The new SHA-3 software shootout

D. J. Bernstein
University of Illinois at Chicago

Tanja Lange
Technische Universiteit Eindhoven

The eBASH data flow
One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.
Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc.
Record median of differences of cycle-counter outputs.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc. Record median of differences of cycle-counter outputs.

User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software. Report median and quartiles.


Record median and quartiles for sha256 on hydra6 using the best software.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc.

Record median of differences of cycle-counter outputs.

More sha256 implementations.

> 1000 sets of compiler options.

Try all possibilities.

Build best sha256 software for hydra6: best implementation with best compiler options.

User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software.

Report median and quartiles.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc. Record median of differences of cycle-counter outputs.

More sha256 implementations.

More sha256 implementations.

> 1000 sets of compiler options.

Try all possibilities.

Build best sha256 software for hydra6: best implementation with best compiler options.

User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software.

Report median and quartiles.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc. Record median of differences of cycle-counter outputs.


Record many cycle counts for sha256 on hydra6 using the best software. Report median and quartiles.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

CPU cycle counter, hash, cycle counter, hash, cycle counter, hash, etc. Record median of differences of cycle-counter outputs.


Record many cycle counts for sha256 on hydra6 using the best software. Report median and quartiles.

hydra6 is just one of 180 computers in our database. 56 computers have run this year's benchmarks. Thanks to all the contributors! bench.cr.yp.to/computers.html

And thanks to NIST for funding. ⇒ 56 reasonably up-to-date measurements of sha256.
The eBASH data flow

One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc.

Record median of differences of cycle-counter outputs.

More sha256 implementations. >1000 sets of compiler options.

Try all possibilities.

Build best sha256 software for hydra6: best implementation with best compiler options.

User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software.

Report median and quartiles.

hydra6 is just one of 180 computers in our database.

56 computers have run this year’s benchmarks.

Thanks to all the contributors!

bench.cr.yp.to/computers.html

And thanks to NIST for funding.

⇒ 56 reasonably up-to-date measurements of sha256.
The eBASH data flow
One computer, hydra6, tries hashing data with the sphlib implementation of sha256, compiled with gcc -O3 -fomit-frame-pointer.

Read CPU cycle counter, hash, read cycle counter, hash, read cycle counter, hash, etc.

Record median of differences of cycle-counter outputs.

More sha256 implementations. >1000 sets of compiler options.

Try all possibilities.
Build best sha256 software for hydra6: best implementation with best compiler options.
User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software.
Report median and quartiles.

hydra6 is just one of 180 computers in our database.

56 computers have run this year's benchmarks.
Thanks to all the contributors!
bench.cr.yp.to /computers.html
And thanks to NIST for funding.
⇒ 56 reasonably up-to-date measurements of sha256.
More sha256 implementations. 
> 1000 sets of compiler options.

Try all possibilities.
Build best sha256 software for hydra6: best implementation with best compiler options.
User who cares about speed will obtain this performance.

Record many cycle counts for sha256 on hydra6 using the best software.
Report median and quartiles.

hydra6 is just one of 180 computers in our database.

56 computers have run this year’s benchmarks.
Thanks to all the contributors! bench.cr.yp.to/computers.html
And thanks to NIST for funding.

⇒ 56 reasonably up-to-date measurements of sha256.

hydra6 is just one of 180 computers in our database. 56 computers have run this year’s benchmarks. Thanks to all the contributors! bench.cr.yp.to/computers.html And thanks to NIST for funding.

56 reasonably up-to-date measurements of sha256.

sha256 is just one of many hash functions. Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors! bench.cr.yp.to/primitives-hash.html
sha256 is just one of many hash functions. Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html
hydra6 is just one of 180 computers in our database.

56 computers have run this year's benchmarks. Thanks to all the contributors!
bench.cr.yp.to/computers.html

And thanks to NIST for funding.

⇒ 56 reasonably up-to-date measurements of sha256.

sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!
bench.cr.yp.to/primitives-hash.html
hydra6 is just one of 180 computers in our database. 56 computers have run this year’s benchmarks. Thanks to all the contributors! bench.cr.yp.to/computers.html

And thanks to NIST for funding.

⇒ 56 reasonably up-to-date measurements of SHA-256.

sha256 is just one of many hash functions. Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors! bench.cr.yp.to/primitives-hash.html
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to
/primitives-hash.html
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html

SHA-{2,3}-{256,512}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512.
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html

SHA-{2,3}--{256,512}:

56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512.
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to /primitives-hash.html

SHA-{2,3}--{256,512}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512. ...
... for many message sizes.
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html

SHA-\{2,3\}-\{256,512\}:

56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccak-c1024, skein512256, skein512512. … for many message sizes.

How to understand all this data?
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-3: 307 implementations of 24 hash functions in 5 families.

Thanks to all the contributors!

bench.cr.yp.to/primitives-hash.html

SHA-\{2,3\}-\{256,512\}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccak-c1024, skein512256, skein512512. ... for many message sizes.

How to understand all this data?

The new shootout graphs are organized by microarchitecture.
sha256 is just one of many hash functions.

Public benchmarking suite contains 715 implementations of 98 hash functions in 36 families.

SHA-{2,3}-{256,512}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512. ... for many message sizes.

How to understand all this data?
The new shootout graphs are organized by microarchitecture.

Microarchitectures:

AMD, high-power, 64-bit:

* amd64 K8:
  - 2005 AMD Opteron 875,
  - 2006 AMD Athlon 64 X2, etc.

* amd64 K10 65nm:
  - 2008 AMD Opteron 8354,
  - 2008 AMD Phenom 9550, etc.

* amd64 K10 45nm:
  - 2008 AMD Opteron 2376,
  - 2010 AMD Phenom II X6 1100T, etc.

* amd64 K10 32nm:
  - 2011 AMD A8-3850, etc.

bencr.yp.to
primitives-hash.html

Thanks to all the contributors!
SHA-\(\{2,3\}\)-\(\{256,512\}\):

56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512.

... for many message sizes.

How to understand all this data?

The new shootout graphs are organized by microarchitecture.

Microarchitectures

AMD, high-power, 64-bit:

**amd64 K8:**
- 2005 AMD Opteron 875
- 2006 AMD Athlon 64 X2 etc.

**amd64 K10 65nm:**
- 2008 AMD Opteron 8354
- 2008 AMD Phenom 9550 etc.

**amd64 K10 45nm:**
- 2008 AMD Opteron 2376
- 2010 AMD Phenom II X6 1100T etc.

**amd64 K10 32nm:**
- 2011 AMD A8-3850, etc.

...
SHA-{2,3}-{256,512}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512. ... for many message sizes.

How to understand all this data?
The new shootout graphs are organized by microarchitecture.

Microarchitectures
AMD, high-power, 64-bit:

amd64 K8:
2005 AMD Opteron 875, 2006 AMD Athlon 64 X2, etc.

amd64 K10 65nm:
2008 AMD Opteron 8354, 2008 AMD Phenom 9550, etc.

amd64 K10 45nm:
2008 AMD Opteron 2376, 2010 AMD Phenom II X6 1100T, etc.

amd64 K10 32nm:
2011 AMD A8-3850, etc.
SHA-\{2,3\}-\{256,512\}:
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, groestl256, groestl512, round3jh256, round3jh512, keccakc512, keccakc1024, skein512256, skein512512. ... for many message sizes.

How to understand all this data?
The new shootout graphs are organized by microarchitecture.

Microarchitectures
AMD, high-power, 64-bit:

amd64 K8:
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

amd64 K10 65nm:
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

amd64 K10 45nm:
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T, etc.

amd64 K10 32nm:
2011 AMD A8-3850, etc.
56 reasonably up-to-date measurements of sha256, sha512, blake256, blake512, gr
testl512, jh256, round3jh512, c512, keccak512, 1256, skein512256, skein512512.
for many message sizes.

How to understand all this data?

The new shootout graphs are organized by microarchitecture.

Microarchitectures
AMD, high-power, 64-bit:

amd64 K8:
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

amd64 K10 65nm:
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

amd64 K10 45nm:
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T, etc.

amd64 K10 32nm:
2011 AMD A8-3850, etc.

Intel, high-power, 64-bit:

amd64 C2 65nm:
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

amd64 C2 45nm:
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

amd64 Nehalem:
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

amd64 Westmere:
2011 Intel Core i5-480M, etc.
Microarchitectures

AMD, high-power, 64-bit:

*amd64 K8:*
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

*amd64 K10 65nm:*
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

*amd64 K10 45nm:*
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T,
2010 AMD Phenom II X6 1100T, etc.

*amd64 K10 32nm:*
2011 AMD A8-3850, etc.

Intel, high-power, 64-bit:

*amd64 C2 65nm:*
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E6400, etc.

*amd64 C2 45nm:*
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

*amd64 Nehalem:*
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

*amd64 Westmere:*
2011 Intel Core i5-480M, etc.

Microarchitectures

AMD, high-power, 64-bit:

*amd64 K8:*
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

*amd64 K10 65nm:*
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

*amd64 K10 45nm:*
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T,
etc.

*amd64 K10 32nm:*
2011 AMD A8-3850, etc.
Microarchitectures

AMD, high-power, 64-bit:

**amd64 K8:**
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

**amd64 K10 65nm:**
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

**amd64 K10 45nm:**
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T, etc.

**amd64 K10 32nm:**
2011 AMD A8-3850, etc.

Intel, high-power, 64-bit:

**amd64 C2 65nm:**
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

**amd64 C2 45nm:**
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

**amd64 Nehalem:**
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

**amd64 Westmere:**
2011 Intel Core i5-480M, etc.
Microarchitectures

AMD, high-power, 64-bit:

amd64 K8:
2005 AMD Opteron 875,
2006 AMD Athlon 64 X2, etc.

amd64 K10 65nm:
2008 AMD Opteron 8354,
2008 AMD Phenom 9550, etc.

amd64 K10 45nm:
2008 AMD Opteron 2376,
2010 AMD Phenom II X6 1100T, etc.

amd64 K10 32nm:
2011 AMD A8-3850, etc.

Intel, high-power, 64-bit:

amd64 C2 65nm:
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

amd64 C2 45nm:
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

amd64 Nehalem:
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

amd64 Westmere:
2011 Intel Core i5-480M, etc.
Microarchitectures

AMD, high-power, 64-bit:

K8:
MD Opteron 875,
MD Athlon 64 X2, etc.

K10 65nm:
MD Opteron 8354,
MD Phenom 9550, etc.

K10 45nm:
MD Opteron 2376,
MD Phenom II X6 1100T,

K10 32nm:
MD A8-3850, etc.

Intel, high-power, 64-bit:

amd64 C2 65nm:
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

amd64 C2 45nm:
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

amd64 Nehalem:
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

amd64 Westmere:
2011 Intel Core i5-480M, etc.

amd64 Westmere + AES:
2010 Intel Core i5-520M, etc.

amd64 Sandy Bridge:
2011 Intel Core i3-2310M, etc.

amd64 SB + AES:
2011 Intel Core i5-2500K, etc.
**AMD, high-power, 64-bit:**

**amd64 K8:**
- 2005 AMD Opteron 875,
- 2006 AMD Athlon 64 X2, etc.

**amd64 K10 65nm:**
- 2008 AMD Opteron 8354,
- 2008 AMD Phenom 9550, etc.

**amd64 K10 45nm:**
- 2008 AMD Opteron 2376,
- 2010 AMD Phenom II X6 1100T, etc.

**amd64 K10 32nm:**
- 2011 AMD A8-3850, etc.

**Intel, high-power, 64-bit:**

**amd64 C2 65nm:**
- 2006 Intel Core 2 Duo E6300,
- 2007 Intel Core 2 Duo E4600, etc.

**amd64 C2 45nm:**
- 2007 Intel Xeon E5420,
- 2008 Intel Core 2 Duo E8400, etc.

**amd64 Nehalem:**
- 2008 Intel Core i7 920,
- 2010 Intel Xeon X7560, etc.

**amd64 Westmere:**
- 2011 Intel Core i5-480M, etc.

**amd64 Sandy Bridge:**
- 2011 Intel Core i3-2310M, etc.

**amd64 SB + AES:**
- 2011 Intel Core i5-2500K, etc.
Intel, high-power, 64-bit:

**amd64 C2 65nm:**
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

**amd64 C2 45nm:**
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

**amd64 Nehalem:**
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

**amd64 Westmere:**
2011 Intel Core i5-480M, etc.

**amd64 Sandy Bridge:**
2011 Intel Core i3-2310M, etc.

**amd64 SB+AES:**
2011 Intel Core i5-2500K, etc.
Intel, high-power, 64-bit:

**amd64 C2 65nm:**
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

**amd64 C2 45nm:**
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

**amd64 Nehalem:**
2008 Intel Core i7 920,
2010 Intel Xeon X7560, etc.

**amd64 Westmere:**
2011 Intel Core i5-480M, etc.

**amd64 Westmere + AES:**
2010 Intel Core i5-520M, etc.

**amd64 Sandy Bridge:**
2011 Intel Core i3-2310M, etc.

**amd64 SB + AES:**
2011 Intel Core i5-2500K, etc.
high-power, 64-bit:

**C2 65nm:**
- Intel Core 2 Duo E6300, etc.
- Intel Core 2 Duo E4600, etc.

**C2 45nm:**
- Intel Xeon E5420, etc.
- Intel Core 2 Duo E8400, etc.

**Nehalem:**
- Intel Core i7 920, etc.
- Intel Xeon X7560, etc.

**Westmere:**
- Intel Core i5-480M, etc.

amd64 Westmere+AES:
- 2010 Intel Core i5-520M, etc.

amd64 Sandy Bridge:
- 2011 Intel Core i3-2310M, etc.

amd64 SB+AES:
- 2011 Intel Core i5-2500K, etc.

amd64 Westmere
Intel/AMD, low-power:

**x86 Atom:**
- 2008 Intel Atom Z520 (2W), etc.
- 2009 Intel Atom N280 (2.5W), etc.
- 2011 Intel Atom Z670 (3W), etc.
- 2012 Intel Atom Z2460 (1W), etc.

**amd64 Atom:**
- 2009 Intel Atom D510 (13W), etc.
- 2010 Intel Atom N455 (6.5W), etc.

**amd64 Bobcat:**
- 2011 AMD E-450 (18W), etc.

amd64 SB:
- 2009 Intel Core 2 Duo E4600, etc.
- 2010 Intel Core 2 Duo E8400, etc.
- 2011 Intel Core i5-2500K, etc.

amd64 Sandy Bridge:
- 2011 Intel Core i3-2310M, etc.

amd64 SB+AES:
- 2011 Intel Core i5-2500K, etc.

amd64 Westmere

amd64 Westmere+AES:
2010 Intel Core i5-520M, etc.

amd64 Sandy Bridge:
2011 Intel Core i3-2310M, etc.

amd64 SB+AES:
2011 Intel Core i5-2500K, etc.

Intel/AMD, low-power:
x86 Atom:
2008 Intel Atom Z520 (2W), etc.
2009 Intel Atom N280 (2.5W), etc.
2011 Intel Atom D510 (13W), etc.
2012 Intel Atom Z7560, etc.

amd64 Atom:
2009 Intel Atom D525, etc.
2010 Intel Atom N455, etc.

amd64 Bobcat:
2011 AMD E-450, etc.
amd64 Westmere+AES:
2010 Intel Core i5-520M, etc.

amd64 Sandy Bridge:
2011 Intel Core i3-2310M, etc.

amd64 SB+AES:
2011 Intel Core i5-2500K, etc.

Intel/AMD, low-power:
x86 Atom:
2008 Intel Atom Z520 (2W), etc.
2009 Intel Atom N280 (2.5W), etc.
2011 Intel Atom Z670 (3W), etc.
2012 Intel Atom Z2460 (1W), etc.

amd64 Atom:
2009 Intel Atom D510 (13W), etc.
2010 Intel Atom N455 (6.5W), etc.

amd64 Bobcat:
2011 AMD E-450 (18W), etc.
**amd64 Westmere + AES:**
2010 Intel Core i5-520M, etc.

**amd64 Sandy Bridge:**
2011 Intel Core i3-2310M, etc.

**amd64 SB + AES:**
2011 Intel Core i5-2500K, etc.

Intel/AMD, low-power:

**x86 Atom:**
2008 Intel Atom Z520 (2W),
2009 Intel Atom N280 (2.5W),
2011 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W?), etc.

**amd64 Atom:**
2009 Intel Atom D510 (13W),
2010 Intel Atom N455 (6.5W), etc.

**amd64 Bobcat:**
2011 AMD E-450 (18W), etc.
Westmere + AES:
Intel Core i5-520M, etc.

Sandy Bridge:
Intel Core i3-2310M, etc.

SB + AES:
Intel Core i5-2500K, etc.

Intel/AMD, low-power:

**x86 Atom:**
2008 Intel Atom Z520 (2W),
2009 Intel Atom N280 (2.5W),
2011 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W?), etc.

**amd64 Atom:**
2009 Intel Atom D510 (13W),
2010 Intel Atom N455 (6.5W), etc.

**amd64 Bobcat:**
2011 AMD E-450 (18W), etc.

Other manufacturers, low-power:

**armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N95, etc.

**armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

**armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

**x86 Eden:**
2006 Via Eden ULV, etc.

**ppc32 G4:**
Freescale e600, etc.
AMD Westmere + AES:
2010 Intel Core i5-520M, etc.
AMD Sandy Bridge:
2011 Intel Core i3-2310M, etc.
AMD SB + AES:
2011 Intel Core i5-2500K, etc.

Intel/AMD, low-power:
x86 Atom:
2008 Intel Atom Z520 (2W),
2009 Intel Atom N280 (2.5W),
2011 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W?), etc.
amd64 Atom:
2009 Intel Atom D510 (13W),
2010 Intel Atom N455 (6.5W),
etc.
amd64 Bobcat:
2011 AMD E-450 (18W), etc.

Other manufacturers, low-power:
armeabi ARM11:
2006 TI OMAP 2420 in Nokia N280, etc.
amreabi Tegra 2:
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.
amreabi Cortex A8:
2009 Freescale i.MX515,
Apple A4 in iPhone 4, etc.
x86 Eden:
2006 Via Eden ULV, etc.
ppc32 G4: Freescale e600, etc.
Intel/AMD, low-power:

**x86 Atom:**
2008 Intel Atom Z520 (2W),
2009 Intel Atom N280 (2.5W),
2011 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W?), etc.

**amd64 Atom:**
2009 Intel Atom D510 (13W),
2010 Intel Atom N455 (6.5W), etc.

**amd64 Bobcat:**
2011 AMD E-450 (18W), etc.

Other manufacturers, low-power:

**armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N280, etc.

**armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

**armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

**x86 Eden:**
2006 Via Eden ULV, etc.

**ppc32 G4:** Freescale e600, etc.
Intel/AMD, low-power:

**x86 Atom:**
2008 Intel Atom Z520 (2W),
2009 Intel Atom N280 (2.5W),
2011 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W?), etc.

**amd64 Atom:**
2009 Intel Atom D510 (13W),
2010 Intel Atom N455 (6.5W),
2011 AMD E-450 (18W), etc.

**amd64 Bobcat:**
2011 AMD E-450 (18W), etc.

Other manufacturers, low-power:

**armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N280, etc.

**armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

**armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

**x86 Eden:**
2006 Via Eden ULV, etc.

**ppc32 G4:** Freescale e600, etc.
### Intel/AMD, low-power:

#### x86 Atom:
- 2008 Intel Atom Z520 (2W),
- 2009 Intel Atom N280 (2.5W),
- 2011 Intel Atom Z670 (3W),
- 2012 Intel Atom Z2460 (1W?), etc.

#### amd64 Atom:
- 2009 Intel Atom D510 (13W),
- 2010 Intel Atom N455 (6.5W), etc.

#### amd64 Bobcat:
- 2011 AMD E-450 (18W), etc.

### Other manufacturers, low-power:

#### armeabi ARM11:
- 2006 TI OMAP 2420 in Nokia N280, etc.

#### armeabi Tegra 2:
- 2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

#### armeabi Cortex A8:
- 2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

#### x86 Eden:
- 2006 Via Eden ULV, etc.

#### ppc32 G4:
- Freescale e600, etc.

---

Not a comprehensive list.

Fujitsu K Computer uses sparc64 CPUs.

PlayStation 3 and many supercomputers use ppc64 CPUs.

Many routers use mips32 CPUs.

Many small devices use 16-bit or 8-bit CPUs.

See XBX for benchmarks.
Other manufacturers, low-power:

**armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N280, etc.

**armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

**armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

**x86 Eden:**
2006 Via Eden ULV, etc.

**ppc32 G4:** Freescale e600, etc.

Not a comprehensive list.
Fujitsu K Computer uses sparc64 CPUs.
PlayStation 3 and many supercomputers use ppc64 CPUs.
Many routers use mips32 CPUs.
Many small devices use 16-bit or 8-bit CPUs.
See XBX for benchmarks.
Other manufacturers, low-power:

 **armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N280, etc.

 **armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

 **armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

 **x86 Eden:**
2006 Via Eden ULV, etc.

 **ppc32 G4:** Freescale e600, etc.

Not a comprehensive list.

Fujitsu K Computer uses sparc64 CPUs.

PlayStation 3 and many supercomputers use ppc64 CPUs.

Many routers use mips32 CPUs.

Many small devices use 16-bit or 8-bit CPUs. See XBX for benchmarks.
Other manufacturers, low-power:

**armeabi ARM11:**
2006 TI OMAP 2420 in Nokia N280, etc.

**armeabi Tegra 2:**
2010 NVIDIA Tegra 2 in Samsung Galaxy Tab 10.1, etc.

**armeabi Cortex A8:**
2009 Freescale i.MX515, Apple A4 in iPhone 4, etc.

**x86 Eden:**
2006 Via Eden ULV, etc.

**ppc32 G4:** Freescale e600, etc.

Not a comprehensive list.

Fujitsu K Computer uses sparc64 CPUs.

PlayStation 3 and many supercomputers use ppc64 CPUs.

Many routers use mips32 CPUs.

Many small devices use 16-bit or 8-bit CPUs.

See XBX for benchmarks.
arm64  Cortex A8
arm64  Bulldozer
arm64  Bobcat
arm64  Nano
arm64  Atom
x86  Atom
x86  Eden
ppc32  G4
armeabi  Cortex A8
armeabi  Tegra 2
armeabi  ARM11

<table>
<thead>
<tr>
<th>Cycles per byte</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
http://bench.cr.yp.to

20120321

groestl512

d3jh256

nanetsu; 4 x 3100MHz; 2011 Intel Core i5-2400; amd64; SB+AES (206a7); supercop-20120310

b6sandy; 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20120310

bridge; 2 x 2100MHz; 2011 Intel Core i3-2310M; amd64; Sandy Bridge (206a7); supercop-20120310

hydra2; 4 x 2400MHz; 2010 Intel Xeon E5620; amd64; Westmere+AES (206c2); supercop-20120310

bazanga; 2 x 2800MHz; 2010 Intel Pentium G6950; amd64; Westmere (20652); supercop-20111120

dragon; 8 x 2000MHz; 2009 Intel Xeon E5504; amd64; Nehalem (106a5); supercop-20120310

cobaltnaga; 8 x 2400MHz; 2009 Intel Xeon E5530; amd64; Nehalem (106a5); supercop-20110929

sto02; 2 x 1995MHz; 2010 Intel Xeon E5503; amd64; Nehalem (106a5); supercop-20120310

sto01; 2 x 1995MHz; 2010 Intel Xeon E5503; amd64; Nehalem (106a5); supercop-20120310

web02; 4 x 2128MHz; 2009 Intel Xeon E5506; amd64; Nehalem (106a5); supercop-20120310

web01; 4 x 2128MHz; 2009 Intel Xeon E5506; amd64; Nehalem (106a5); supercop-20120310

boing; 2 x 3000MHz; 2008 Intel Core 2 Duo E8400; amd64; C2 45nm (1067a); supercop-20120310

floodyberry; 2 x 2500MHz; 2008 Intel Pentium E5200; amd64; C2 45nm (1067a); supercop-20120310

berlekamp; 4 x 2833MHz; 2008 Intel Core 2 Quad Q9550; amd64; C2 45nm (10677); supercop-20120310

jos; 4 x 2494MHz; 2007 Intel Xeon E5420; amd64; C2 45nm (10676); supercop-20120219

gcc14; 8 x 2992MHz; 2007 Intel Xeon X5450; amd64; C2 45nm (10676); supercop-20120310

giant5; 8 x 2666MHz; 2007 Intel Xeon E5450; amd64; C2 45nm (10676); supercop-20120707

katana; 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (8f6); supercop-20120310

la tour; 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (8f6); supercop-20120310

nargues; 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (8f6); supercop-20120310

utrecht; 4 x 2405MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (8f6); supercop-20120310

trident; 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; C2 65nm (8f6); supercop-20120310

hydra4; 4 x 2600MHz; 2011 AMD A6-3650; amd64; K10 32nm (300f10); supercop-20120310

hydra5; 4 x 2900MHz; 2011 AMD A8-3850; amd64; K10 32nm (300f10); supercop-20120310

phenom; 6 x 2800MHz; 2010 AMD Phenom II X6 1055T; amd64; K10 45nm (100fa0); supercop-20120310

hydra3; 6 x 3300MHz; 2010 AMD Phenom II X6 1100T; amd64; K10 45nm (100fa0); supercop-20120310

agamemnon; 6 x 3200MHz; 2010 AMD Phenom II X6 1090T; amd64; K10 45nm (100fa0); supercop-20111120

hydra1; 6 x 3200MHz; 2010 AMD Phenom II X6 1090T; amd64; K10 45nm (100fa0); supercop-20120310

ranger; 4 x 2200MHz; 2008 AMD Phenom 9550; amd64; K10 65nm (100f23); supercop-20120310

gcc16; 8 x 2194MHz; 2008 AMD Opteron 8354; amd64; K10 65nm (100f23); supercop-20120310