 v5; amd64; Broadwell+AES (506e4); <a href="#">supercep-20230630</a>
bolsh: 18 x 1700MHz; 2015 Intel Xeon E3-1225 v5; amd64; Broadwell+AES (506e4); <a href="#">supercep-20230630</a>
gawj1465: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e2); <a href="#">supercep-20190910</a>
gawj1465: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e2); <a href="#">supercep-20230630</a>
gawj1465: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e2); <a href="#">supercep-20211232</a>
gawj1465: 20 x 2200MHz; 2014 Intel Xeon E5-2650 v3; amd64; Haswell+AES (306e2); <a href="#">supercep-20230630</a>
hadesa: 4 x 3000MHz; 2012 Intel Xeon E3-1275 V2; amd64; Ivy Bridge+AES (306e9); <a href="#">supercep-20230630</a>
hadesa: 4 x 2500MHz; 2012 Intel Xeon E3-1265L V2; amd64; Ivy Bridge+AES (306e9); <a href="#">supercep-20210326</a>
robin281: 8 x 2600MHz; 2012 Intel Xeon E5-4650L; amd64; Sandy Bridge+AES (206d7); <a href="#">supercep-20170228</a>
hydra7: 4 x 3100MHz; 2011 Intel Xeon E3-1225; amd64; Sandy Bridge+AES (206d7); <a href="#">supercep-20230630</a>
hSandy: 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); <a href="#">supercep-20211232</a>
glys: 2 x 3200MHz; 2010 Intel Core i5-650; amd64; Westmere (20652); <a href="#">supercep-20170105</a>
voirdale: 2 x 3060MHz; 2009 Intel Core 2 Duo E7600; amd64; Core 2 45nm (1067a); <a href="#">supercep-20230630</a>
katana: 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; Core 2 65nm (6f6); <a href="#">supercep-20170105</a>
trsdant: 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; Core 2 65nm (6f6); <a href="#">supercep-20230630</a>
augap: 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); <a href="#">supercep-20230630</a>
l'auou: 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; Core 2 65nm (6f6); <a href="#">supercep-20201130</a>
alder2.1f62690.3300000: 4 x 1600MHz; 2022 Intel Core i3-1215U efficiency cores; amd64; Gracemont (906A4-20); <a href="#">supercep-20230630</a>
jasper2: 2 x 1100MHz; 2021 Intel Celeron N4500; amd64; Tremont (906c0); <a href="#">supercep-20230630</a>
jasper3: 4 x 2000MHz; 2021 Intel Celeron N5105; amd64; Tremont (906c0); <a href="#">supercep-20230630</a>
jasper: 4 x 1100MHz; 2021 Intel Pentium Silver N6000; amd64; Tremont (906c0); <a href="#">supercep-20230630</a>
gemini: 2 x 1100MHz; 2019 Intel Celeron N4020; amd64; Goldmont Plus (706a8); <a href="#">supercep-20230630</a>
wooden: 4 x 1500MHz; 2016 Intel Celeron J3455; amd64; Goldmont (506c9); <a href="#">supercep-20230630</a>
soviM8h1: 16 x 2100MHz; 2017 Intel Atom C3955; amd64; Goldmont (506f1); <a href="#">supercep-20191017</a>
muscc: 4 x 1600MHz; 2015 Intel Pentium N3700; amd64; Airmont (406c3); <a href="#">supercep-20230630</a>
cherry: 4 x 1440MHz; 2016 Intel Atom i5-28350; amd64; Silvermont (406c4); <a href="#">supercep-20230630</a>
hbat: 2 x 1866MHz; 2011 Intel Atom D2500; amd64; Bonnell (306f1); <a href="#">supercep-20230630</a>
alntendosillauzang: 1 x 729MHz; 2006 IBM PowerPC Broadway; ppc32; G3 (G3); <a href="#">supercep-20191221</a>
hifiveunleashedriscv: 4 x 1400MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); <a href="#">supercep-20191221</a>
riscvunleashed000: 4 x 1000MHz; 2017 SiFive Freedom U540; riscv64; U54 (sifive,u54-mc); <a href="#">supercep-20210326</a>
gcc23: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips32; Octeon II (cmnips64v2); <a href="#">supercep-20230630</a>
expofsfz2: 2 x 2000MHz; 2011 Cavium Octeon II CN6120; mips32; Octeon II (cmnips64v2); <a href="#">supercep-20220213</a>
teside: 1 x 1200MHz; 2010 Marvell Armada 310; armeabi; Armada (562f311); <a href="#">supercep-20170718</a>
berry2: 4 x 900MHz; 2016 Broadcom BCM2836; armeabi; Cortex-A7 (410f075); <a href="#">supercep-20230630</a>
nblack: 1 x 1000MHz; 2012 TI Sitara XAM3359AZC2100; armeabi; Cortex-A8 (413fc082); <a href="#">supercep-20230630</a>
norveblue: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); <a href="#">supercep-20200702</a>
artix: 4 x 1200MHz; 2012 Samsung Exynos 4412; armeabi; Cortex-A9+NEON (413fc090); <a href="#">supercep-20191221</a>
norveblue: 4 x 1200MHz; 2011 Freescale i.MX6 Quad; armeabi; Cortex-A9+NEON (412fc09a); <a href="#">supercep-20191221</a>
jetsontxt: 4 x 2065MHz; 2014 NVIDIA Tegra K1; armeabi; Cortex-A15 (413fc0f3); <a href="#">supercep-20170728</a>
gcc16: 8 x 1600MHz; 2014 APM 88320B-X1; aarch64; X-Gene (500F000); <a href="#">supercep-20171218</a>
pi3hplus: 4 x 1400MHz; 2018 Broadcom BCM20837B0; aarch64; Cortex-A53 (410f034); <a href="#">supercep-20230630</a>
pi3hplus: 4 x 1400MHz; 2018 Broadcom BCM20837B0; aarch64; Cortex-A53 (410f034); <a href="#">supercep-20211232</a>
leeds: 8 x 1500MHz; 2015 ARMv8-A Cortex-A53; aarch64; Cortex-A53+crypto (410f034); <a href="#">supercep-20170704</a>
leeds: 8 x 1500MHz; 2015 ARMv8-A Cortex-A53; aarch64; Cortex-A53+crypto (410f034); <a href="#">supercep-20230630</a>
leeds: 8 x 1500MHz; 2015 ARMv8-A Cortex-A53; aarch64; Cortex-A53+crypto (410f034); <a href="#">supercep-20211232</a>
reegadesk3200c: 4 x 1820MHz; 2011 Rockchip RK3288; aarch64; Cortex-A53+crypto (410f034); <a href="#">supercep-20191221</a>
jetsontxt: 4 x 1734MHz; 2015 NVIDIA Tegra X1; aarch64; Cortex-A57+crypto (418f071); <a href="#">supercep-20191017</a>
warbear: 8 x 2000MHz; 2016 AMD Opteron A1100; aarch64; Cortex-A57+crypto (411f072); <a href="#">supercep-20200626</a>
pi4h: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); <a href="#">supercep-20211232</a>
rp16bunus64: 4 x 1500MHz; 2019 Broadcom BCM2711; aarch64; Cortex-A72 (410f083); <a href="#">supercep-20191221</a>
a7: 2 x 2100MHz; 2015 Mediatek MT8173; aarch64; Cortex-A72+crypto (418f080); <a href="#">supercep-20170904</a>
pmo145: 64 x 2500MHz; 2018 Cavium ThunderX2 CN9980; aarch64; ThunderX2 (431f0af1); <a href="#">supercep-20191017</a>