

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.

software shootout

ernstein

ty of Illinois at Chicago

ange

the 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 sh

>1000 s

Try all p

Build *be*

for hydr

with *bes*

User wh

will obta

Record r

for sha2

using th

Report r

ootout

is at Chicago

siteit 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 imp

>1000 sets of com

Try all possibilities

Build *best* sha256

for hydra6: *best*

with *best* compiler

User who cares ab

will obtain this pe

Record many cycle

for sha256 on hyc

using the best soft

Report median and

## 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

ago

hoven

## 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.

## SHA data flow

computer, hydra6,  
hashing data with  
Lib implementation  
56, compiled with  
-fomit-frame-pointer.  
CPU cycle counter, hash,  
le counter, hash,  
le counter, hash, etc.  
median of differences  
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  
compute  
56 comp  
this year  
Thanks  
[bench.c](#)  
[/compute](#)  
And tha  
⇒ 56 re  
measure

flow

dra6,

with

mentation

ed with

ame-pointer.

ounter, hash,

, hash,

, hash, etc.

differences

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

computers in our c

56 computers have

this year's benchm

Thanks to all the

[bench.cr.yp.to](http://bench.cr.yp.to)

[/computers.htm](http://computers.htm)

And thanks to NIS

⇒ 56 reasonably u

measurements of s

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](http://bench.cr.yp.to)

[/computers.html](http://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](http://bench.cr.yp.to)

[/computers.html](http://bench.cr.yp.to/computers.html)

And thanks to NIST for funding.

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

sha256 implementations.  
sets of compiler options.  
possibilities.  
best sha256 software  
ra6: *best* implementation  
st compiler options.  
o cares about speed  
in this performance.  
many cycle counts  
256 on hydra6  
e best software.  
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](http://bench.cr.yp.to/computers.html)  
And thanks to NIST for funding.  
⇒ 56 reasonably up-to-date  
measurements of sha256.

sha256  
of many  
Public b  
contains  
of 98 ha  
in 36 fa  
SHA-3:  
of 24 ha  
in 5 fam  
Thanks  
[bench.c  
/primit](http://bench.cr.yp.to/primit)

implementations.  
compiler options.

s.  
3 software  
implementation  
r options.  
out speed  
rformance.

e counts  
dra6  
ware.  
d 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](http://bench.cr.yp.to)

[/computers.html](http://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 func

Public benchmark  
contains 715 imple  
of 98 hash functio  
in 36 families.

SHA-3: 307 imple  
of 24 hash functio  
in 5 families.

Thanks to all the  
[bench.cr.yp.to](http://bench.cr.yp.to)  
[/primitives-ha](http://bench.cr.yp.to/primitives-ha)

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](http://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](http://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](http://bench.cr.yp.to)

[/computers.html](http://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](http://bench.cr.yp.to)

[/primitives-hash.html](http://bench.cr.yp.to/primitives-hash.html)

is just one of 180  
ers in our database.

outers have run  
's benchmarks.

to all the contributors!

[cr.yp.to](http://bench.cr.yp.to)

[primitives-hash.html](http://bench.cr.yp.to/primitives-hash.html)

anks to NIST for funding.

asonably up-to-date

ments 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](http://bench.cr.yp.to)

[/primitives-hash.html](http://bench.cr.yp.to/primitives-hash.html)

SHA-{2,

56 reaso

measure

sha512,

groestl

round3j

keccakc

skein51

e of 180  
database.

e run  
marks.

contributors!

L  
ST for funding.

up-to-date  
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](http://bench.cr.yp.to)

[/primitives-hash.html](http://bench.cr.yp.to/primitives-hash.html)

SHA- $\{2,3\}$ - $\{256,5$

56 reasonably up-t

measurements of s

sha512, blake256

groestl256, groe

round3jh256, rou

keccakc512, kecc

skein512256, ske

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](http://bench.cr.yp.to)

[/primitives-hash.html](http://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](http://bench.cr.yp.to)

[/primitives-hash.html](http://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](http://bench.cr.yp.to)

[/primitives-hash.html](http://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](http://bench.cr.yp.to)

[/primitives-hash.html](http://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?

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](http://bench.cr.yp.to)

[/primitives-hash.html](http://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.

is just one  
hash functions.  
enchmarking suite  
715 implementations  
sh functions  
amilies.  
307 implementations  
sh functions  
ilies.  
to all the contributors!  
[cr.yp.to](http://cr.yp.to)  
[notes-hash.html](http://cr.yp.to/notes-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.

Microarc

AMD, h

**amd64**

2005 AM

2006 AM

**amd64**

2008 AM

2008 AM

**amd64**

2008 AM

2010 AM

etc.

**amd64**

2011 AM

e  
ctions.  
ing suite  
ementations  
ns  
mentations  
ns  
contributors!  
[sh.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.

Microarchitectures

AMD, high-power,

**amd64 K8:**

2005 AMD Opteron

2006 AMD Athlon

**amd64 K10 65nr**

2008 AMD Opteron

2008 AMD Phenom

**amd64 K10 45nr**

2008 AMD Opteron

2010 AMD Phenom

etc.

**amd64 K10 32nr**

2011 AMD A8-385

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, et

### **amd64 K10 65nm:**

2008 AMD Opteron 8354,  
2008 AMD Phenom 9550, e

### **amd64 K10 45nm:**

2008 AMD Opteron 2376,  
2010 AMD Phenom II X6 1  
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.



3}-{256,512}:  
nably up-to-date  
ments of sha256,  
blake256, blake512,  
l256, groestl512,  
jh256, round3jh512,  
c512, keccakc1024,  
l2256, skein512512.  
many message sizes.  
understand all this data?  
y shootout graphs are  
d 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, hig

### **amd64**

2006 Int

2007 Int

### **amd64**

2007 Int

2008 Int

### **amd64**

2008 Int

2010 Int

### **amd64**

2011 Int

12}:  
to-date  
sha256,  
6, blake512,  
est1512,  
und3jh512,  
cakc1024,  
ein512512.  
sage sizes.

and all this data?

graphs are  
architecture.

## 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,

### **amd64 C2 65nm**

2006 Intel Core 2  
2007 Intel Core 2

### **amd64 C2 45nm**

2007 Intel Xeon E  
2008 Intel Core 2

### **amd64 Nehalem:**

2008 Intel Core i7  
2010 Intel Xeon X

### **amd64 Westmere**

2011 Intel Core i5-

## 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 E630  
2007 Intel Core 2 Duo E460

### **amd64 C2 45nm:**

2007 Intel Xeon E5420,  
2008 Intel Core 2 Duo E840

### **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.

## architectures

high-power, 64-bit:

### **K8:**

AMD Opteron 875,

AMD Athlon 64 X2, etc.

### **K10 65nm:**

AMD Opteron 8354,

AMD Phenom 9550, etc.

### **K10 45nm:**

AMD Opteron 2376,

AMD Phenom II X6 1100T,

### **K10 32nm:**

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**

2010 Int

### **amd64**

2011 Int

### **amd64**

2011 Int

64-bit:

on 875,  
64 X2, etc.

n:  
on 8354,  
m 9550, etc.

n:  
on 2376,  
m II X6 1100T,

n:  
50, 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:**

2010 Intel Core i5-

**amd64 Sandy Br**

2011 Intel Core i3-

**amd64 SB+AES**

2011 Intel Core i5-

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.

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.



gh-power, 64-bit:

### **C2 65nm:**

Intel Core 2 Duo E6300,

Intel Core 2 Duo E4600, etc.

### **C2 45nm:**

Intel Xeon E5420,

Intel Core 2 Duo E8400, etc.

### **Nehalem:**

Intel Core i7 920,

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.

Intel/AM

### **x86 Ato**

2008 Int

2009 Int

2011 Int

2012 Int

etc.

### **amd64**

2009 Int

2010 Int

etc.

### **amd64**

2011 AM

64-bit:

:

Duo E6300,

Duo E4600, etc.

:

5420,

Duo E8400, etc.

:

920,

7560, etc.

e:

-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.

Intel/AMD, low-p

**x86 Atom:**

2008 Intel Atom Z

2009 Intel Atom N

2011 Intel Atom Z

2012 Intel Atom Z

etc.

**amd64 Atom:**

2009 Intel Atom D

2010 Intel Atom M

etc.

**amd64 Bobcat:**

2011 AMD E-450

**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), et

### **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 m

### **armeabi**

2006 TI

Nokia N

### **armeabi**

2010 NV

Samsung

### **armeabi**

2009 Fre

Apple A

### **x86 Ede**

2006 Via

### **ppc32 C**

**e+AES:**

-520M, etc.

**idge:**

-2310M, etc.

**:**

-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

**armeabi ARM11:**

2006 TI OMAP 24

Nokia N280, etc.

**armeabi Tegra 2:**

2010 NVIDIA Tegra

Samsung Galaxy T

**armeabi Cortex A:**

2009 Freescale i.M

Apple A4 in iPhone

**x86 Eden:**

2006 Via Eden UL

**ppc32 G4:** Freesc

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-po

**armeabi ARM11:**

2006 TI OMAP 2420 in  
Nokia N280, etc.

**armeabi Tegra 2:**

2010 NVIDIA Tegra 2 in  
Samsung Galaxy Tab 10.1, e

**armeabi Cortex A8:**

2009 Freescale i.MX515,  
Apple A4 in iPhone 4, etc.

**x86 Eden:**

2006 Via Eden ULV, etc.

**ppc32 G4:** Freescale e600,

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.



MD, low-power:

**Atom:**

Intel Atom Z520 (2W),

Intel Atom N280 (2.5W),

Intel Atom Z670 (3W),

Intel Atom Z2460 (1W?),

**Atom:**

Intel Atom D510 (13W),

Intel Atom N455 (6.5W),

**Bobcat:**

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 co

Fujitsu k

uses spa

PlayStat

and mar

use ppc6

Many ro

use mips

Many sn

use 16-b

See XB>

ower:

520 (2W),  
280 (2.5W),  
670 (3W),  
2460 (1W?),

510 (13W),  
455 (6.5W),

(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 comprehens

Fujitsu K Comput  
uses sparc64 CPUs

PlayStation 3  
and many superco  
use ppc64 CPUs.

Many routers  
use mips32 CPUs.

Many small device  
use 16-bit or 8-bit  
See XBX for benc

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.

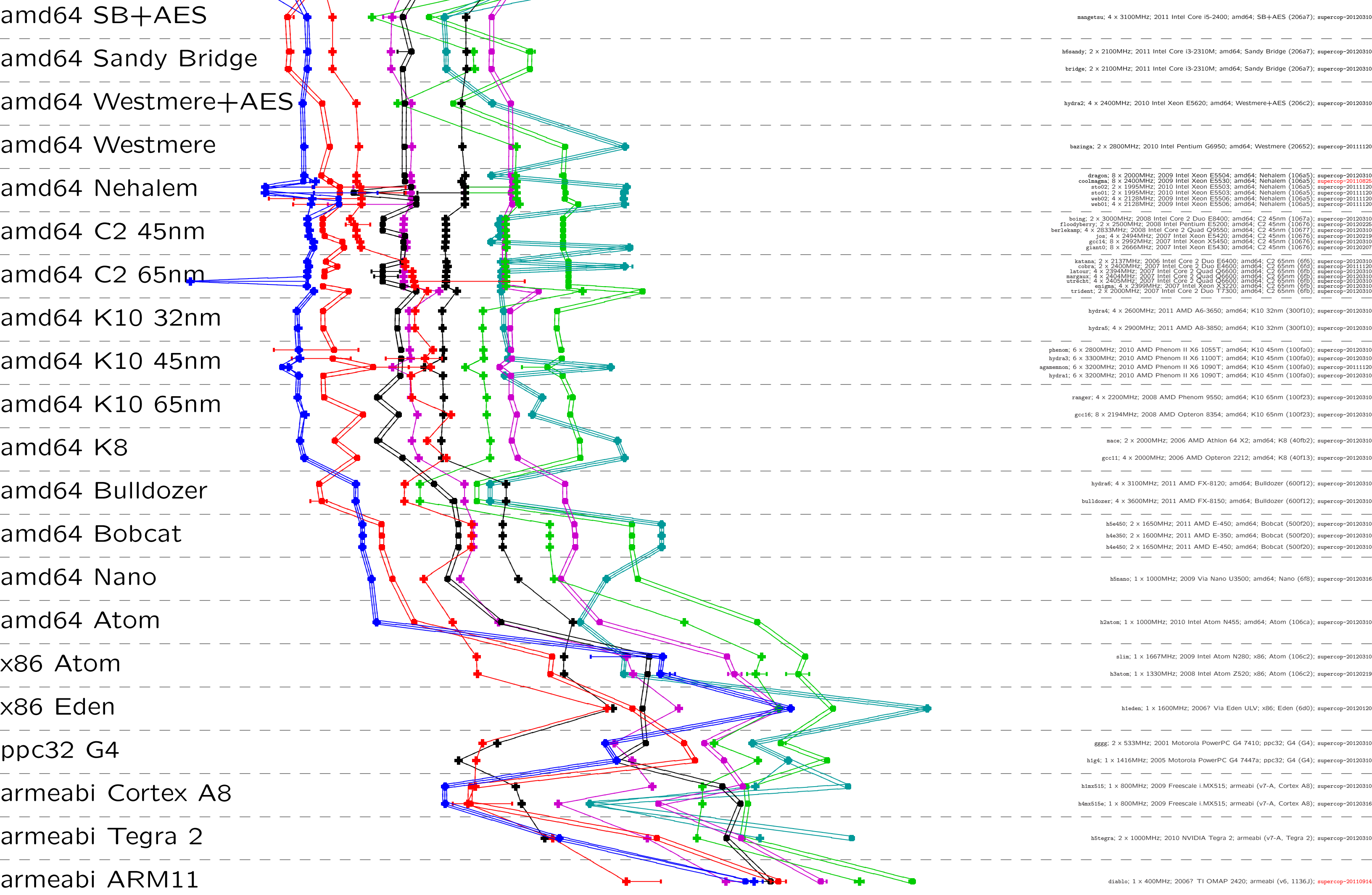
Many routers  
use mips32 CPUs.

Many small devices  
use 16-bit or 8-bit CPUs.  
See XBX for benchmarks.

crypto\_sha3  
Long messages

<http://bench.cr.yp.to/20120321>

skein512512    blake512    sha512    keccak1024    round3jh512    groest1512  
skein512256    blake256    keccak256    sha256    groest1256    round3jh256



Cycles per byte    4    8    16    32    64    128    256    512    1024    2048    4096

crypto\_sha3  
Long messages

skein512512    blake512    sha512    keccakc1024round3jh512  
skein512256    blake256    keccakc512    sha256    groestl1256    round3jh512

amd64 SB+AES

amd64 Sandy Bridge

amd64 Westmere+AES

amd64 Westmere

amd64 Nehalem

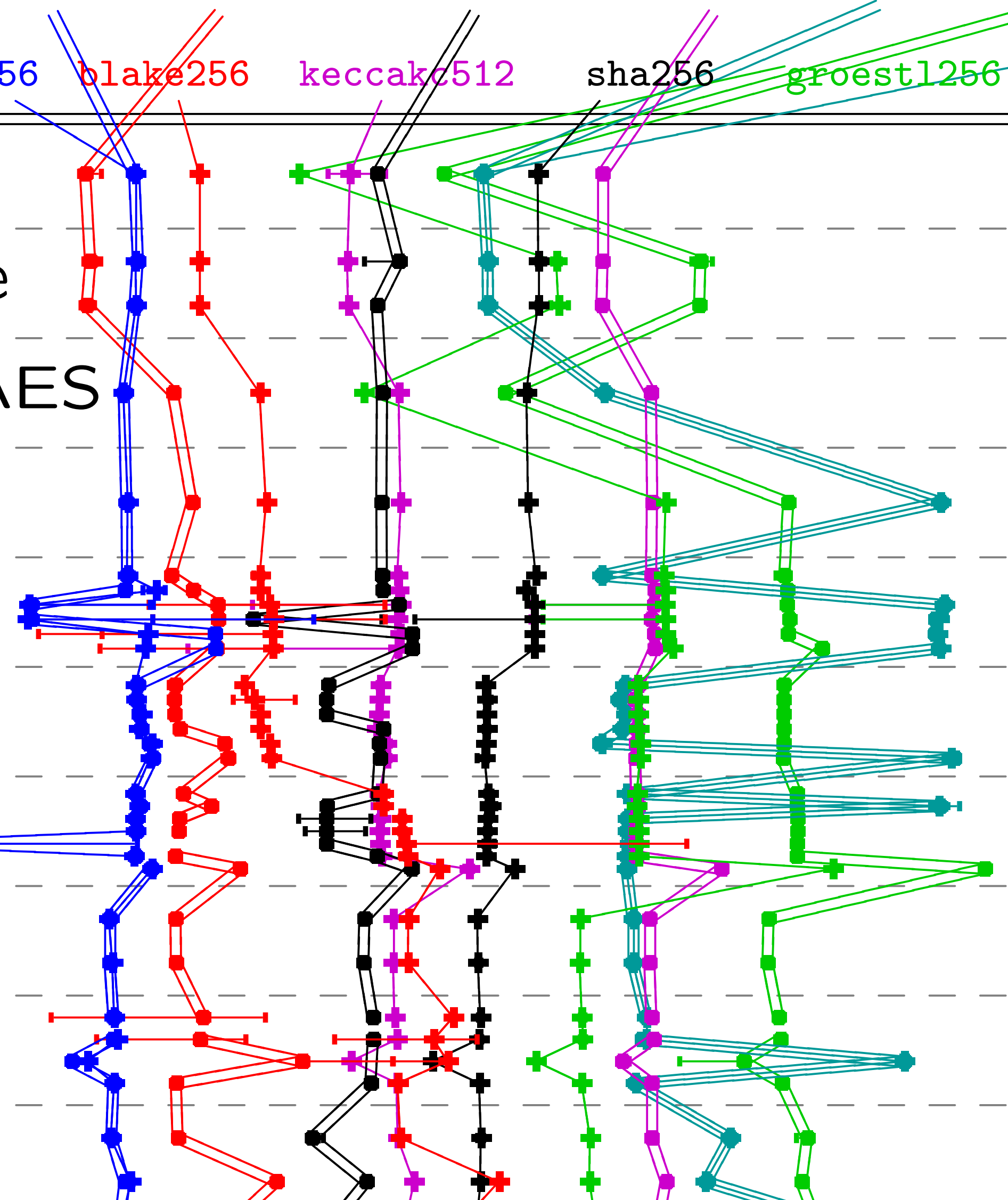
amd64 C2 45nm

amd64 C2 65nm

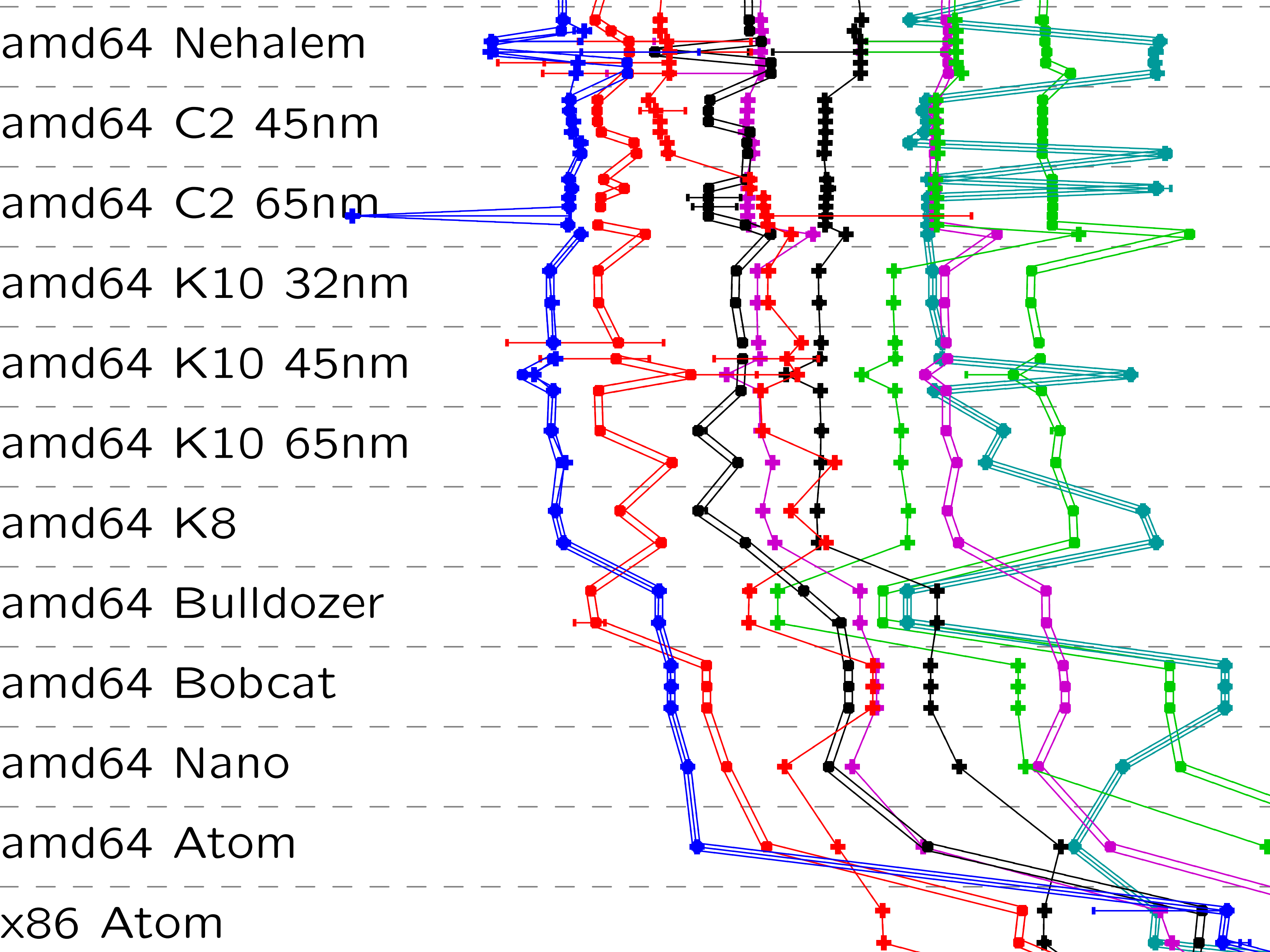
amd64 K10 32nm

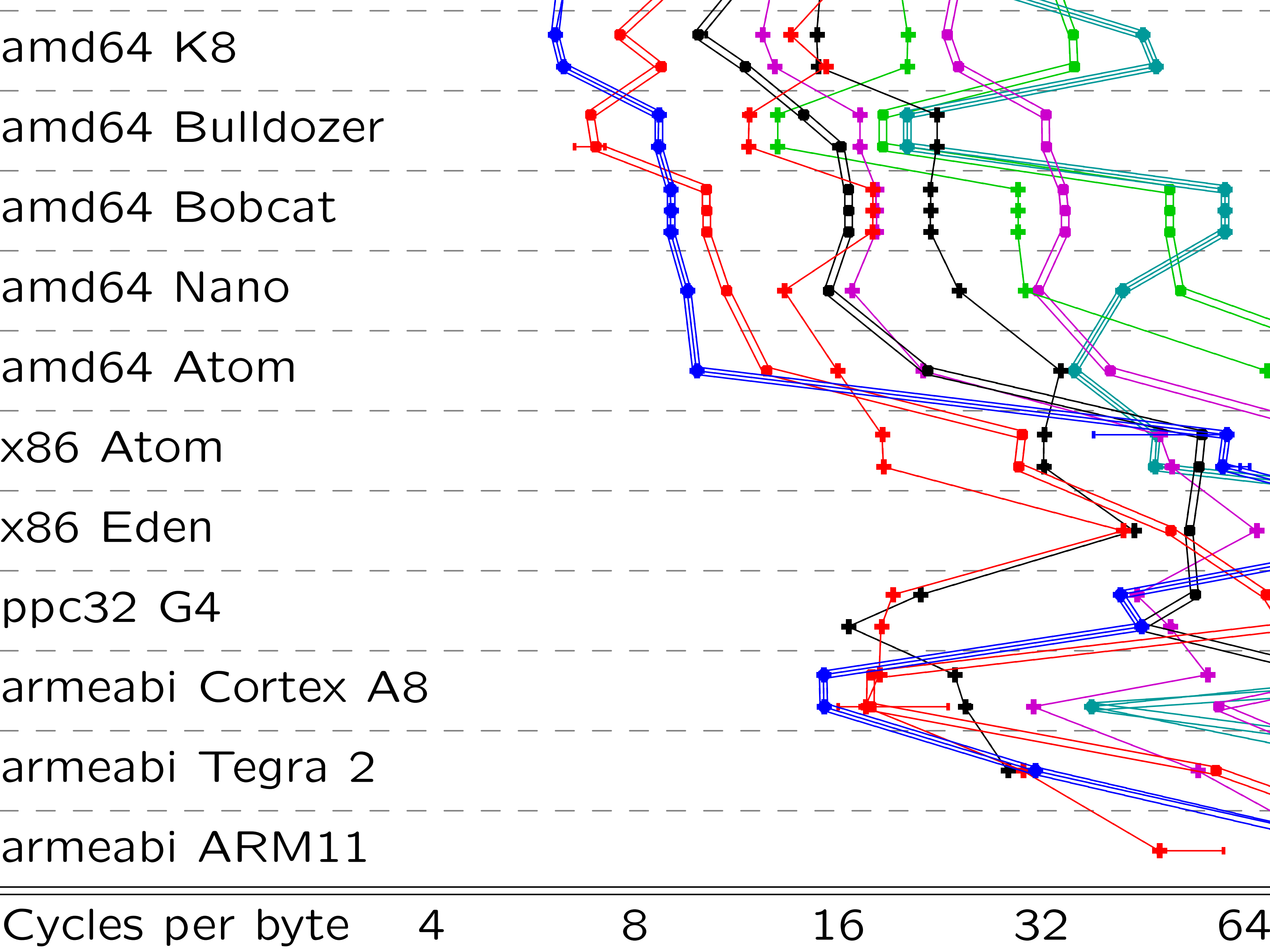
amd64 K10 45nm

amd64 K10 65nm





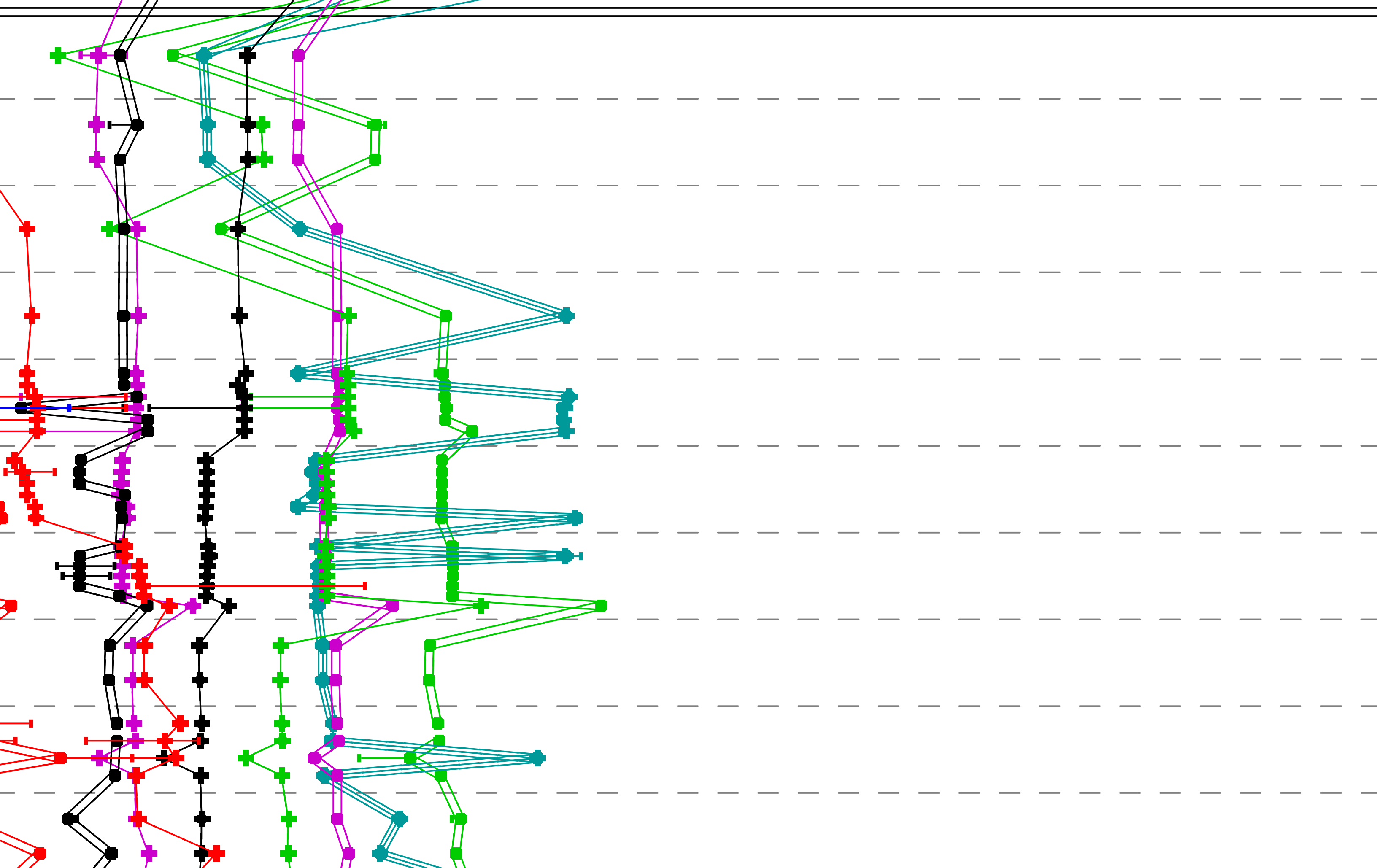


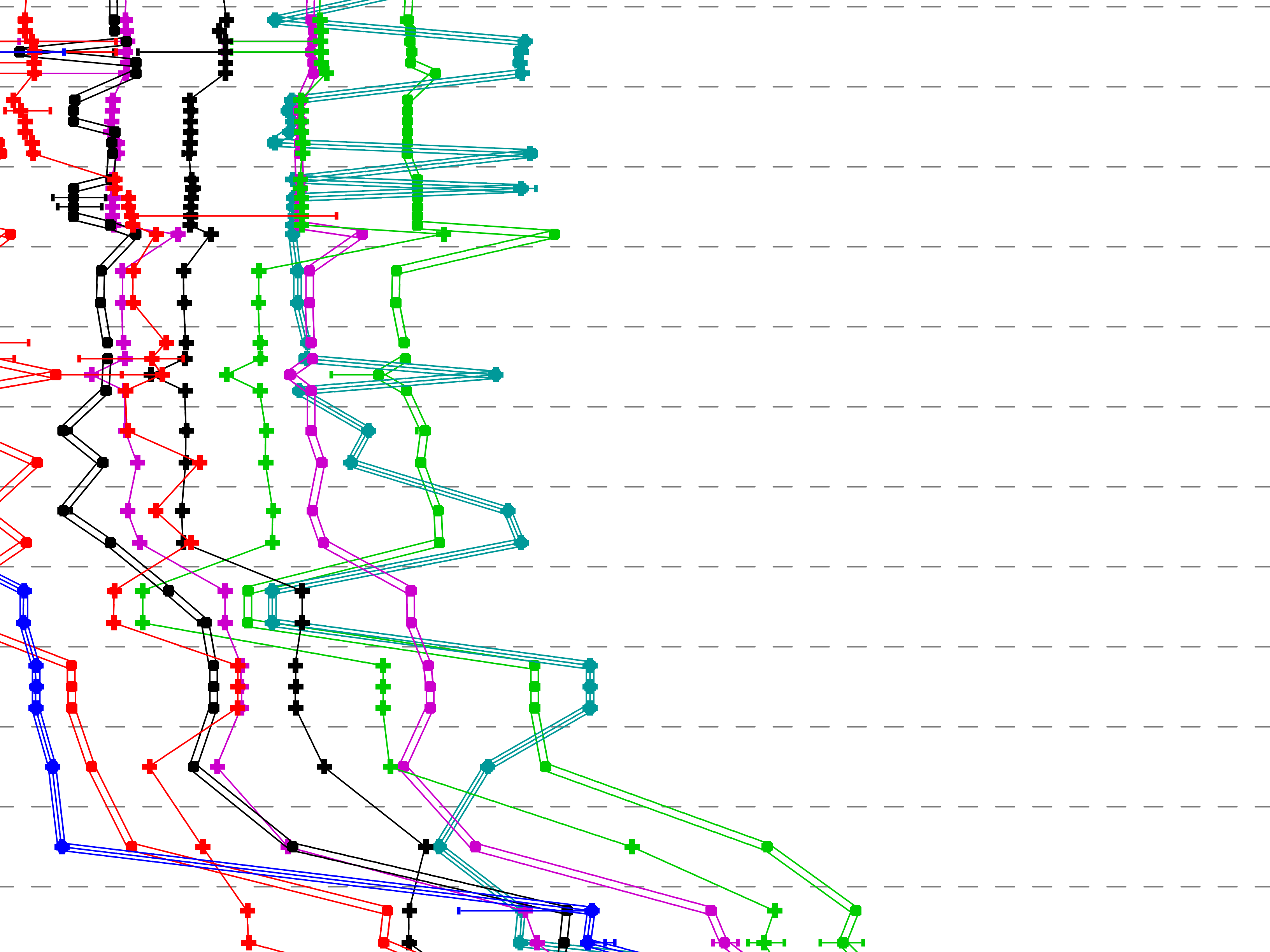


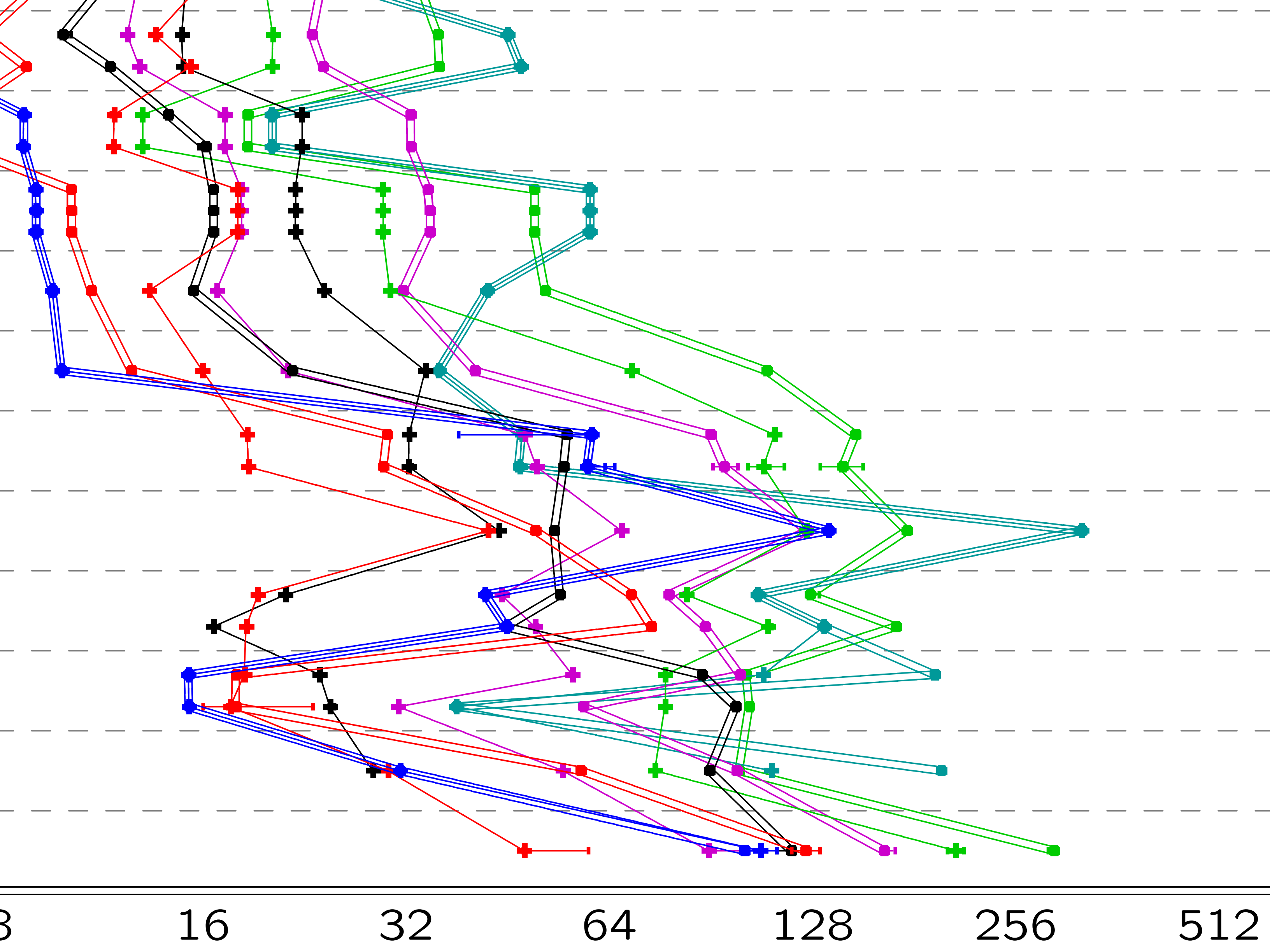


shake512 sha512 keccak1024 round3jh512 groestl1512

6 keccak512 sha256 groestl1256 round3jh256







2groest1512

nd3jh256

http://bench.cr.yp.to  
20120321

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

h6sandy; 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

bazinga; 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  
coolmagma; 8 x 2400MHz; 2009 Intel Xeon E5530; amd64; Nehalem (106a5); supercop-20110825  
sto02; 2 x 1995MHz; 2010 Intel Xeon E5503; amd64; Nehalem (106a5); supercop-20111120  
sto01; 2 x 1995MHz; 2010 Intel Xeon E5503; amd64; Nehalem (106a5); supercop-20111120  
web02; 4 x 2128MHz; 2009 Intel Xeon E5506; amd64; Nehalem (106a5); supercop-20111120  
web01; 4 x 2128MHz; 2009 Intel Xeon E5506; amd64; Nehalem (106a5); supercop-20111120

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 (10676); supercop-20120225  
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  
giant0; 8 x 2666MHz; 2007 Intel Xeon E5430; amd64; C2 45nm (10676); supercop-20120207

katana; 2 x 2137MHz; 2006 Intel Core 2 Duo E6400; amd64; C2 65nm (6f6); supercop-20120310  
cobra; 2 x 2400MHz; 2007 Intel Core 2 Duo E4600; amd64; C2 65nm (6fd); supercop-20111120  
latour; 4 x 2394MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6fb); supercop-20120310  
margaux; 4 x 2404MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6fb); supercop-20120310  
utrecht; 4 x 2405MHz; 2007 Intel Core 2 Quad Q6600; amd64; C2 65nm (6fb); supercop-20120310  
enigma; 4 x 2399MHz; 2007 Intel Xeon X3220; amd64; C2 65nm (6fb); supercop-20120310  
trident; 2 x 2000MHz; 2007 Intel Core 2 Duo T7300; amd64; C2 65nm (6fb); 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  
agamegnon; 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

