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.

v
software shootout

ernstein
ty of Illinois at Chicago

ange
che 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
for `sha2`
using th
Report

hootout

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* compile
User who cares ab
will obtain this pe

Record many cycle
for `sha256` on `hyd`
using the best soft
Report median an

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` implementatio
>1000 sets of compiler opti

Try all possibilities.
Build *best* `sha256` software
for `hydra6`: *best* implement
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.
$>$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.

ASH data flow

nputer, `hydra6`,
shing data with
`lib` implementation
56, compiled with
`-fomit-frame-pointer`.

PU 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
/comput
And tha

⇒ 56 re
measure

flow

dra6,
with
mentation
ed with
rame-pointer.

ounter, hash,
, hash,
, hash, etc.
differences
utputs.

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

56 computers have
this year's benchm
Thanks to all the
bench.cr.yp.to
/computers.html
And thanks to NIS

⇒ 56 reasonably u
measurements of

ter.

sh,

c.

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 contributo
`bench.cr.yp.to`
`/computers.html`
And thanks to NIST for fun

⇒ 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.

$\Rightarrow$ 56 reasonably up-to-date
measurements of `sha256`.

a256 implementations.
sets of compiler options.

possibilities.
est sha256 software
ra6: *best* implementation
st compiler options.
o cares about speed
ain 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
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

lementations.
npiler options.

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

e counts
dra6
tware.
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`
`/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 benchmarki
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`
`/primitives-has`

ons.
ons.

tation

.

s.

`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 implementation
of 98 hash functions
in 36 families.

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

Thanks to all the contributo
`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.

$\Rightarrow$ 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`

is just one of 180
ers in our database.

puters have run
r's benchmarks.
to all the contributors!
cr.yp.to
ters.html
nks 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
/primitives-hash.html

SHA-{2,

56 reaso
measure
sha512,
groestl
round3j
keccak
skein51

e of 180
database.

e run
narks.
contributors!

1

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
/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

rs!

ding.

`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`, `blake5`
`groestl256`, `groestl512`,
`round3jh256`, `round3jh51`
`keccakc512`, `keccakc1024`
`skein512256`, `skein51251`

`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`, `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`
`/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
milies.

307 implementations
sh functions
ilies.

to all the contributors!

cr.yp.to
tives-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 Opter
2006 AMD Athlon

amd64 K10 65nm
2008 AMD Opter
2008 AMD Pheno

amd64 K10 45nm
2008 AMD Opter
2010 AMD Pheno

etc.

amd64 K10 32nm
2011 AMD A8-385

ns

s

rs!

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`,
1256, `groestl512`,
jh256, `round3jh512`,
c512, `keccakc1024`,
12256, `skein512512`.
many message sizes.

understand all this data?

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

512}:

to-date
sha256,
6, blake512,
estl512,
und3jh512,
cakc1024,
ein512512.
sage sizes.

d all this data?

graphs are
barchitecture.

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-

12,

2,

,

2.

data?

re

ure.

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.

chitectures

igh-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

2010 Int

amd64

2011 Int

amd64

2011 Int

s

, 64-bit:

on 875,
n 64 X2, etc.

m:

on 8354,
m 9550, etc.

m:

on 2376,
m II X6 1100T,

m:

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 Westmer
2010 Intel Core i5-

amd64 Sandy Br
2011 Intel Core i3-

amd64 SB+AES
2011 Intel Core i5-

tc.

tc.

100T,

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, e

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

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:

tel Core 2 Duo E6300,

tel Core 2 Duo E4600, etc.

C2 45nm:

tel Xeon E5420,

tel Core 2 Duo E8400, etc.

Nehalem:

tel Core i7 920,

tel Xeon X7560, etc.

Westmere:

tel 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 N

etc.

amd64 Bobcat:

2011 AMD E-450

0,

0, etc.

0, etc.

c.

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:

tel Core i5-520M, etc.

Sandy Bridge:

tel Core i3-2310M, etc.

SB+AES:

tel 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 manufacture

armeabi ARM11:

2006 TI OMAP 24
Nokia N280, etc.

armeabi Tegra 2:

2010 NVIDIA Teg
Samsung Galaxy T

armeabi Cortex A

2009 Freescale i.M
Apple A4 in iPhon

x86 Eden:

2006 Via Eden UL

ppc32 G4: Freesc

c.

tc.

tc.

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:

om:

tel Atom Z520 (2W),
tel Atom N280 (2.5W),
tel Atom Z670 (3W),
tel Atom Z2460 (1W?),

Atom:

tel Atom D510 (13W),
tel Atom N455 (6.5W),

Bobcat:

MD 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 sm
use 16-b
See XBX

ower:

Z520 (2W),
N280 (2.5W),
Z670 (3W),
Z2460 (1W?),

D510 (13W),
N455 (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 CPU

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

,
W),
,
W?),
W),
W),
tc.

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.

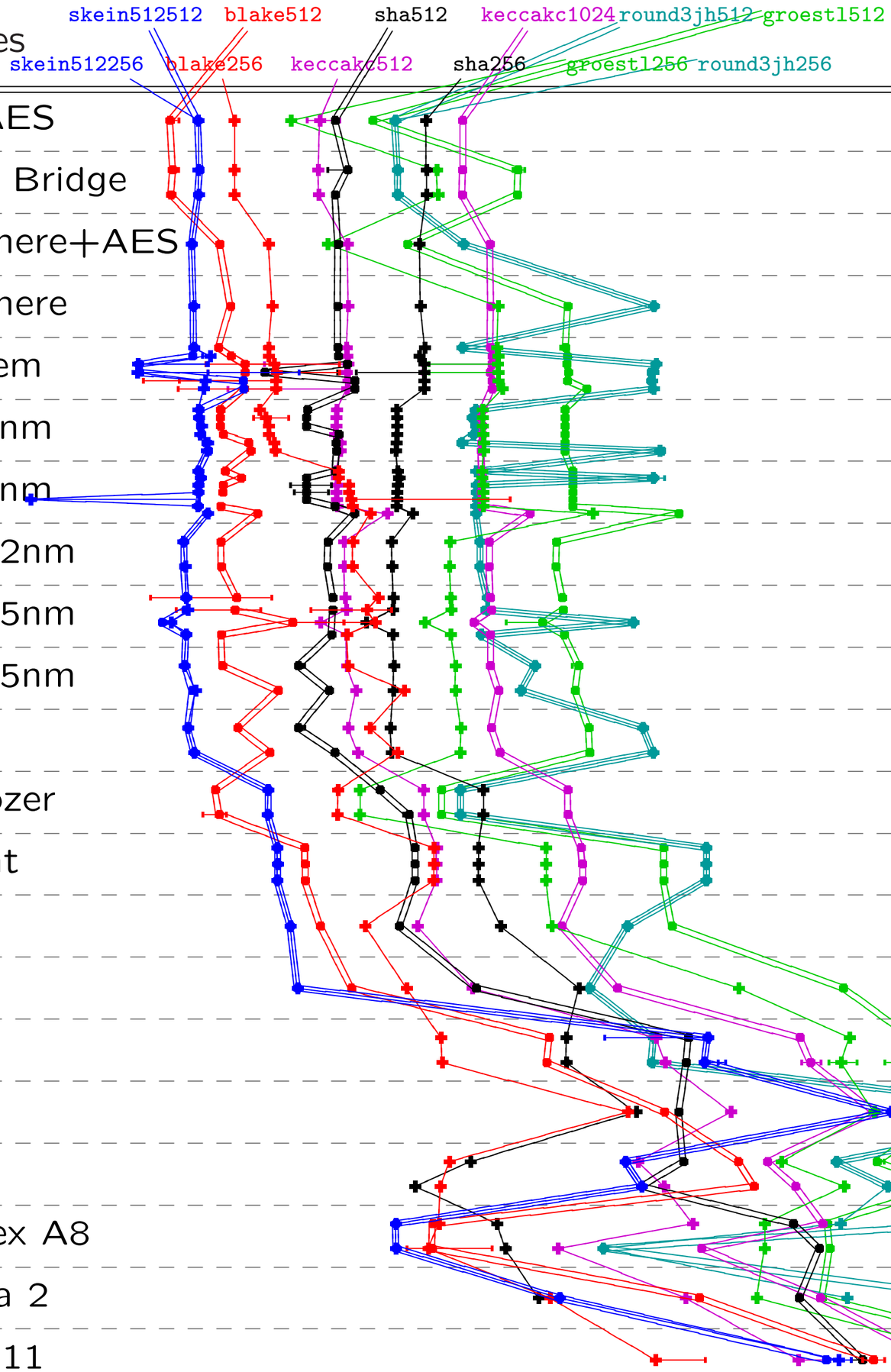
PlayStation 3
and many supercomputers
use ppc64 CPUs.

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



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

amd64 Sandy Bridge
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

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

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

amd64 Nehalem
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

amd64 C2 45nm
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

amd64 C2 65nm
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

amd64 K10 32nm
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

amd64 K10 45nm
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

amd64 K10 65nm
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

amd64 K8
mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20120310
gcc11; 4 x 2000MHz; 2006 AMD Opteron 2212; amd64; K8 (40f13); supercop-20120310

amd64 Bulldozer
hydra6; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20120310
bulldozer; 4 x 3600MHz; 2011 AMD FX-8150; amd64; Bulldozer (600f12); supercop-20120310

amd64 Bobcat
h5e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310
h4e350; 2 x 1600MHz; 2011 AMD E-350; amd64; Bobcat (500f20); supercop-20120310
h4e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310

amd64 Nano
h5nano; 1 x 1000MHz; 2009 Via Nano U3500; amd64; Nano (6f8); supercop-20120316

amd64 Atom
h2atom; 1 x 1000MHz; 2010 Intel Atom N455; amd64; Atom (106ca); supercop-20120310

x86 Atom
slim; 1 x 1667MHz; 2009 Intel Atom N280; x86; Atom (106c2); supercop-20120310
h3atom; 1 x 1330MHz; 2008 Intel Atom Z520; x86; Atom (106c2); supercop-20120219

x86 Eden
h1eden; 1 x 1600MHz; 2006? Via Eden ULV; x86; Eden (6d0); supercop-20120120

ppc32 G4
gggg; 2 x 533MHz; 2001 Motorola PowerPC G4 7410; ppc32; G4 (G4); supercop-20120310
h1g4; 1 x 1416MHz; 2005 Motorola PowerPC G4 7447a; ppc32; G4 (G4); supercop-20120310

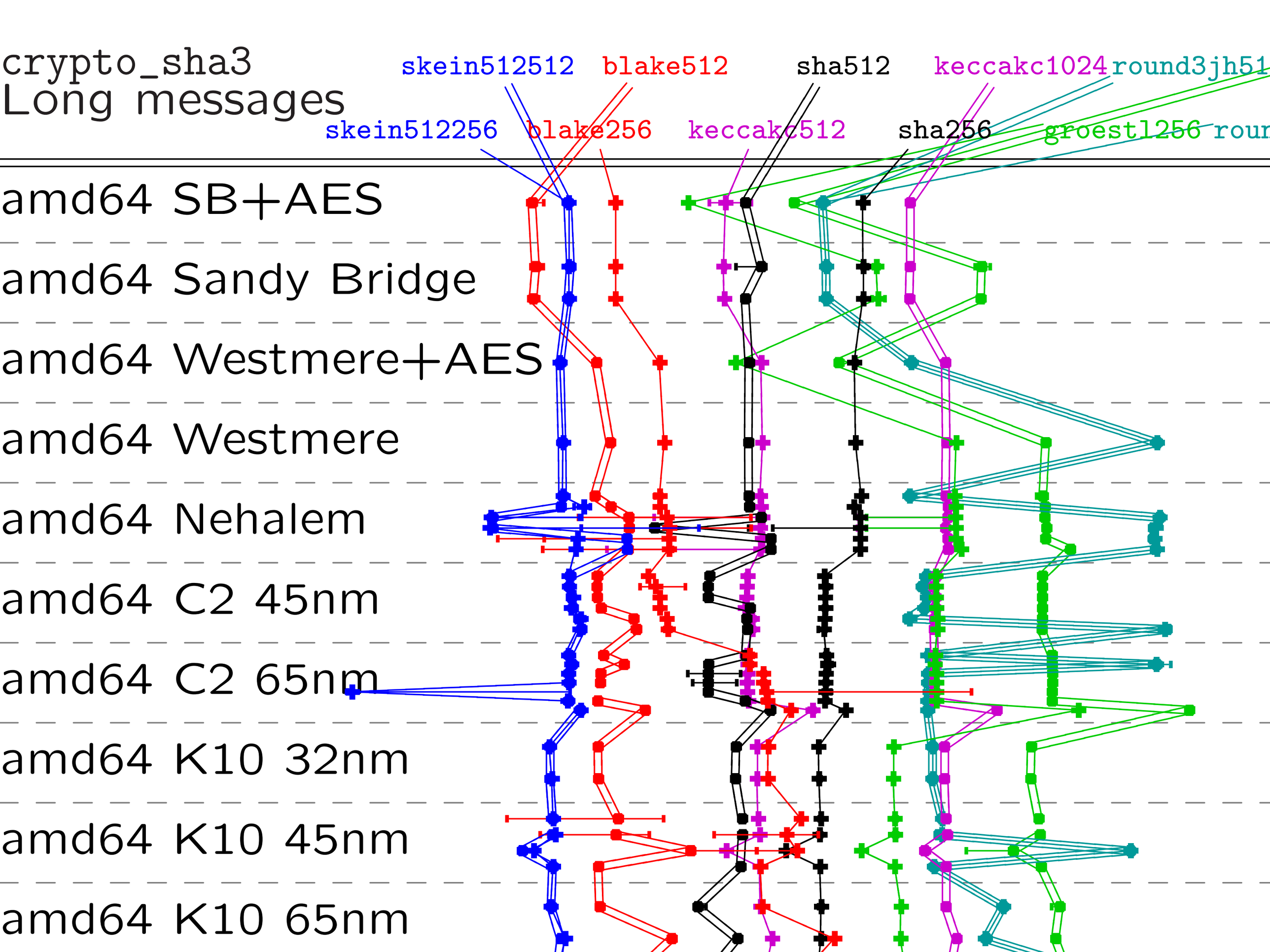
armeabi Cortex A8
h1mx515; 1 x 800MHz; 2009 Freescale i.MX515; armeabi (v7-A, Cortex A8); supercop-20120310
h4mx515e; 1 x 800MHz; 2009 Freescale i.MX515; armeabi (v7-A, Cortex A8); supercop-20120316

armeabi Tegra 2
h5tegra; 2 x 1000MHz; 2010 NVIDIA Tegra 2; armeabi (v7-A, Tegra 2); supercop-20120310

armeabi ARM11
diablo; 1 x 400MHz; 2006? TI OMAP 2420; armeabi (v6, 1136J); supercop-20110914

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

crypto_sha3
Long messages



amd64 Nehalem

amd64 C2 45nm

amd64 C2 65nm

amd64 K10 32nm

amd64 K10 45nm

amd64 K10 65nm

amd64 K8

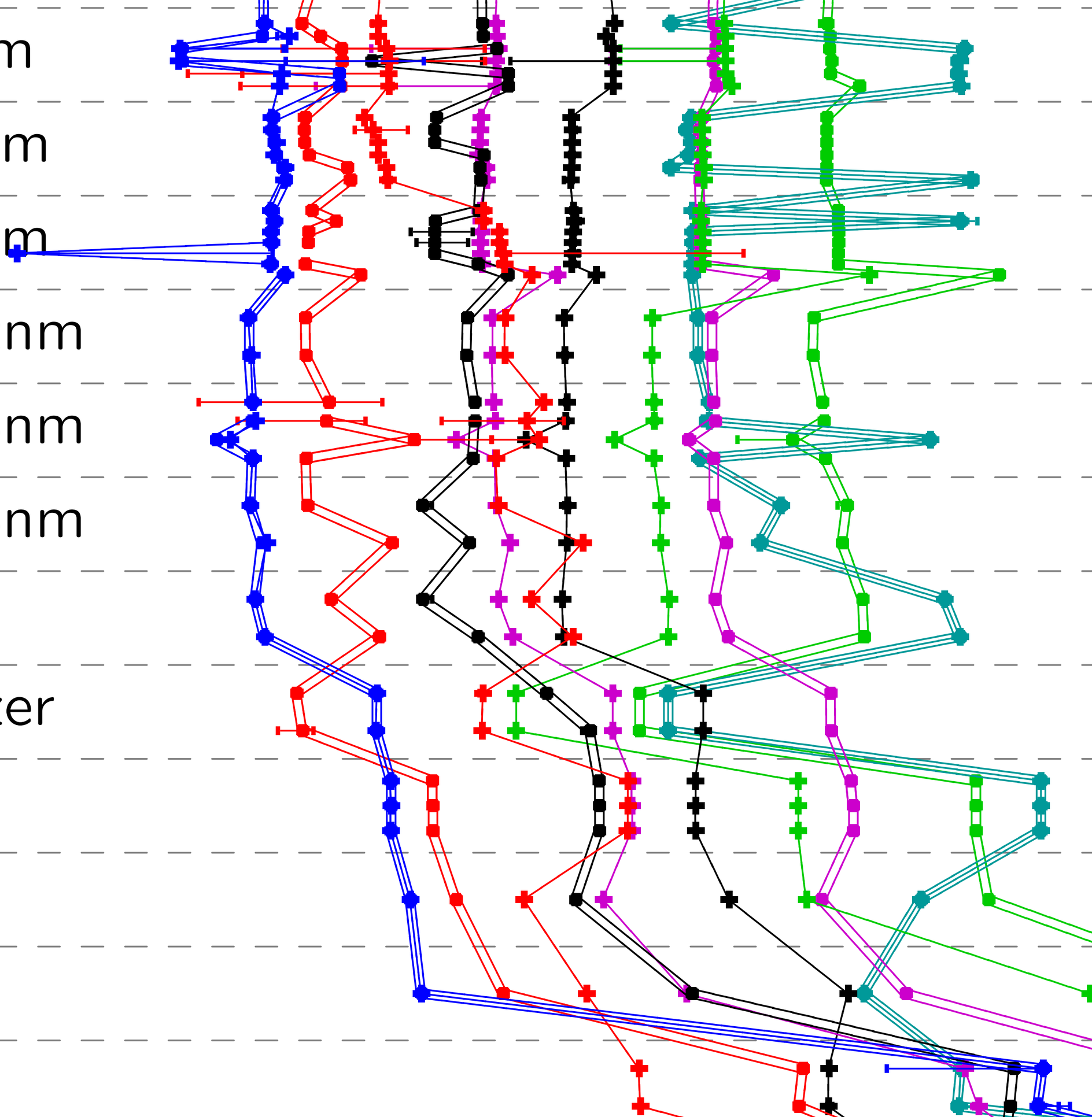
amd64 Bulldozer

amd64 Bobcat

amd64 Nano

amd64 Atom

x86 Atom



amd64 K8

amd64 Bulldozer

amd64 Bobcat

amd64 Nano

amd64 Atom

x86 Atom

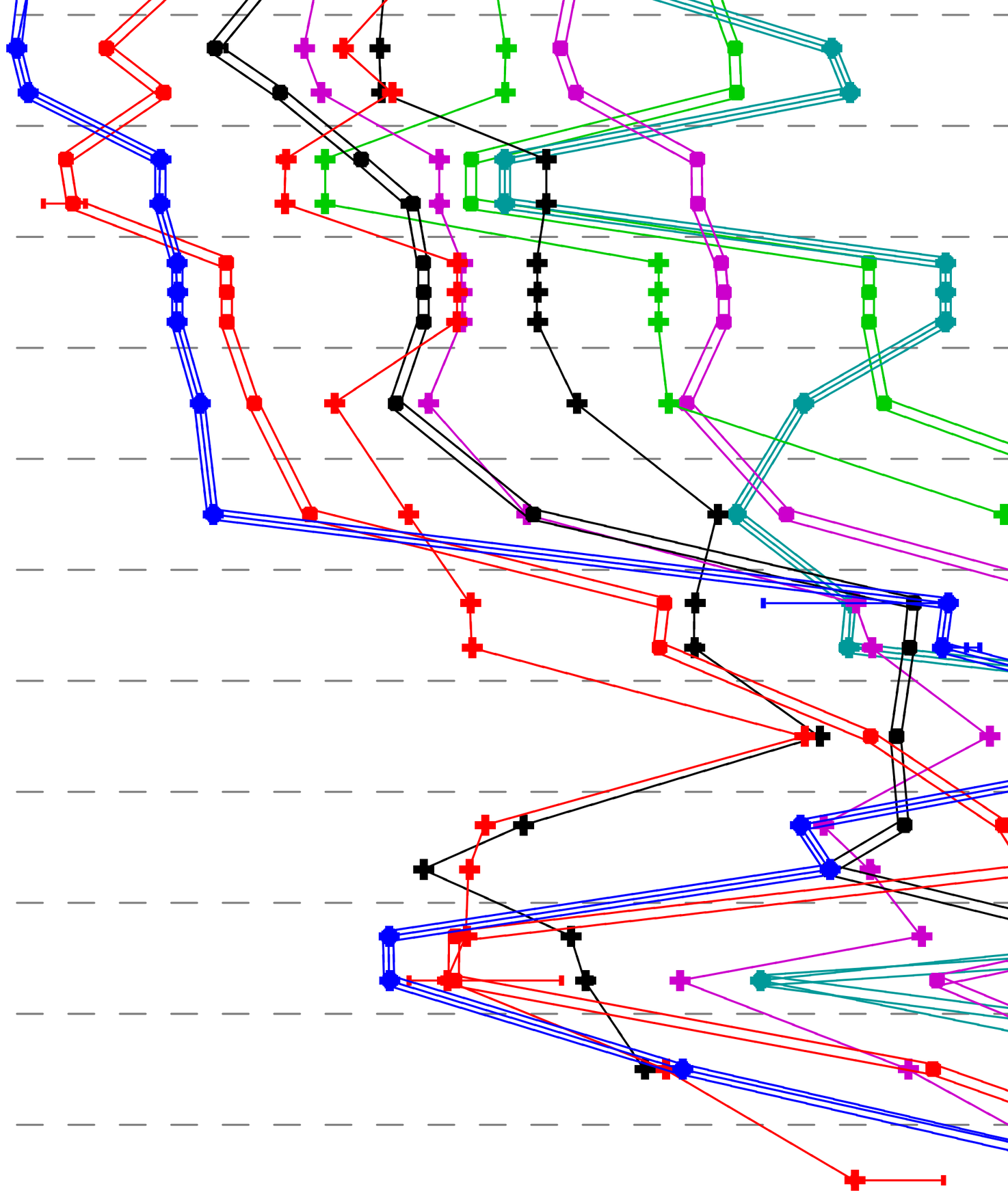
x86 Eden

ppc32 G4

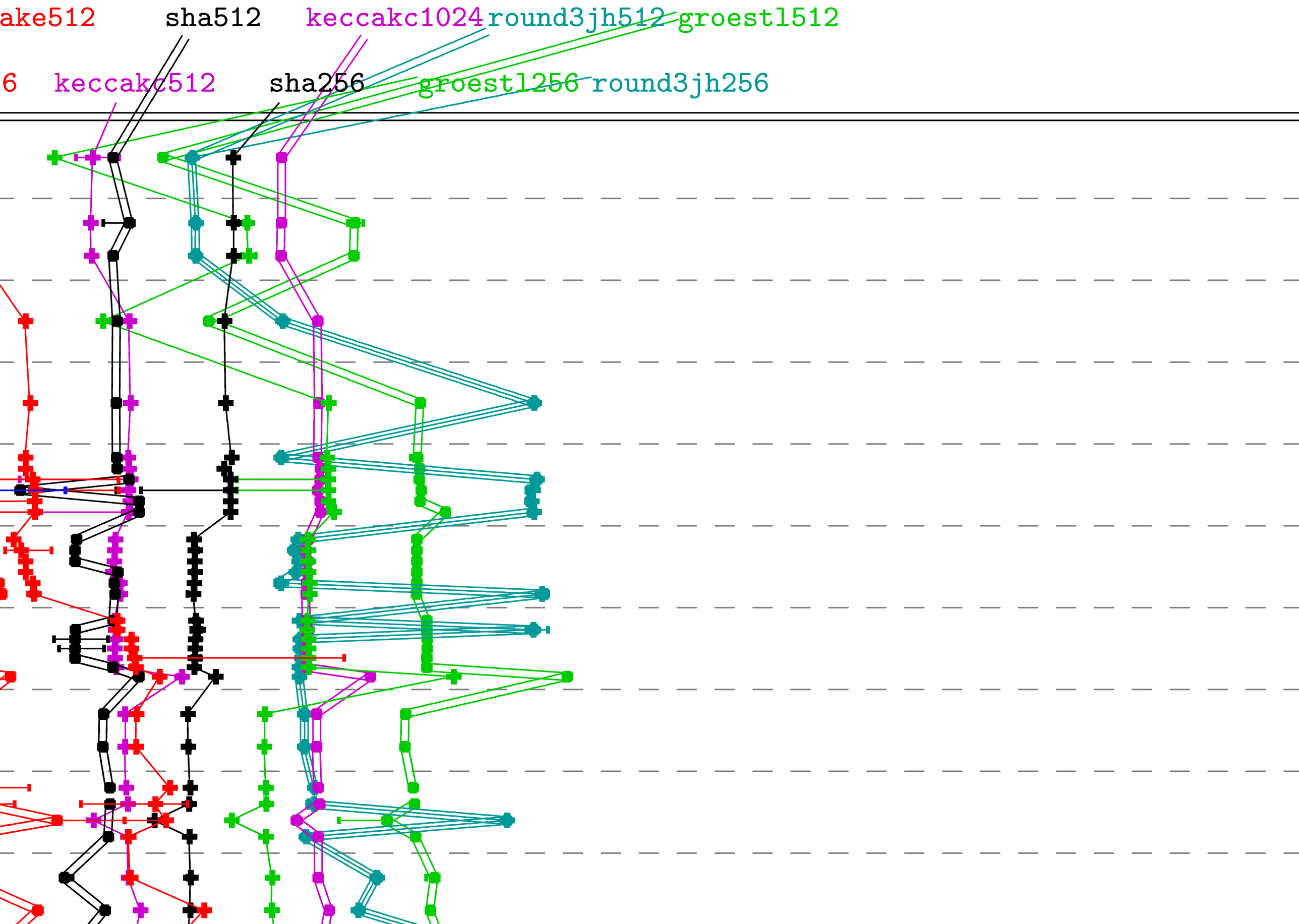
armeabi Cortex A8

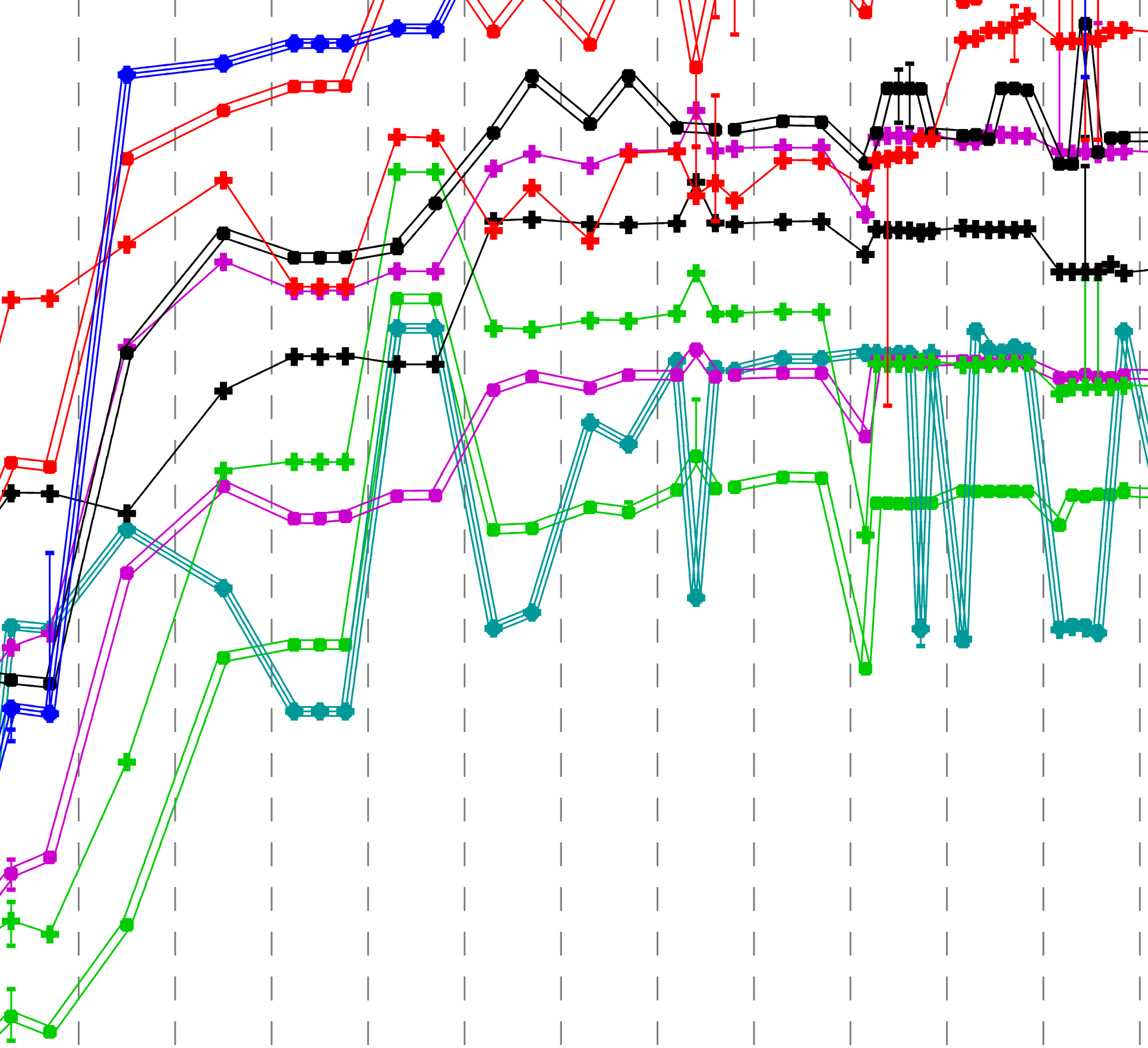
armeabi Tegra 2

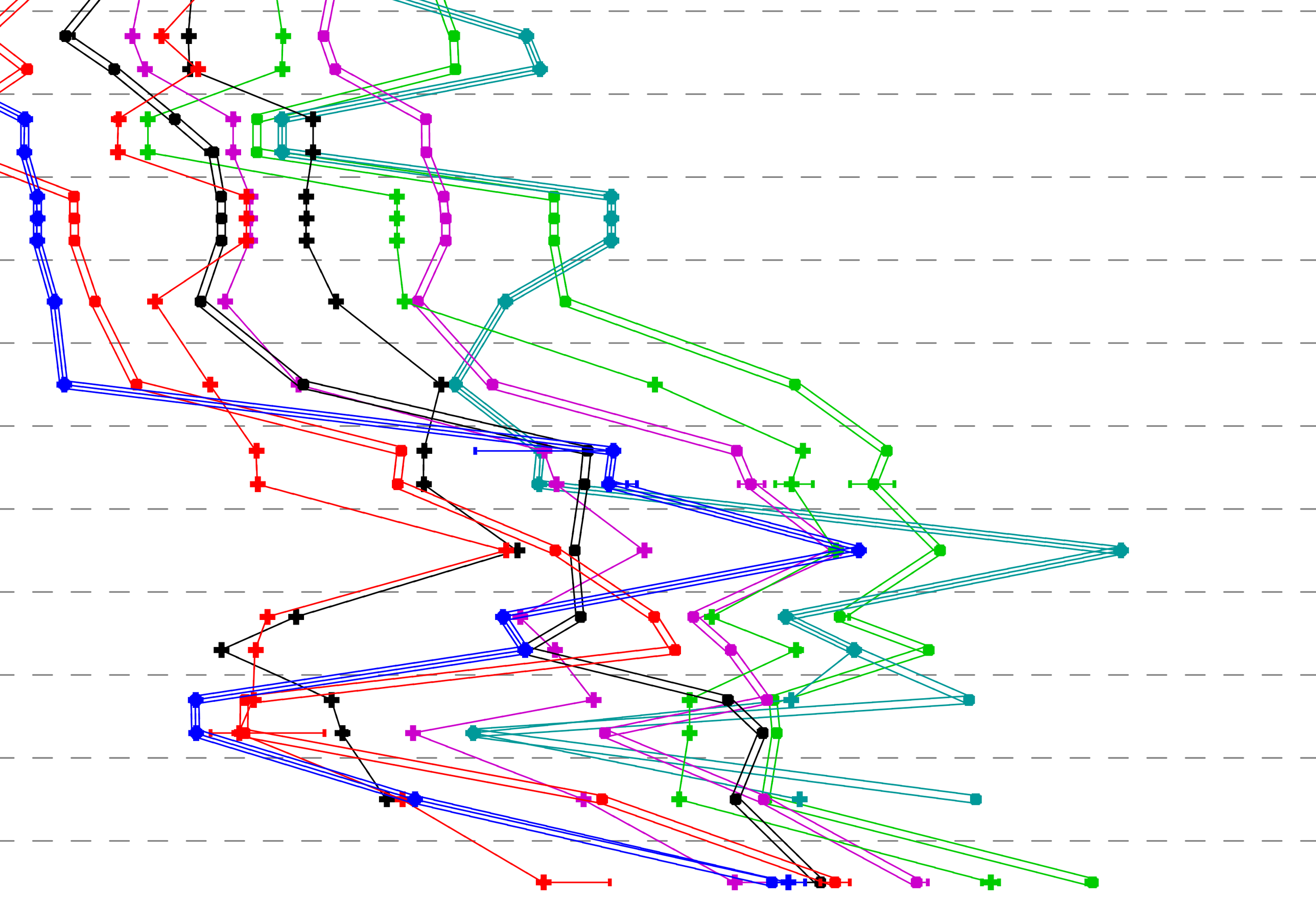
armeabi ARM11



Cycles per byte 4 8 16 32 64


ake512
sha512
keccakc1024
round3jh512
groestl512
6
keccakc512
sha256
groestl256
round3jh256




8
16
32
64
128
256
512

~~2~~groestl512

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
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

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
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

mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20120310

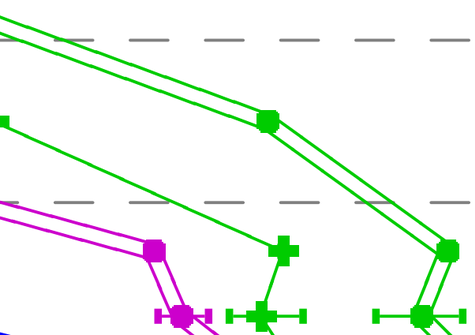
gcc11; 4 x 2000MHz; 2006 AMD Opteron 2212; amd64; K8 (40f13); supercop-20120310

hydra6; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20120310

bulldozer; 4 x 3600MHz; 2011 AMD FX-8150; amd64; Bulldozer (600f12); supercop-20120310

h5e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310
h4e350; 2 x 1600MHz; 2011 AMD E-350; amd64; Bobcat (500f20); supercop-20120310
h4e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310

h5nano; 1 x 1000MHz; 2009 Via Nano U3500; amd64; Nano (6f8); supercop-20120316



h2atom; 1 x 1000MHz; 2010 Intel Atom N455; amd64; Atom (106ca); supercop-20120310

slim; 1 x 1667MHz; 2009 Intel Atom N280; x86; Atom (106c2); supercop-20120310

h3atom; 1 x 1330MHz; 2008 Intel Atom Z520; x86; Atom (106c2); supercop-20120219

mace; 2 x 2000MHz; 2006 AMD Athlon 64 X2; amd64; K8 (40fb2); supercop-20120310

gcc11; 4 x 2000MHz; 2006 AMD Opteron 2212; amd64; K8 (40f13); supercop-20120310

hydra6; 4 x 3100MHz; 2011 AMD FX-8120; amd64; Bulldozer (600f12); supercop-20120310

bulldozer; 4 x 3600MHz; 2011 AMD FX-8150; amd64; Bulldozer (600f12); supercop-20120310

h5e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310

h4e350; 2 x 1600MHz; 2011 AMD E-350; amd64; Bobcat (500f20); supercop-20120310

h4e450; 2 x 1650MHz; 2011 AMD E-450; amd64; Bobcat (500f20); supercop-20120310

h5nano; 1 x 1000MHz; 2009 Via Nano U3500; amd64; Nano (6f8); supercop-20120316

h2atom; 1 x 1000MHz; 2010 Intel Atom N455; amd64; Atom (106ca); supercop-20120310

slim; 1 x 1667MHz; 2009 Intel Atom N280; x86; Atom (106c2); supercop-20120310

h3atom; 1 x 1330MHz; 2008 Intel Atom Z520; x86; Atom (106c2); supercop-20120219

h1eden; 1 x 1600MHz; 2006? Via Eden ULV; x86; Eden (6d0); supercop-20120120

gggg; 2 x 533MHz; 2001 Motorola PowerPC G4 7410; ppc32; G4 (G4); supercop-20120310

h1g4; 1 x 1416MHz; 2005 Motorola PowerPC G4 7447a; ppc32; G4 (G4); supercop-20120310

h1mx515; 1 x 800MHz; 2009 Freescale i.MX515; armeabi (v7-A, Cortex A8); supercop-20120310

h4mx515e; 1 x 800MHz; 2009 Freescale i.MX515; armeabi (v7-A, Cortex A8); supercop-20120316

h5tegra; 2 x 1000MHz; 2010 NVIDIA Tegra 2; armeabi (v7-A, Tegra 2); supercop-20120310

diablo; 1 x 400MHz; 2006? TI OMAP 2420; armeabi (v6, 1136J); supercop-20110914

128 256 512 1024 2048 4096