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 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.

More sha256 implementations.
> 1000 sets of compiler options.
Try all possibilities.
Build best sha256 software for hydra6 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.

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.

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.


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! Thanks to NIST for funding.

And that ⇒ 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.
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, 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.
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.

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
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.

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 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
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.
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, keccak1024, 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!

dl://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, keccak1024, 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, keccakc1024, 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.
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 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, 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.

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

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.
56 reasonably up-to-date measurements of SHA-256, SHA-512, 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.

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:

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

**amd64 K10 65nm:**
- 2008 AMD Opteron 8354,
- 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.
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.
amd64 Sandy Bridge:
2011 Intel Core i3-2310M, etc.
amd64 SB+AES:
2011 Intel Core i5-2500K, etc.
amd64 Westmere+AES:
2010 Intel Core i5-520M, 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 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:

**amd64 Westmere+:**
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.

Intel, high-power, 64-bit:

**amd64 Westmere:**
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

**amd64 C2 65nm:**
2007 Intel Xeon E5420,
2008 Intel Core 2 Duo E8400, etc.

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

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

**Westmere:**
2009 Intel Core i5-480M, etc.
2010 Intel Xeon X7560, etc.

2011 AMD E-450 (18W), etc.

2011 Intel Core i5-480M, etc.

2011 Intel Core i3-2310M, 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, 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:
2006 Intel Core 2 Duo E6300,
2007 Intel Core 2 Duo E4600, etc.

amd64 C2 65nm:
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.

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 Intel Atom Z670 (3W),
2012 Intel Atom Z2460 (1W), 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?),
e tc.

**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), 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.
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),
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.
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.
crypto_sha3  Long messages
skein512512  blake512  sha512  keccak512  round3jh512  groestl512
skein512256  blake256  keccak256  sha256  groestl256  round3jh256

ad64 SB+AES
ad64 Sandy Bridge
ad64 Westmre+AES
ad64 Westmre
ad64 Nehalem
ad64 C2 45nm
ad64 C2 65nm
ad64 K10 32nm
ad64 K10 45nm
ad64 K10 65nm
ad64 K8
ad64 Bulldozer
ad64 Bobcat
ad64 Nano
ad64 Atom
x86 Atom
x86 Eden
ppc32 G4
armabi Cortex A8
armabi Tegra 2
armabi ARM11
<table>
<thead>
<tr>
<th></th>
<th>Cycles per byte</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>64</td>
</tr>
</tbody>
</table>

- **amd64 K8**
- **amd64 Bulldozer**
- **amd64 Bobcat**
- **amd64 Nano**
- **amd64 Atom**
- **x86 Atom**
- **x86 Eden**
- **ppc32 G4**
- **armeabi Cortex A8**
- **armeabi Tegra 2**
- **armeabi ARM11**