

crypto_kem
mceliece460896f
implementations

- 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 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



Table of processor specifications and benchmarks:

Processor	Configuration	Frequency	Architecture	SuperCop Score
Bobcat	2 x 1650MHz; 2011 AMD G-T56N; amd64; Bobcat (500F10);	1650MHz	amd64; Bobcat (500F10);	supercop-20230630
K8	m4650; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500F20);	1650MHz	amd64; Bobcat (500F20);	supercop-20200618
K10 65nm	naca; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fB2);	2000MHz	amd64; K8 (40fB2);	supercop-20170105
K10 45nm	gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100F23);	2194MHz	amd64; K10 65nm (100F23);	supercop-20171218
K10 32nm	hydra3; 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100F40);	3300MHz	amd64; K10 45nm (100F40);	supercop-20171218
Bulldozer	sonistar; 4 x 3200MHz; 2009 AMD Phenom II X4 955; amd64; K10 45nm (100F42);	3200MHz	amd64; K10 45nm (100F42);	supercop-20170904
Piledriver	hbaev; 1 x 1700MHz; 2010 AMD Athlon II Neo K125; amd64; K10 45nm (100F63);	1700MHz	amd64; K10 45nm (100F63);	supercop-20171218
Zen	hydra4; 4 x 2600MHz; 2011 AMD A6-3650; amd64; K10 32nm (300F10);	2600MHz	amd64; K10 32nm (300F10);	supercop-20230630
Zen 2	hydra5; 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300F10);	2900MHz	amd64; K10 32nm (300F10);	supercop-20230630
Zen 3	bobcat; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20);	4000MHz	amd64; Bulldozer (600F20);	supercop-20171218
Knights Landing	calista; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20);	4000MHz	amd64; Bulldozer (600F20);	supercop-20171218
Golden Cove	hydra4; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600F12);	3100MHz	amd64; Bulldozer (600F12);	supercop-20171218
Cascade Lake	hawer210; 4 x 4000MHz; 2012 AMD FX-8350; amd64; Bulldozer (600F20);	4000MHz	amd64; Bulldozer (600F20);	supercop-20230630
Tiger Lake	hydra9; 2 x 3800MHz; 2012 AMD A10-5800K; amd64; Piledriver (610F01);	3800MHz	amd64; Piledriver (610F01);	supercop-20171218
Skylake+512x2	hprariaty; 2 x 2000MHz; 2012 AMD A10-6650M; amd64; Piledriver (610F01);	2000MHz	amd64; Piledriver (610F01);	supercop-20200618
Ice Lake	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Comet Lake	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Cannon Lake	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Kaby Lake	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Skylake	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Broadwell+AES	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Haswell+AES	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Ivy Bridge+AES	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Sandy Bridge+AES	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Sandy Bridge	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Westmere	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Core 2 45nm	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Core 2 65nm	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Gracemont	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Tremont	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Goldmont Plus	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Goldmont	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Airmont	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Silvermont	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
Bonnell	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
ppc32 G3	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
riscv64 U54	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
mipso32 Octeon II	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
armeabi Armada	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
armeabi Cortex-A7	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
armeabi Cortex-A8	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
armeabi Cortex-A9+NEON	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
armeabi Cortex-A15	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 X-Gene	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 Cortex-A53	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 Cortex-A53+crypto	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 Cortex-A57+crypto	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 Cortex-A72	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 Cortex-A72+crypto	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628
aarch64 ThunderX2	zen4; 8 x 3000MHz; 2017 AMD Ryzen 7 1700; amd64; Zen (800H11);	3000MHz	amd64; Zen (800H11);	supercop-20170628

Time 524288 4194304 33554432 268435456