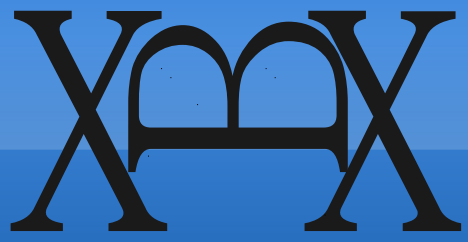
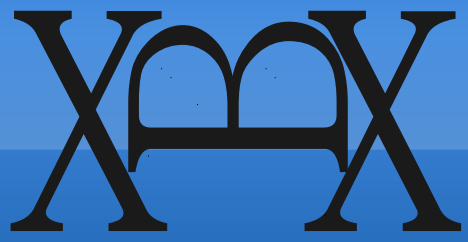


Benchmarking SHA-3 Candidates on Embedded Platforms

e**X**ternal **B**enchmarking e**X**tension for SUPERCOP-eBASH

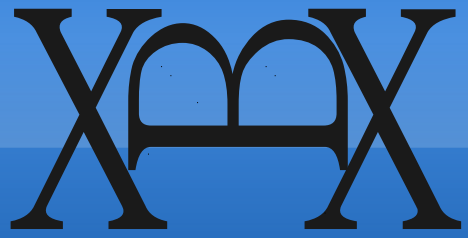
2nd SHA-3 Candidate Conference, August 23-24, UCSB

Christian Wenzel-Benner, ITK Engineering AG
Jens Gräf, LiNetCo GmbH



Overview

- XBX is almost 'SUPERCOP on microcontrollers'
- Some differences:
  - Maximum plaintext length = 2048 bytes
    - 'Long messages' := 2048 - 1024
  - Records ROM/RAM usage by default
- Please see CHES paper or website for details on XBX
- URL: https://xbx.das-labor.org/trac/wiki

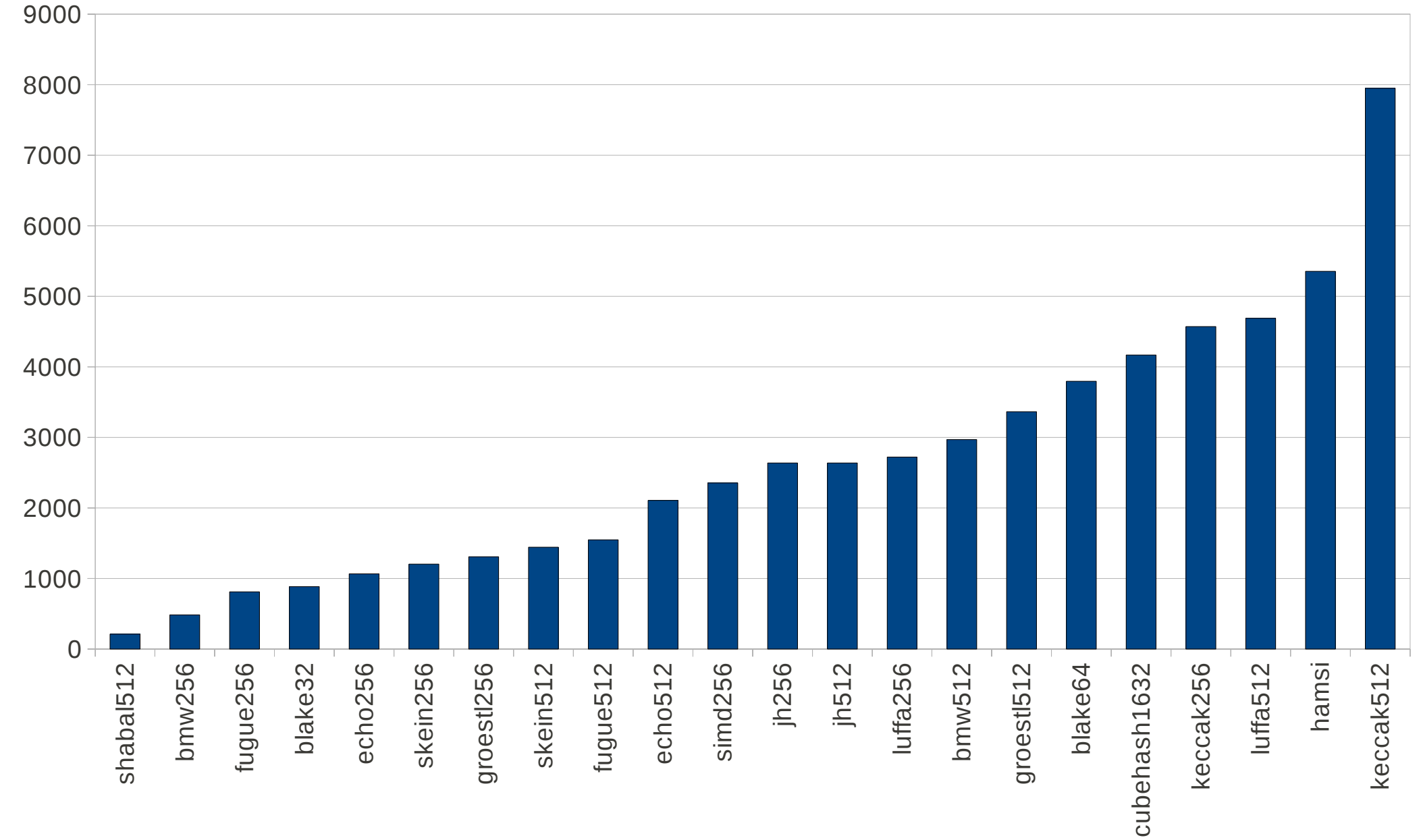


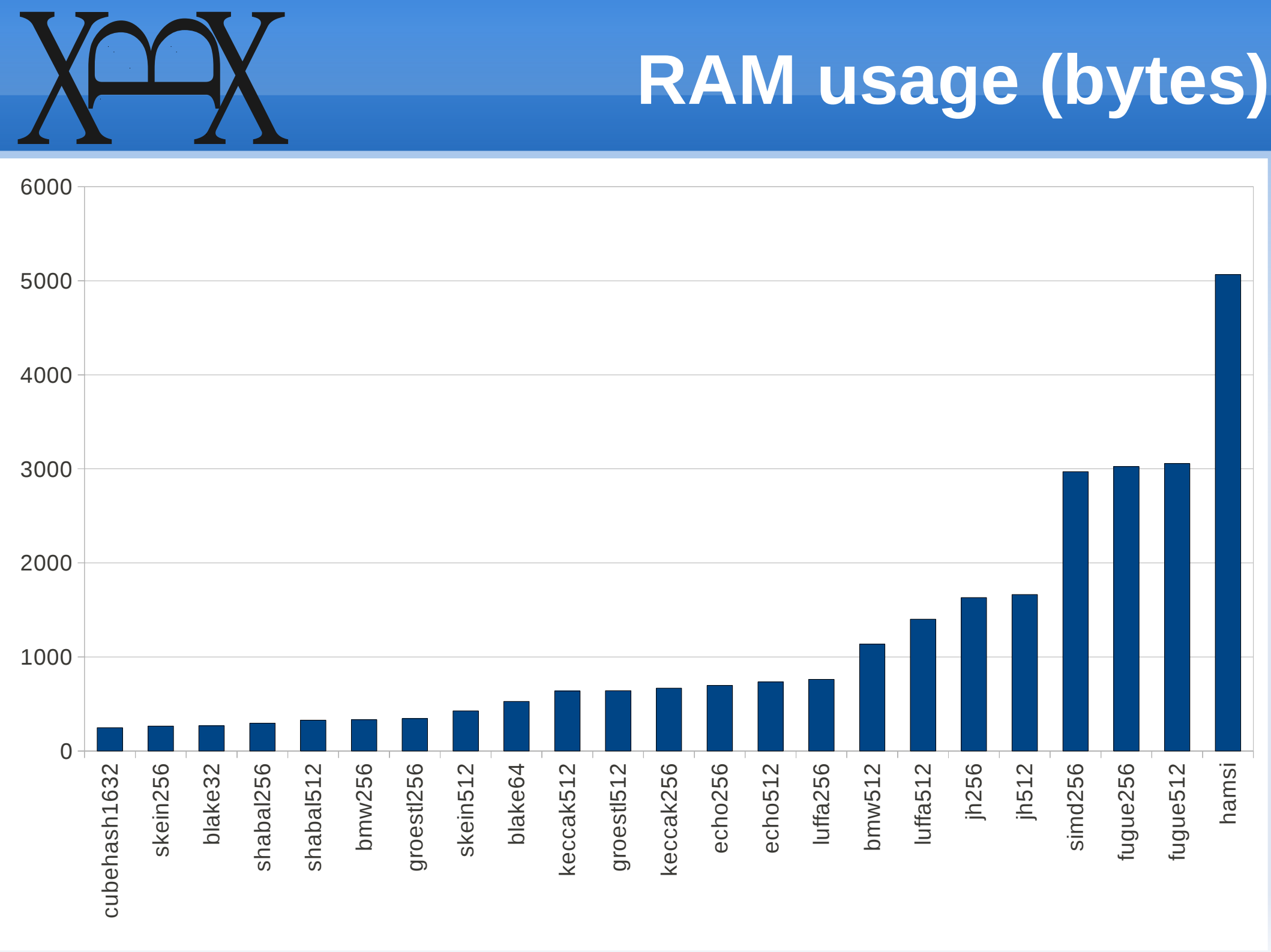
Atmel ATmega1281

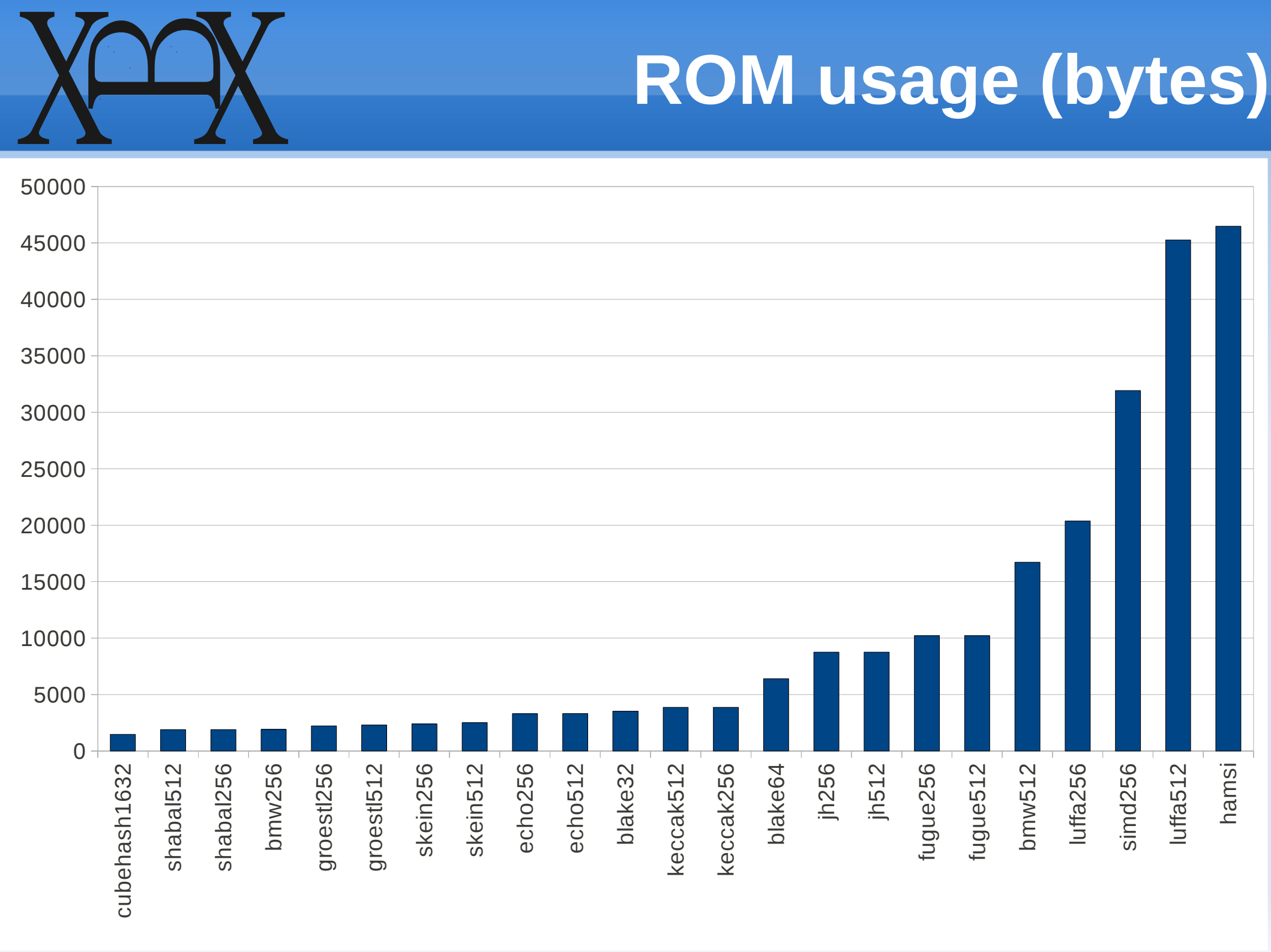
8bit microcontroller

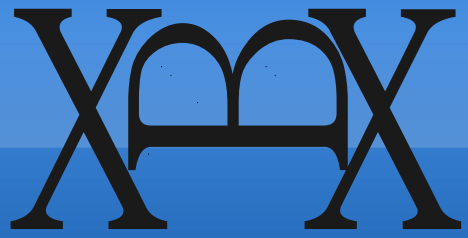
(atmega1281_16mhz)

Speed (cpb, long messages)




RAM usage (bytes)
6000
5000
4000
3000
2000
1000
0
cubehash1632
skein256
blake32
shabal256
shabal512
bmw256
groestl256
skein512
blake64
keccak512
groestl512
keccak256
echo256
echo512
luffa256
bmw512
luffa512
jh256
jh512
simd256
fugue256
fugue512
hamsi


ROM usage (bytes)
50000
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
cubehash1632
shabal512
shabal256
bmw256
groestl256
groestl512
skein256
skein512
echo256
echo512
blake32
keccak512
keccak256
blake64
jh256
jh512
fugue256
fugue512
bmw512
luffa256
simd256
luffa512
hamsi

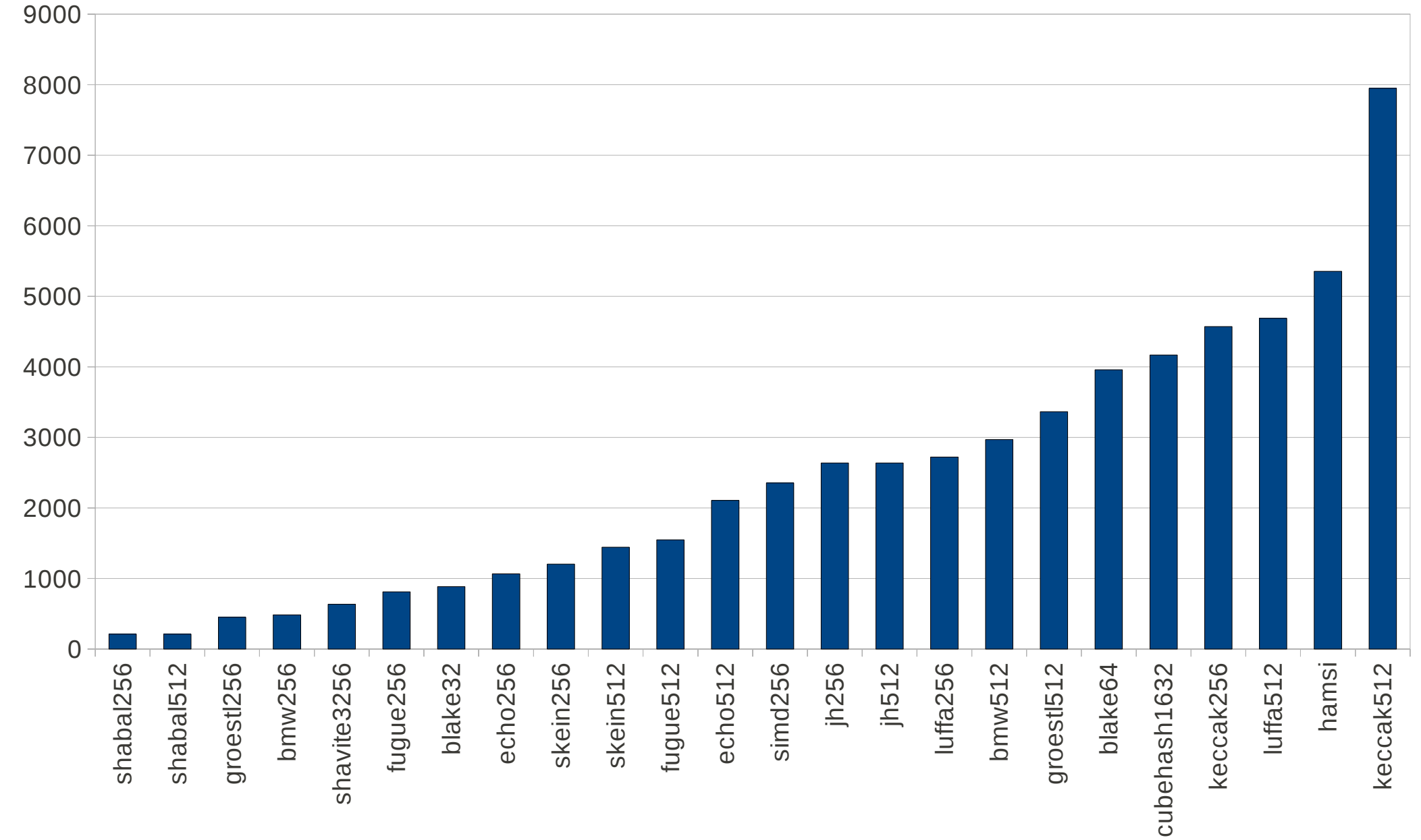


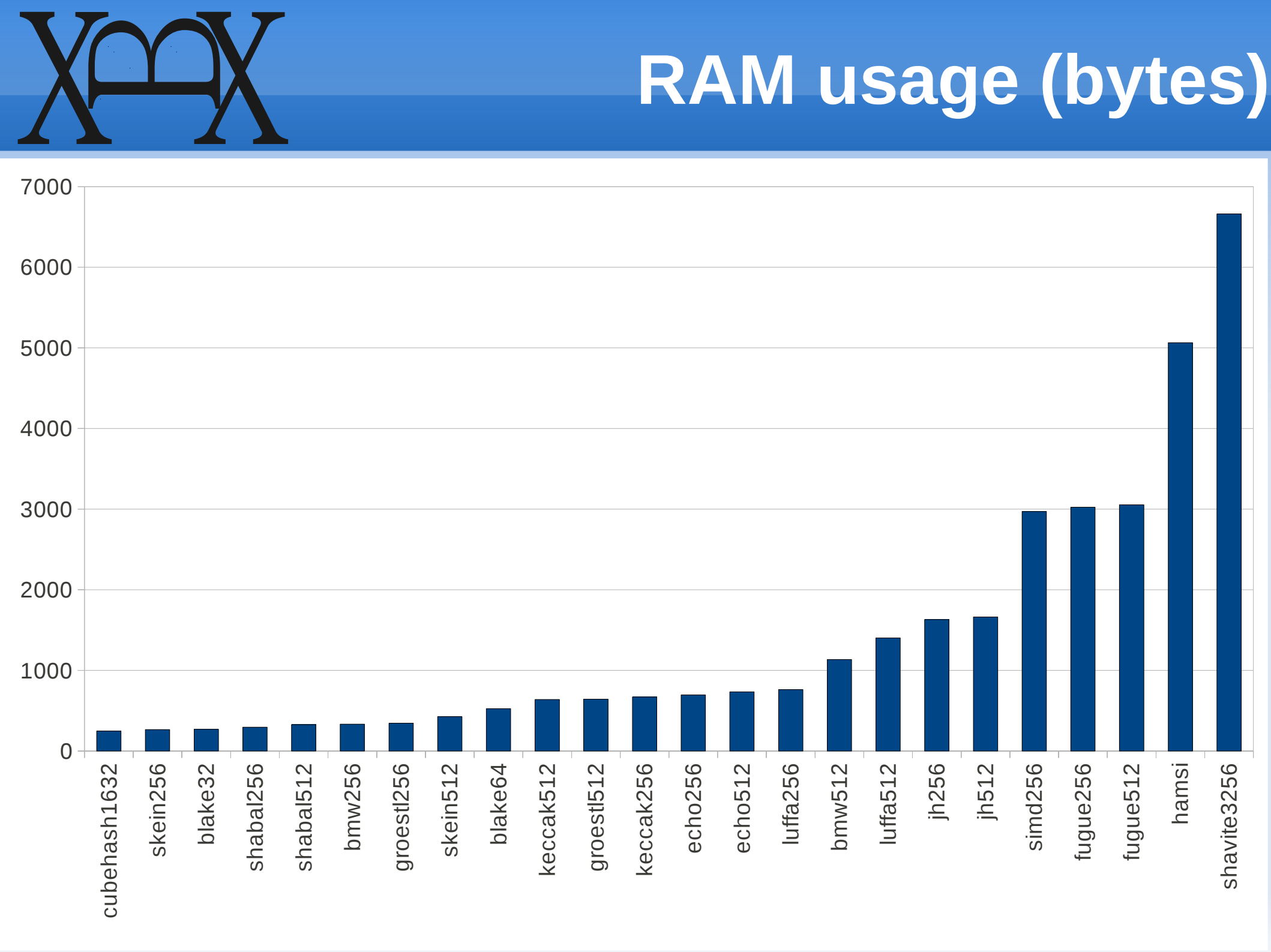
Atmel ATmega1284P

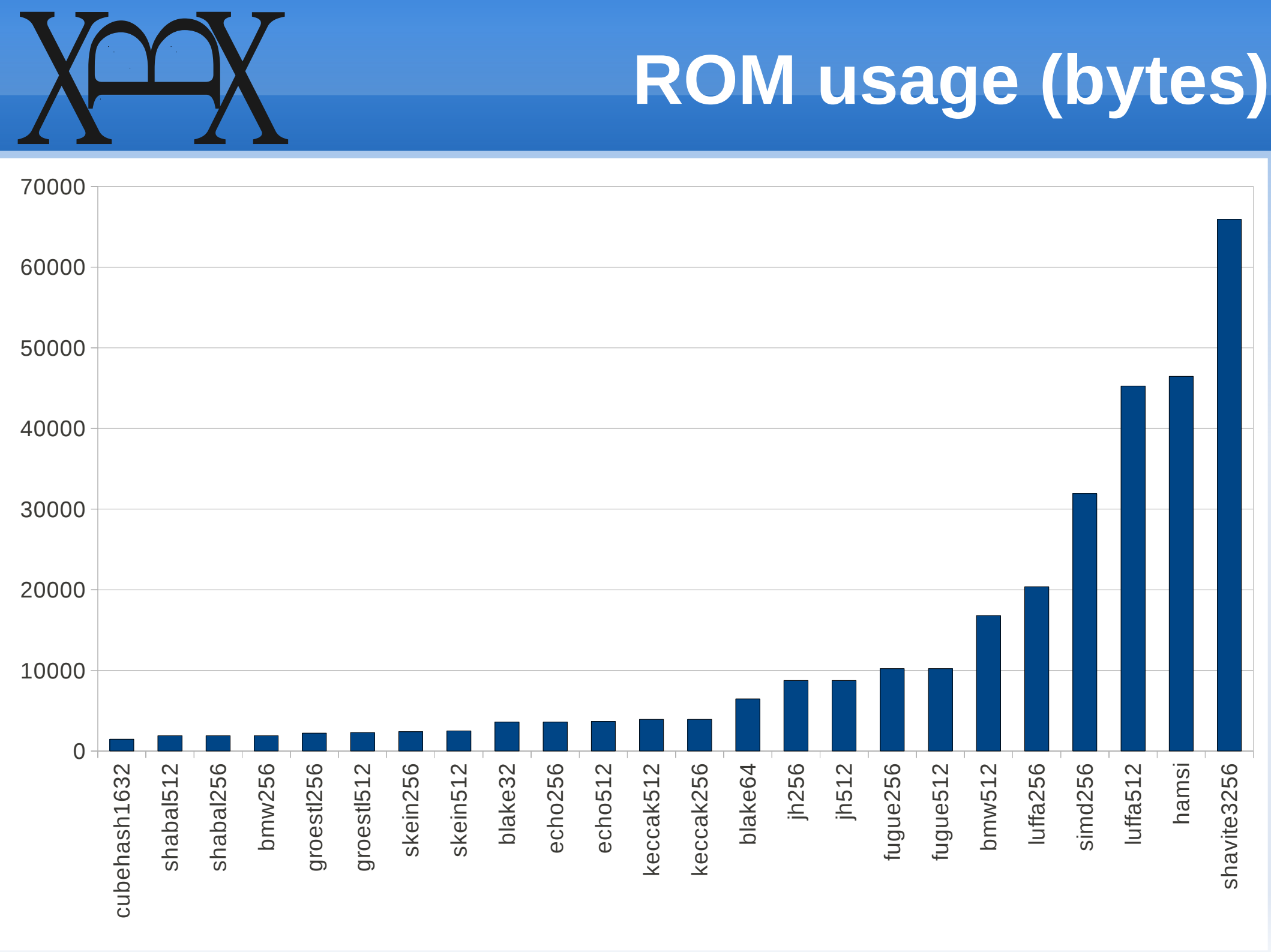
8bit microcontroller

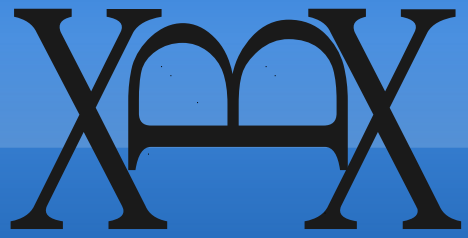
(atmega1284p_16mhz)

Speed (cpb, long messages)




RAM usage (bytes)
7000
6000
5000
4000
3000
2000
1000
0
cubehash1632
skein256
blake32
shabal256
shabal512
bmw256
groestl256
skein512
blake64
keccak512
groestl512
keccak256
echo256
echo512
luffa256
bmw512
luffa512
jh256
jh512
simd256
fugue256
fugue512
hamsi
shavite3256

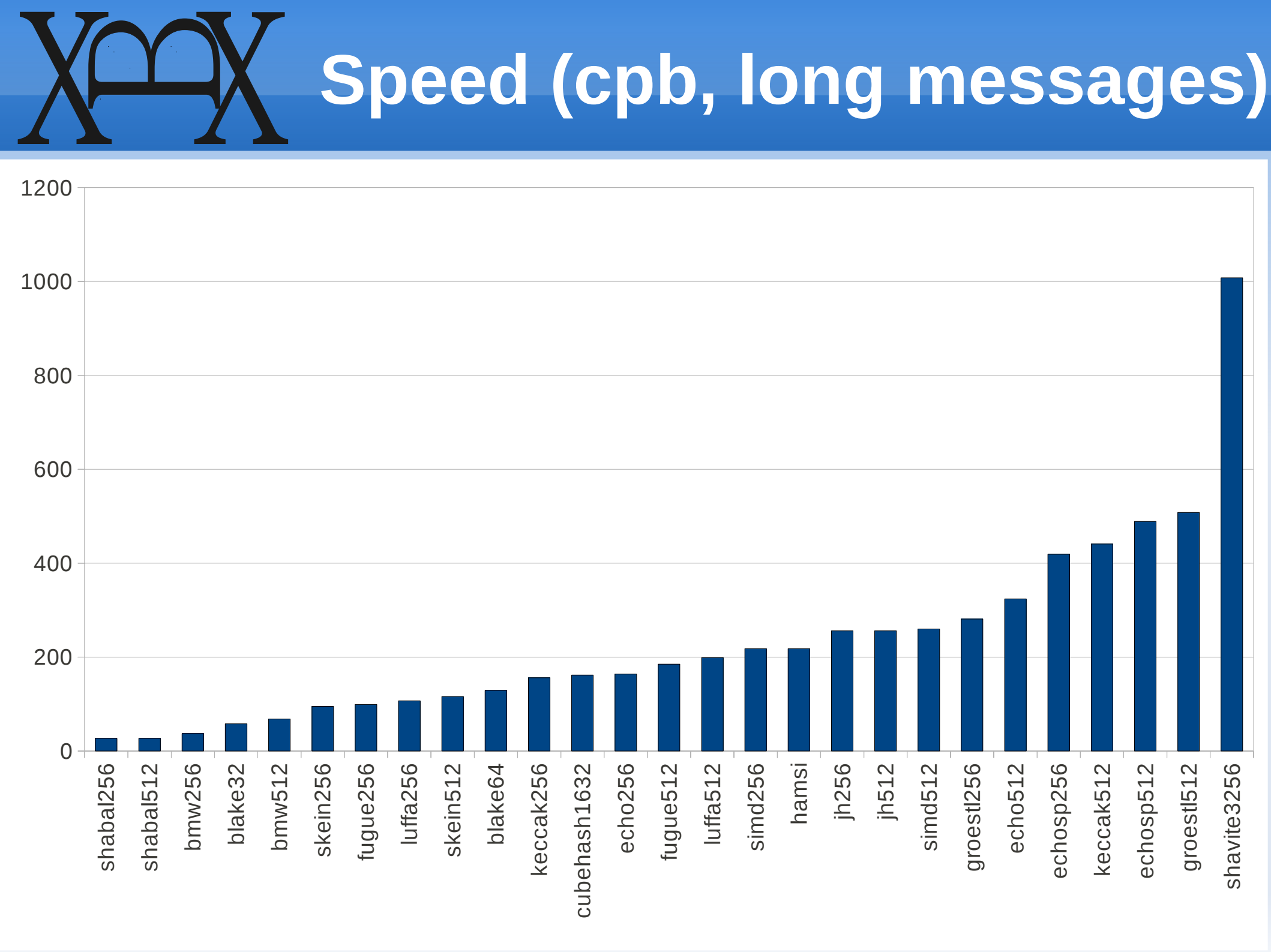

ROM usage (bytes)
70000
60000
50000
40000
30000
20000
10000
0
cubehash1632
shabal512
shabal256
bmw256
groestl256
groestl512
skein256
skein512
blake32
echo256
echo512
keccak512
keccak256
blake64
jh256
jh512
fugue256
fugue512
bmw512
luffa256
simd256
luffa512
hamsi
shavite3256



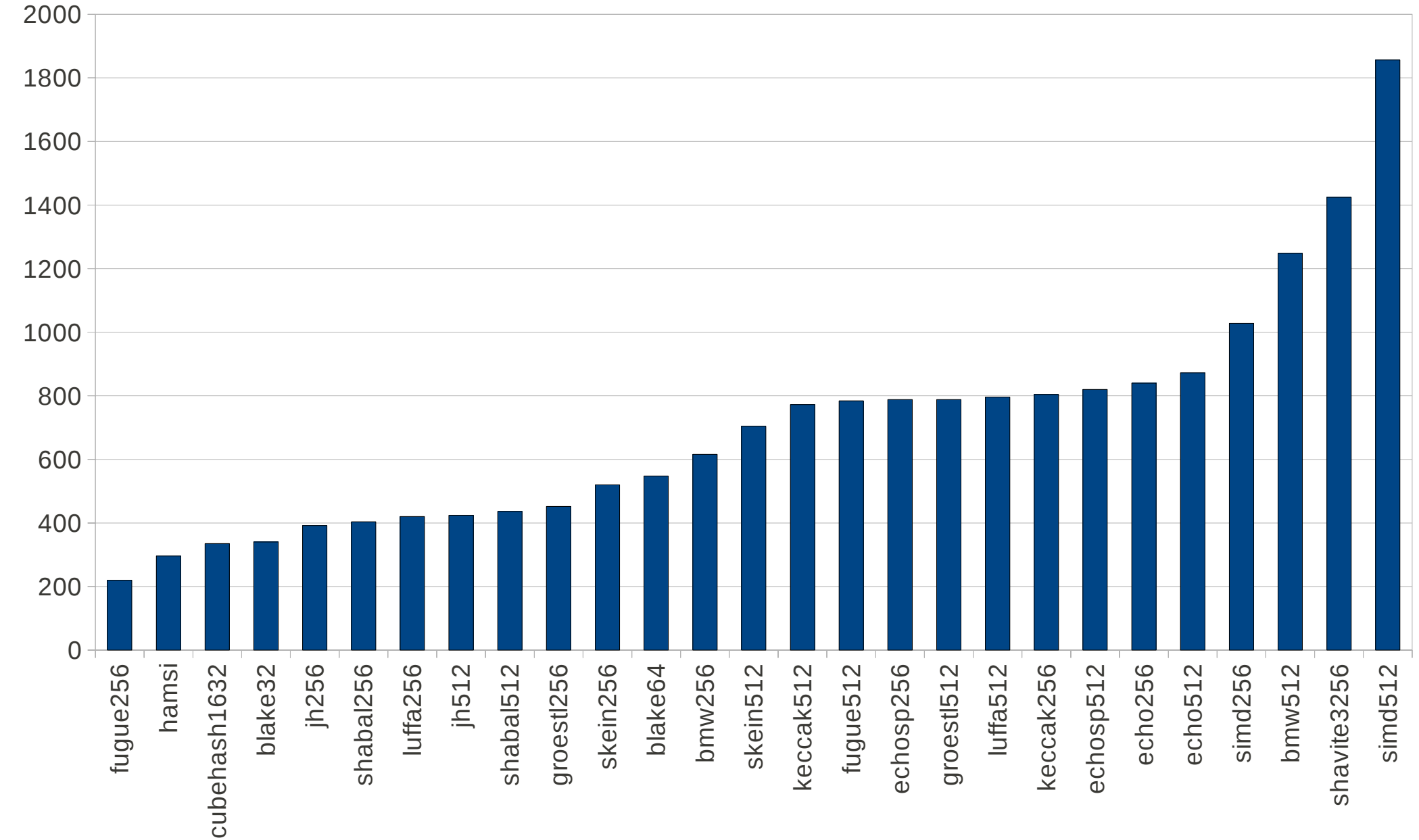
Texas Instruments AR7

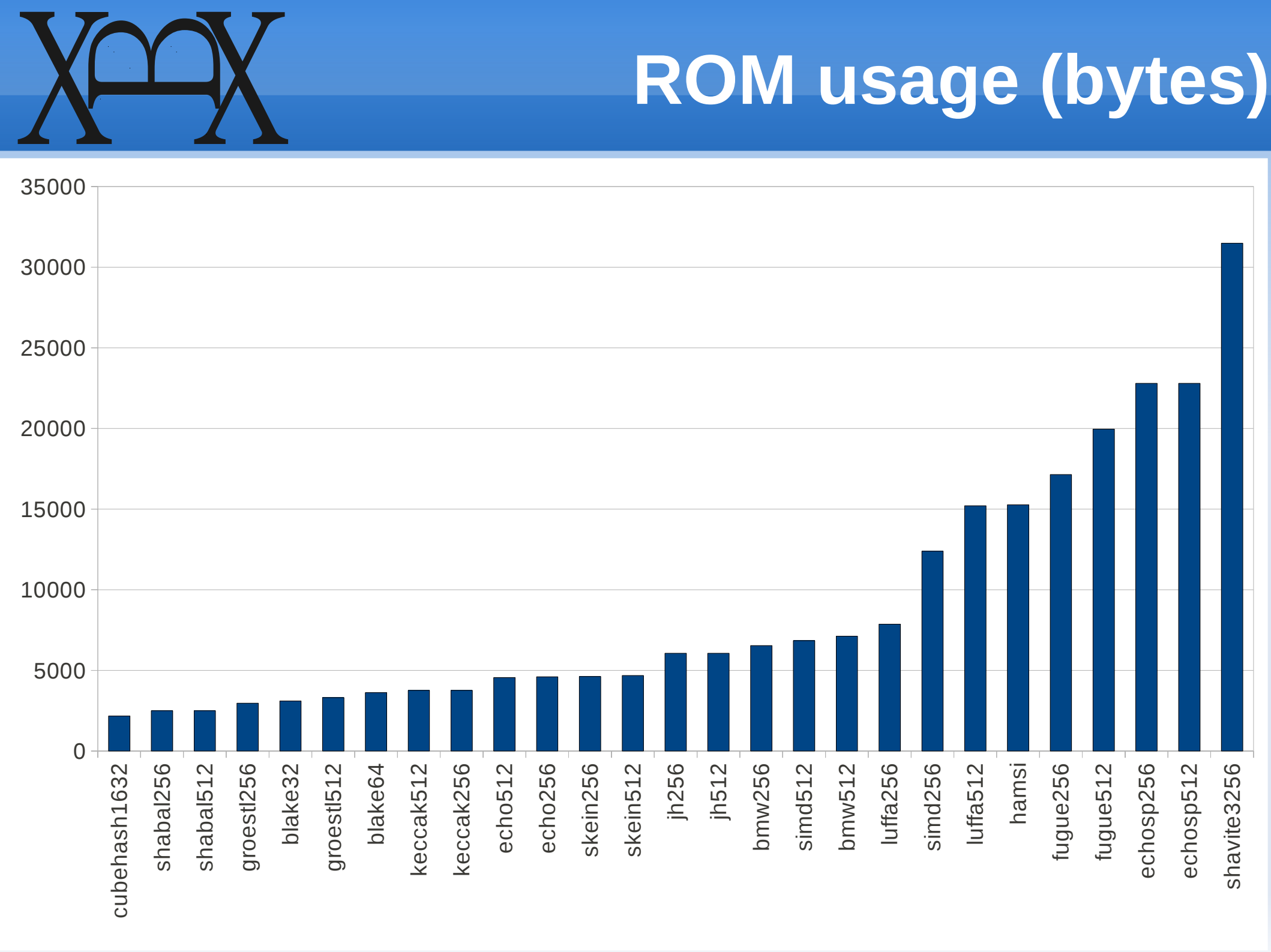
MIPS based 32bit SoC

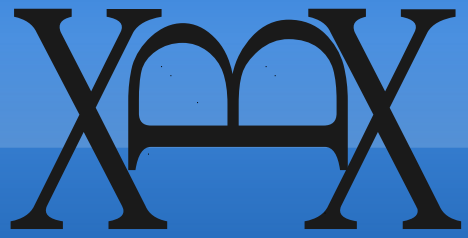
(fritzbox-7170)


Speed (cpb, long messages)
1200
1000
800
600
400
200
0
shabal256
shabal512
bmw256
blake32
bmw512
skein256
fugue256
luffa256
skein512
blake64
keccak256
cubehash1632
echo256
fugue512
luffa512
simd256
hamsi
jh256
jh512
simd512
groestl256
echo512
echosp256
keccak512
echosp512
groestl512
shavite3256

RAM usage (bytes)




ROM usage (bytes)
35000
30000
25000
20000
15000
10000
5000
0
cubehash1632
shabal256
shabal512
groestl256
blake32
groestl512
blake64
keccak512
keccak256
echo512
echo256
skein256
skein512
jh256
jh512
bmw256
simd512
bmw512
luffa256
simd256
luffa512
hamsi
fugue256
fugue512
echosp256
echosp512
shavite3256

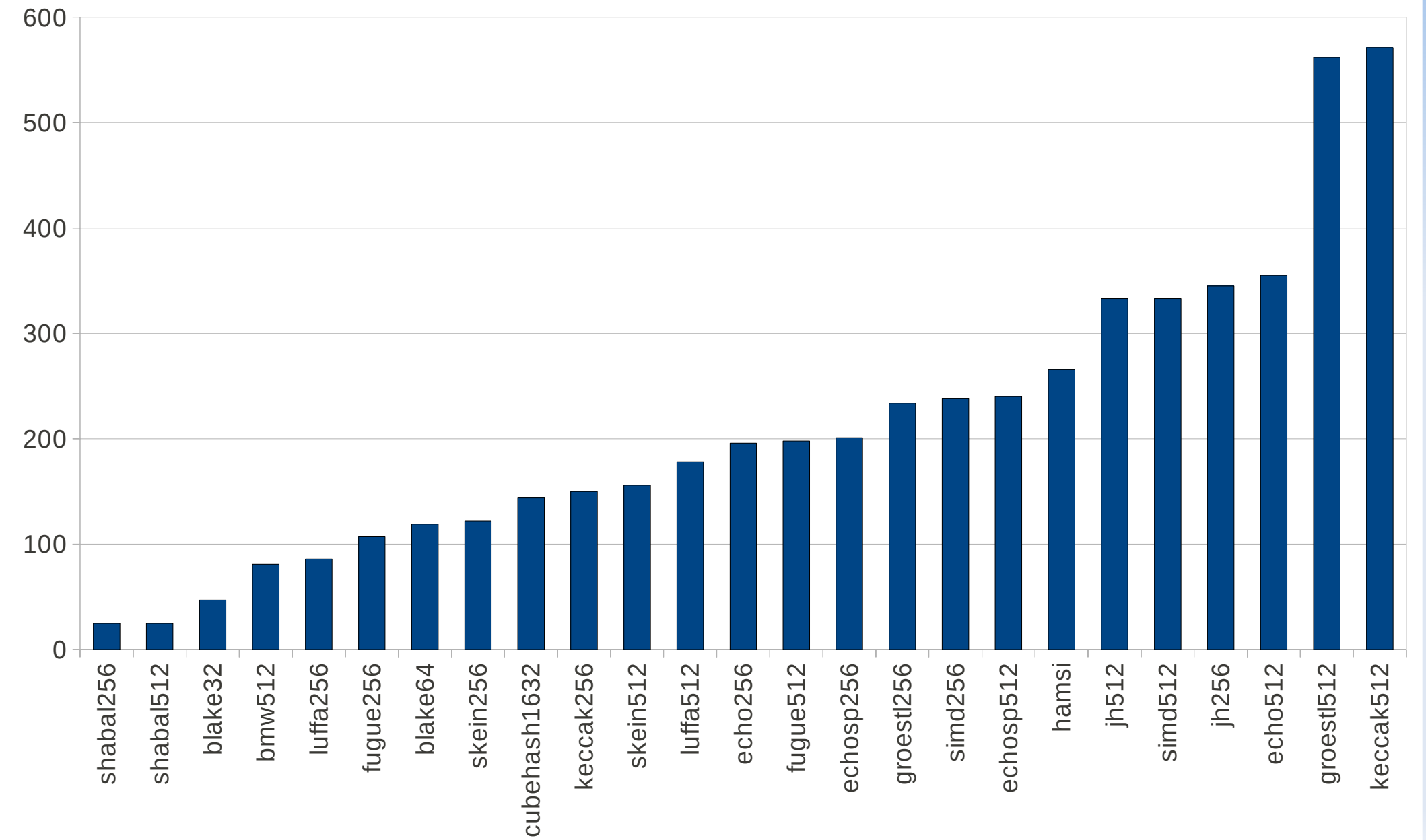


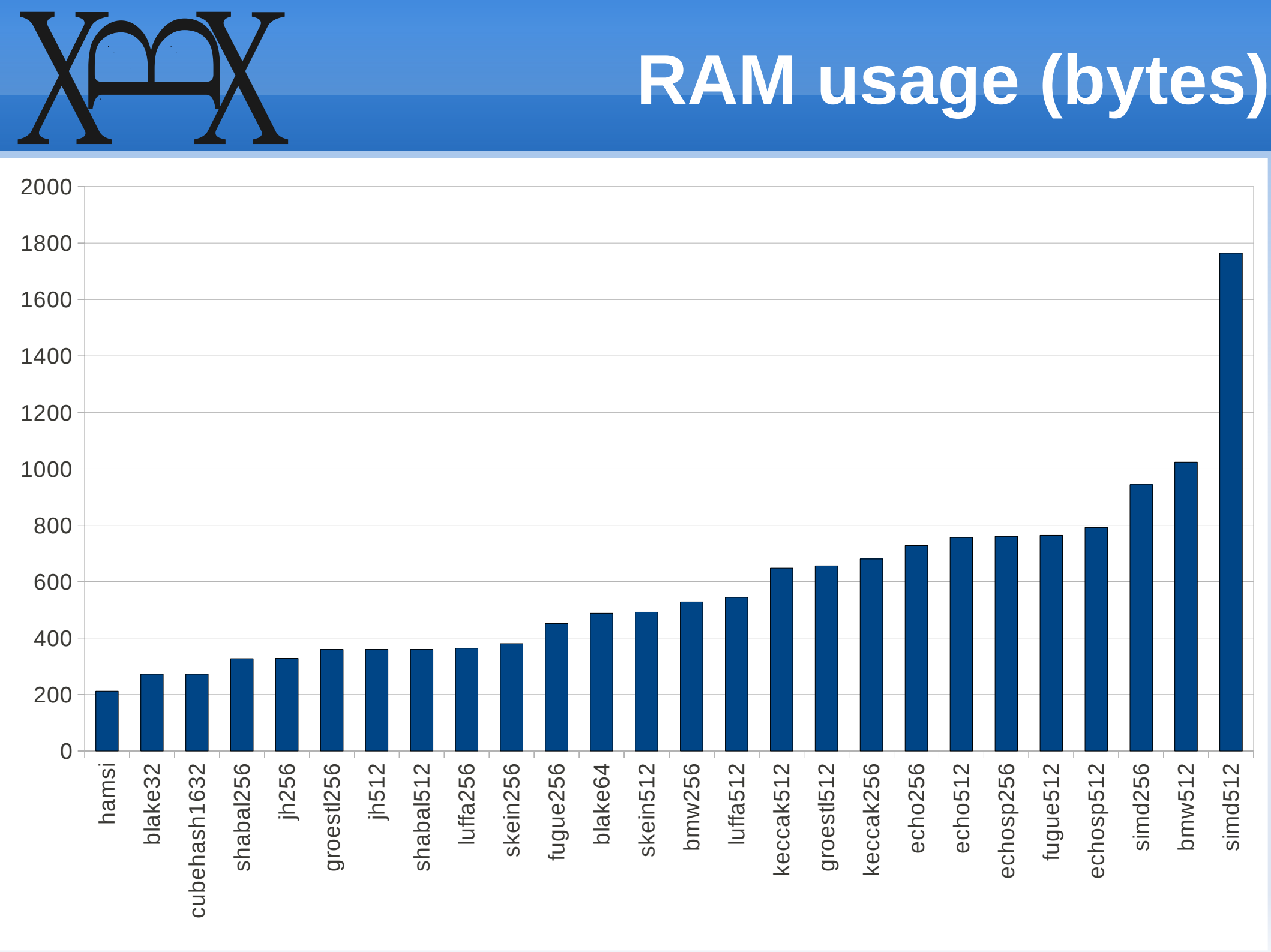
Atmel AT91RM9200

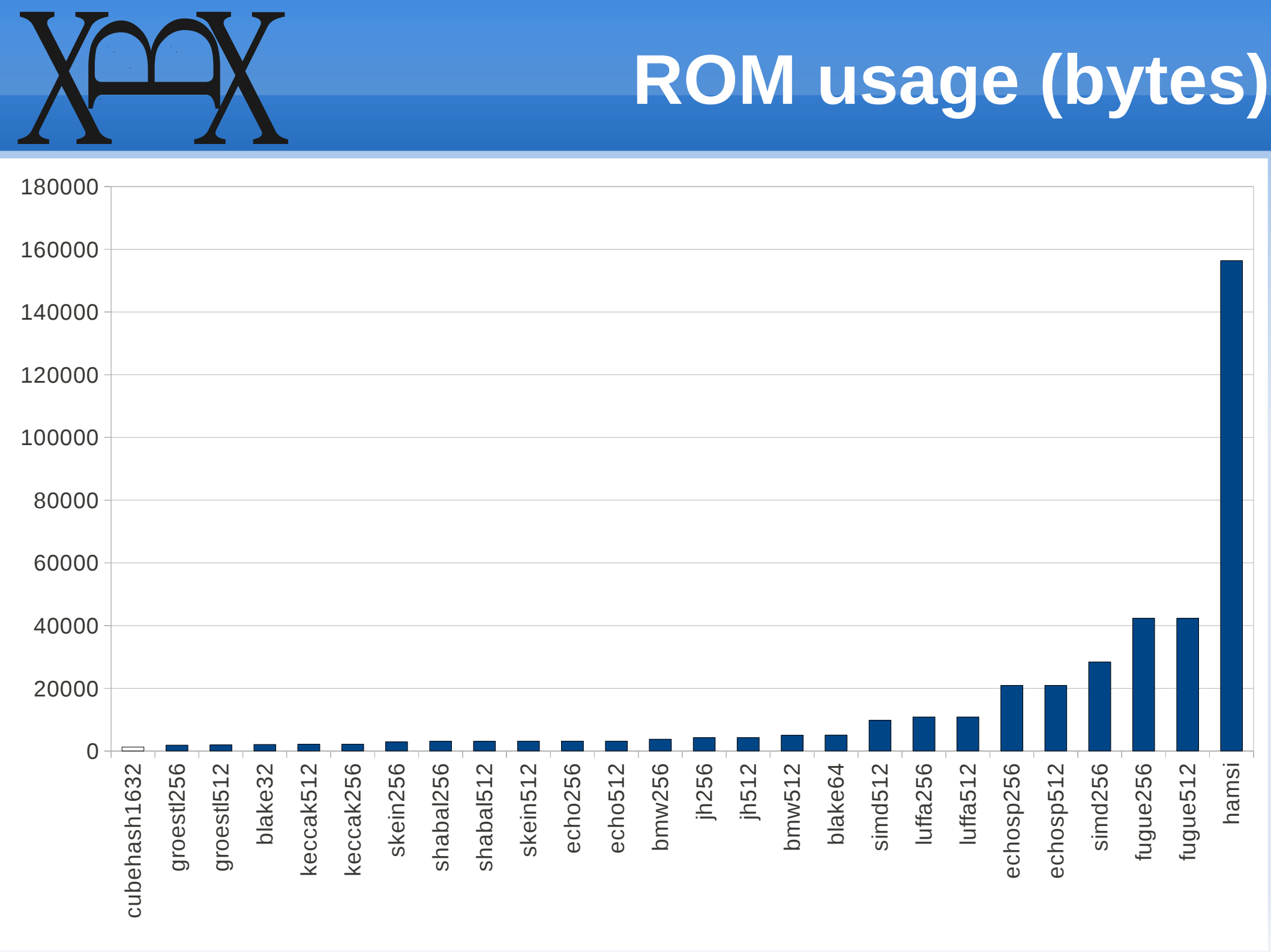
ARM 920T based 32bit SoC

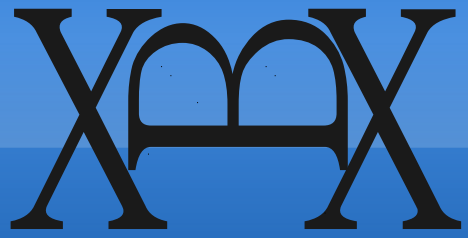
(artila_m501)

Speed (cpb, long messages)




RAM usage (bytes)
2000
1800
1600
1400
1200
1000
800
600
400
200
0
hamsi
blake32
cubehash1632
shabal256
jh256
groestl256
jh512
shabal512
luffa256
skein256
fugue256
blake64
skein512
bmw256
luffa512
keccak512
groestl512
keccak256
echo256
echo512
echosp256
fugue512
echosp512
simd256
bmw512
simd512

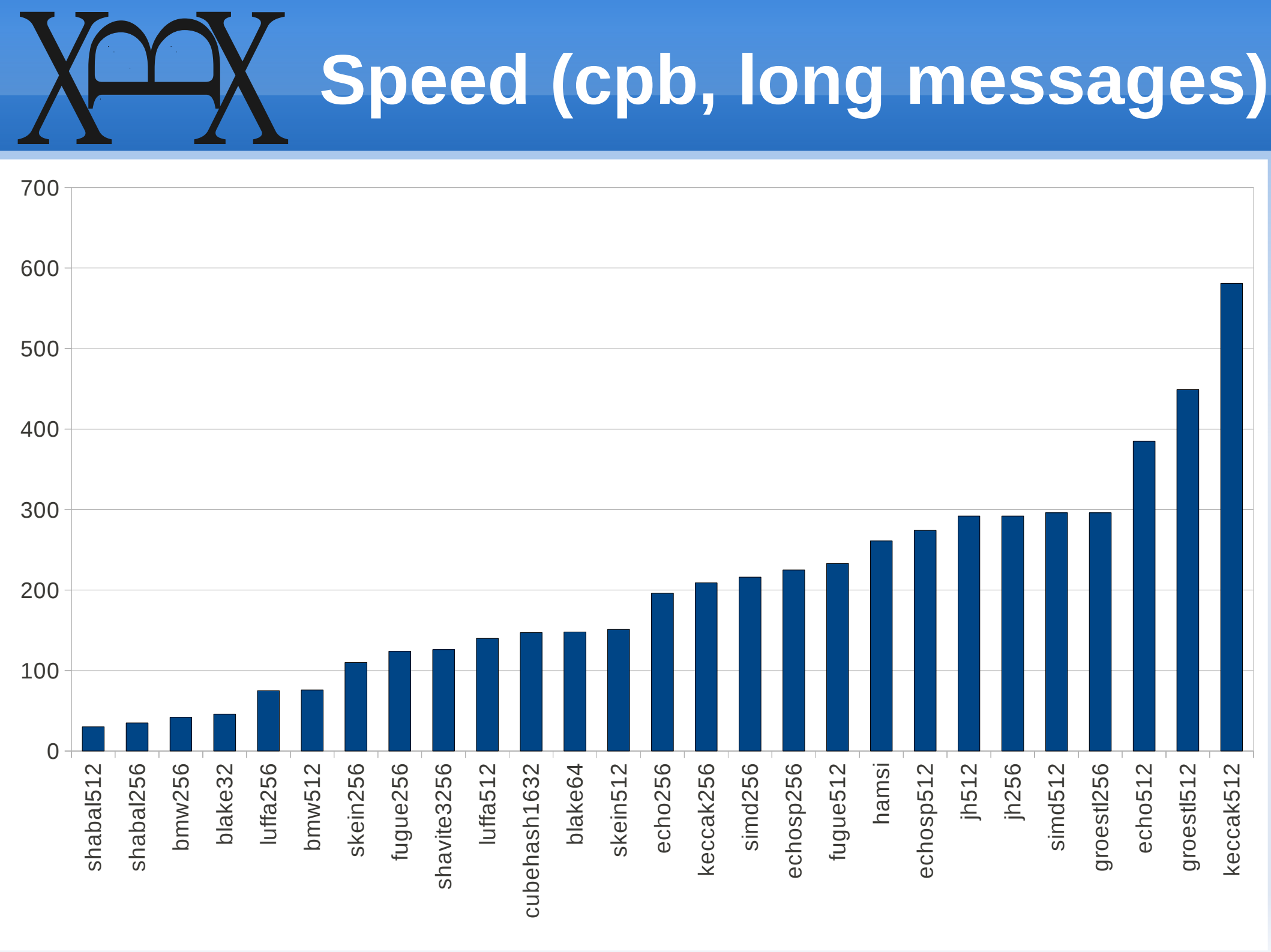

ROM usage (bytes)
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
cubehash1632
groestl256
groestl512
blake32
keccak512
keccak256
skein256
shabal256
shabal512
skein512
echo256
echo512
bmw256
jh256
jh512
bmw512
blake64
simd512
luffa256
luffa512
echosp256
echosp512
simd256
fugue256
fugue512
hamsi

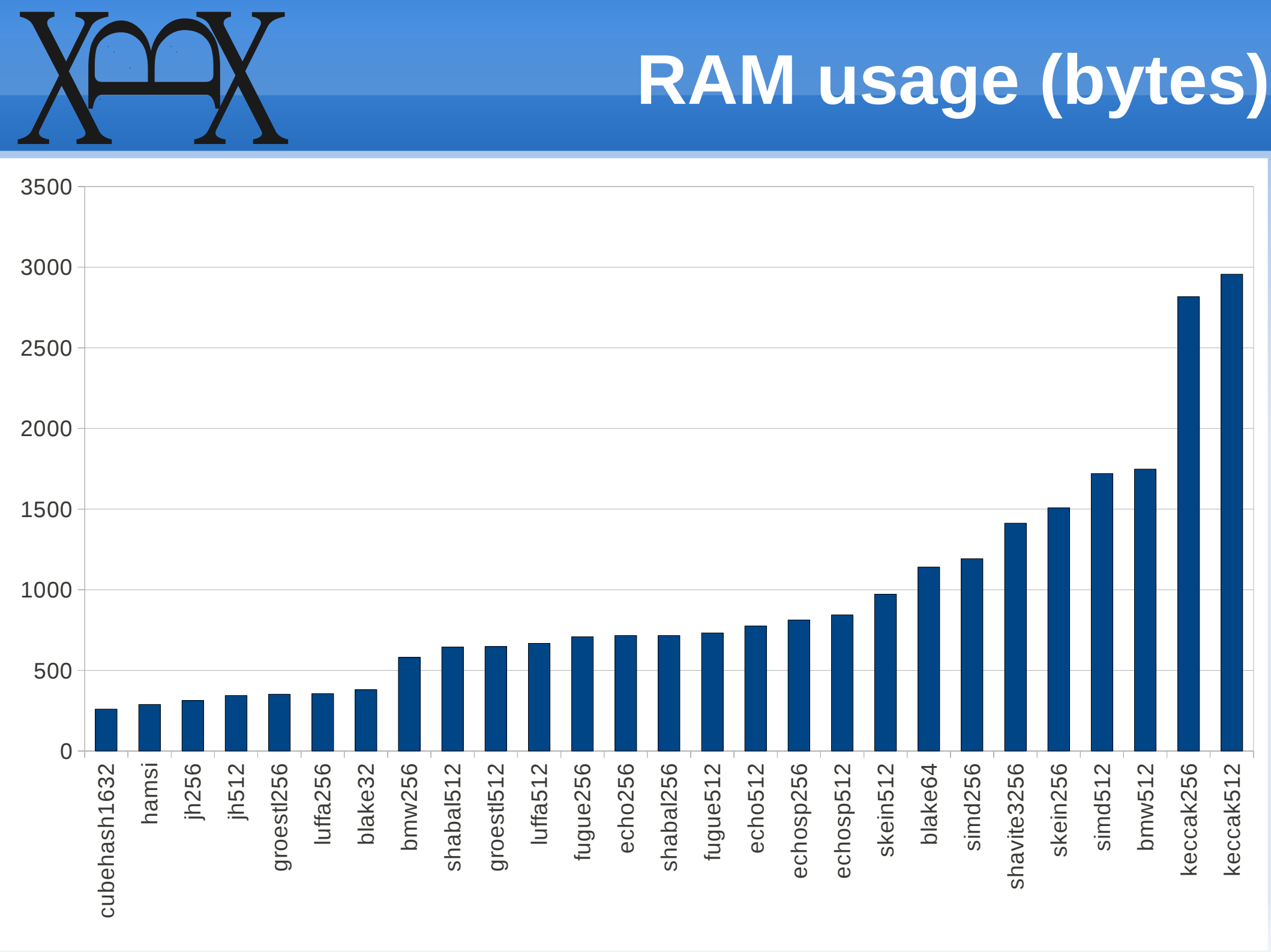


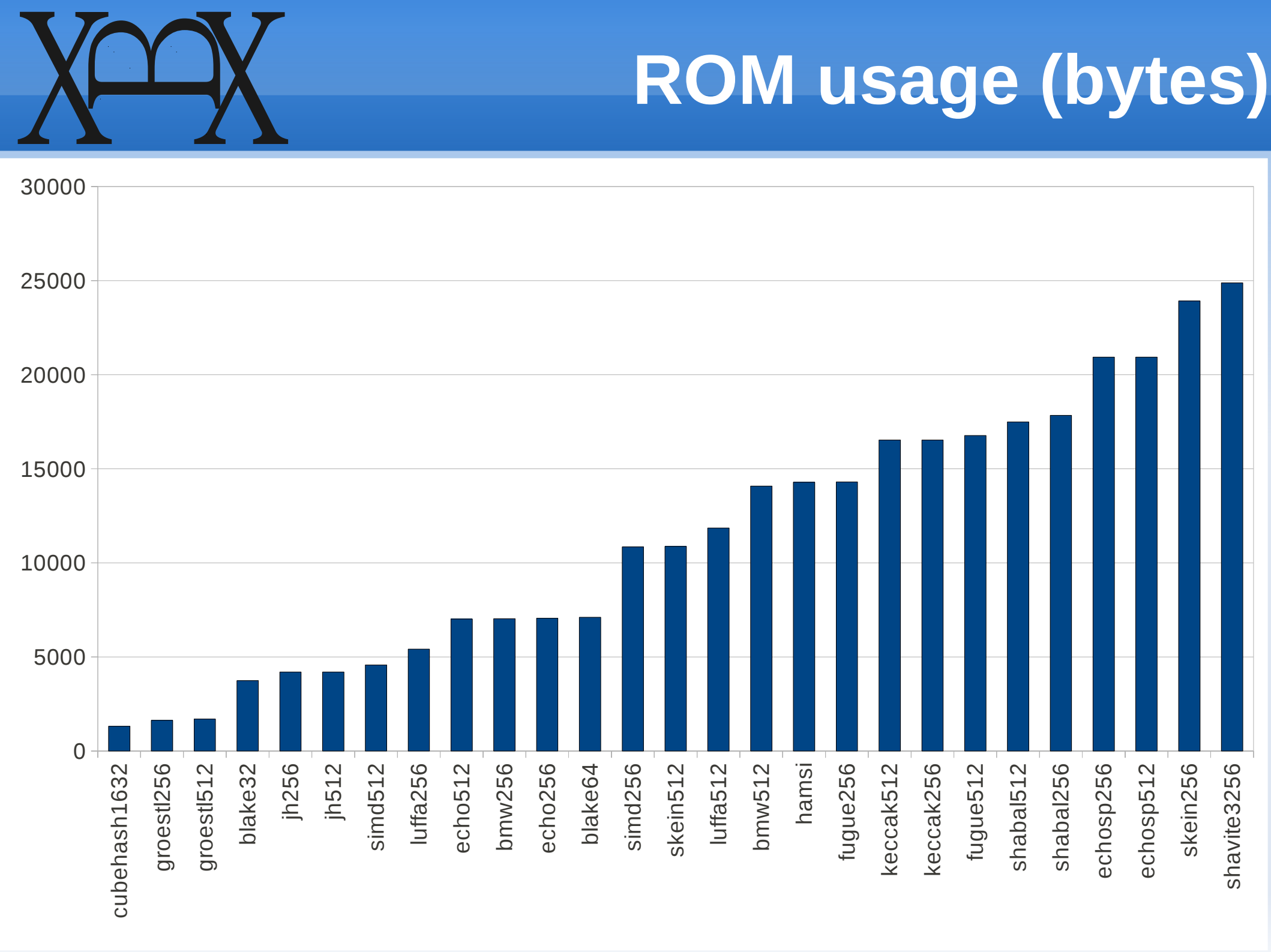
Intel XScale IXP420

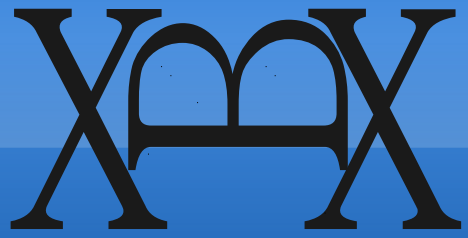
ARMv5TE architecture

(nslu2-openwrt)


Speed (cpb, long messages)
700
600
500
400
300
200
100
0
shabal512
shabal256
bmw256
blake32
luffa256
bmw512
skein256
fugue256
shavite3256
luffa512
cubehash1632
blake64
skein512
echo256
keccak256
simd256
echosp256
fugue512
hamsi
echosp512
jh512
jh256
simd512
groestl256
echo512
groestl512
keccak512


RAM usage (bytes)
3500
3000
2500
2000
1500
1000
500
0
cubehash1632
hamsi
jh256
jh512
groestl256
luffa256
blake32
bmw256
shabal512
groestl512
luffa512
fugue256
echo256
shabal256
fugue512
echo512
echosp256
echosp512
skein512
blake64
simd256
shavite3256
skein256
simd512
bmw512
keccak256
keccak512


ROM usage (bytes)
30000
25000
20000
15000
10000
5000
0
cubehash1632
groestl256
groestl512
blake32
jh256
jh512
simd512
luffa256
echo512
bmw256
echo256
blake64
simd256
skein512
luffa512
bmw512
hamsi
fugue256
keccak512
keccak256
fugue512
shabal512
shabal256
echosp256
echosp512
skein256
shavite3256

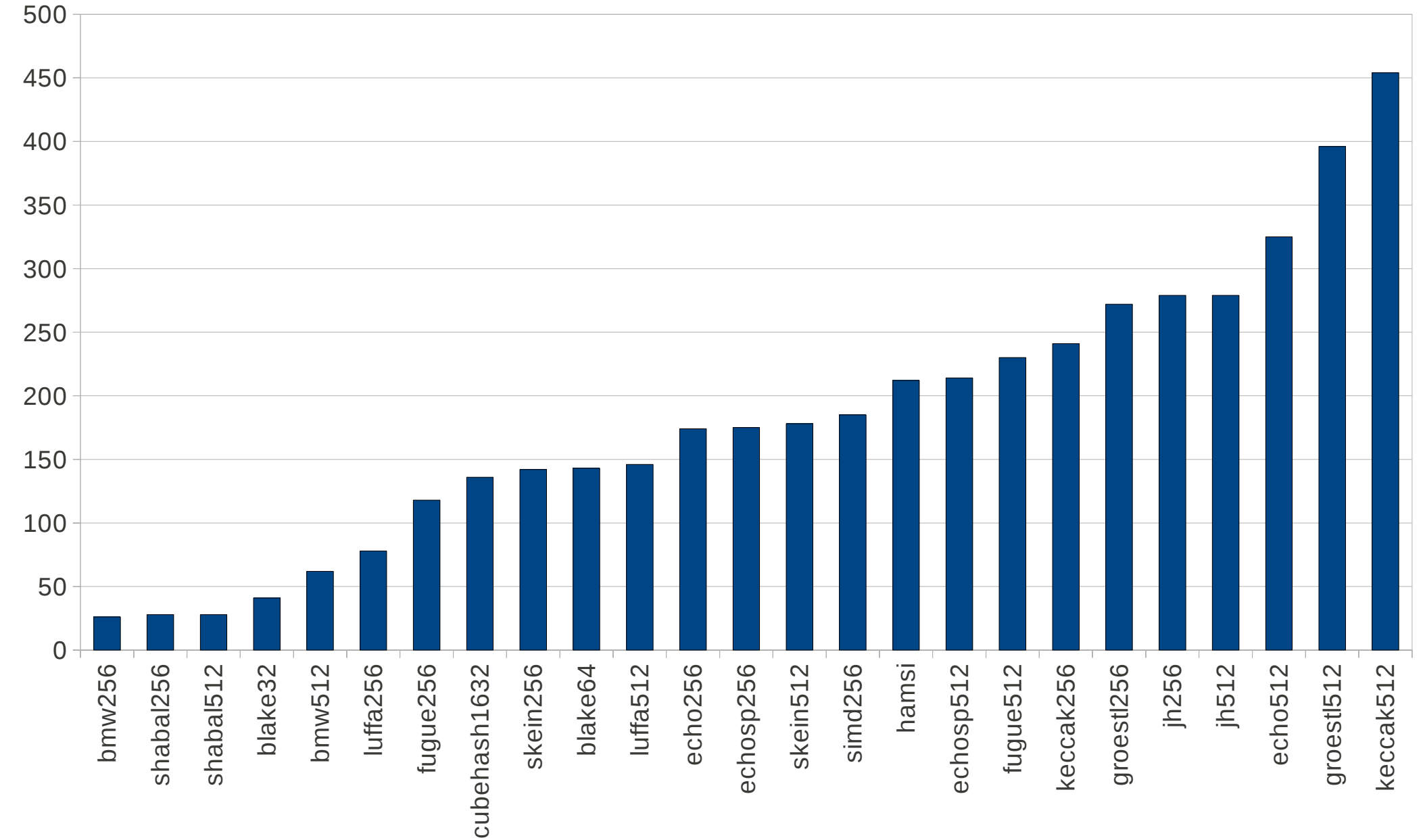


Luminary Micro (TI) lm3s811

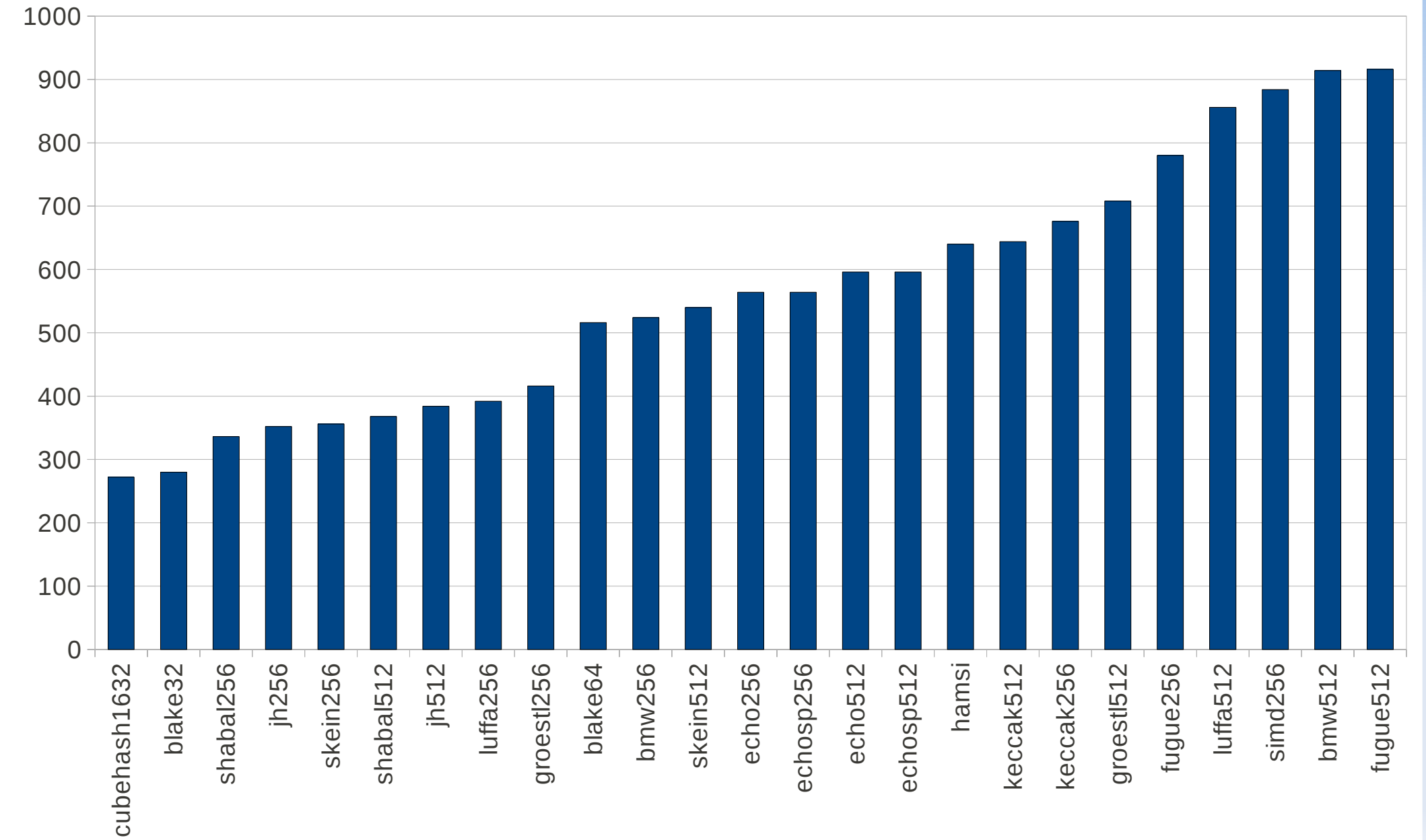
ARM Cortex-M3

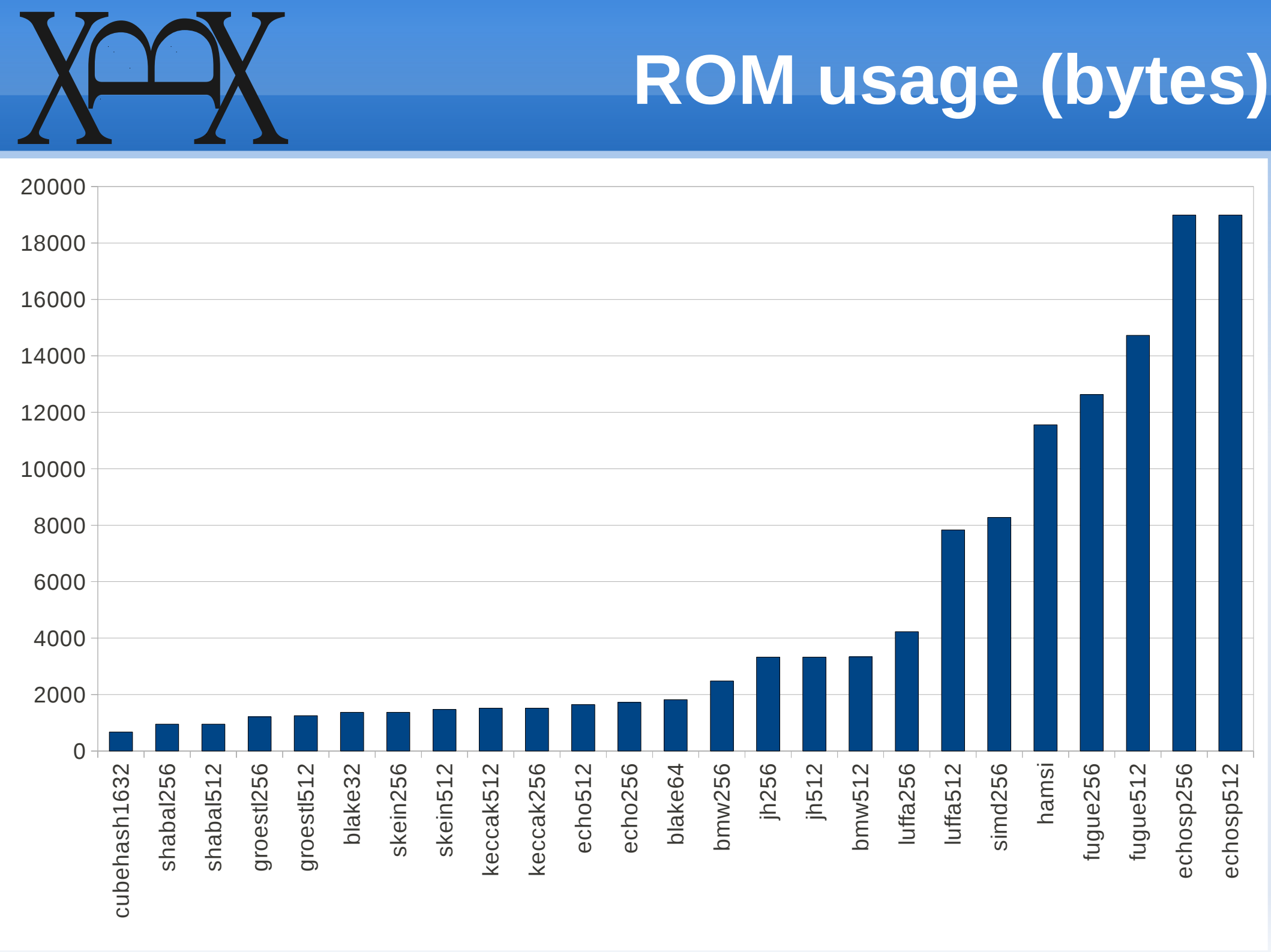
(lm3s811-evb)

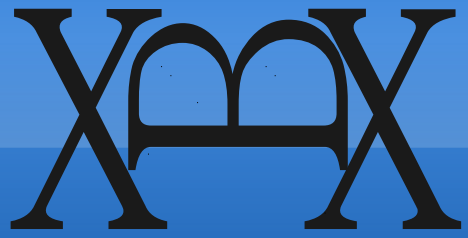
Speed (cpb, long messages)



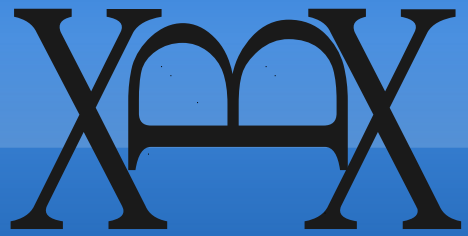
RAM usage (bytes)




ROM usage (bytes)
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
cubehash1632
shabal256
shabal512
groestl256
groestl512
blake32
skein256
skein512
keccak512
keccak256
echo512
echo256
blake64
bmw256
jh256
jh512
bmw512
luffa256
luffa512
simd256
hamsi
fugue256
fugue512
echosp256
echosp512



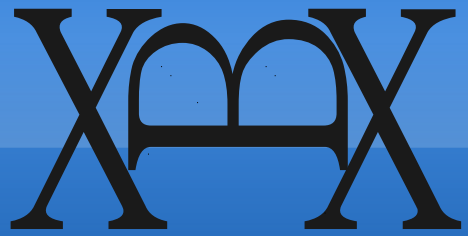
Summary and Conclusion



Speed (long msg)

Algorithm	Atmega1281,AVR	Atmega1284,AVR	Fritzbox,AR7(MIPS)	Artila M501,ARM920T	NSLU2,ARMv5TE	LM3S811,Cortex-M3
blake32	**884**	**884**	**58**	**47**	**46**	**41**
blake64	*3795*	*3960*	**129**	**119**	**148**	143
bmw256	**485**	**485**	**37**	**25**	**42**	**26**
bmw512	*2969*	*2969*	**68**	**81**	**76**	**62**
cubehash1632	*4168*	*4168*	162	144	**147**	136
echo256	1065	1065	164	196	196	174
echo512	*2108*	*2108*	*324*	*355*	*385*	*325*
echosp256	-	-	*419*	201	225	175
echosp512	-	-	*489*	240	274	214
fugue256	**810**	**810**	**99**	**107**	**124**	**118**
fugue512	1549	1549	185	198	233	230
groestl256	1309	**451**	*281*	234	296	*272*
groestl512	*3365*	*3365*	*508*	*562*	*449*	*396*
hamsi	*5353*	*5353*	218	*266*	261	212
jh256	*2637*	*2637*	256	*345*	292	*279*
jh512	*2637*	*2637*	256	*333*	292	*279*
keccak512	*7949*	*7949*	*441*	*571*	*581*	*454*
keccak256	*4572*	*4572*	156	150	209	241
luffa256	*2722*	*2722*	**107**	**86**	**75**	**78**
luffa512	*4688*	*4688*	199	178	**140**	146
shabal256	**210**	**210**	**27**	**25**	**35**	**28**
shabal512	**210**	**210**	**27**	**25**	**30**	**28**
shavite3256	-	**635**	-	-	**126**	-
simd256	*2353*	*2353*	218	238	216	185
simd512	-	-	260	*333*	296	-
skein256	1204	1204	**95**	**122**	**110**	142
skein512	1443	1443	**116**	156	151	178

Visual coding	**Best – 2.5 X Best**	**2.5 X – 5 X Best**	5 X – 10 X Best	*>10X Best*



RAM

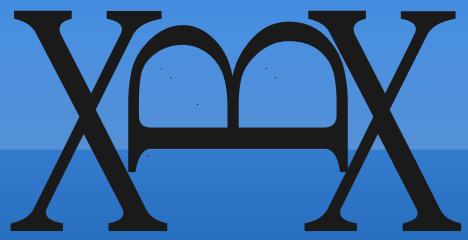
Algorithm	Atmega1281,AVR	Atmega1284,AVR	Fritzbox,AR7(MIPS)	Artila M501,ARM920T	NSLU2,ARMv5TE	LM3S811,Cortex-M3
blake32	**269**	**269**	**340**	**272**	**380**	**280**
blake64	**527**	**527**	**548**	**488**	**1140**	**516**
bmw256	**333**	**333**	**616**	**528**	**580**	**524**
bmw512	**1136**	**1136**	1248	**1024**	1748	**914**
cubehash1632	**249**	**249**	**335**	**272**	**260**	**272**
echo256	**697**	**697**	**840**	**728**	**716**	**564**
echo512	**735**	**735**	**872**	**756**	**776**	**596**
echosp256	-	-	**788**	**760**	**812**	**564**
echosp512	-	-	**820**	**792**	**844**	**596**
fugue256	*3024*	*3024*	**220**	**452**	**708**	**780**
fugue512	*3056*	*3055*	**784**	**764**	**732**	**916**
groestl256	**346**	**346**	**452**	**360**	**352**	**416**
groestl512	**642**	**642**	**788**	**656**	**648**	**708**
hamsi	*5065*	*5065*	**296**	**212**	**288**	**640**
jh256	1631	1631	**392**	**328**	**312**	**352**
jh512	1663	1663	**424**	**360**	**344**	**384**
keccak512	**638**	**638**	**772**	**648**	*2956*	**644**
keccak256	**669**	**670**	**804**	**680**	*2816*	**676**
luffa256	**762**	**762**	**420**	**364**	**356**	**392**
luffa512	1402	1402	**796**	**544**	**667**	**856**
shabal256	**296**	**296**	**404**	**327**	**716**	**336**
shabal512	**328**	**328**	**436**	**360**	**644**	**368**
shavite3256	-	*6663*	1424	-	1412	-
simd256	*2970*	*2970*	**1028**	**944**	**1192**	**884**
simd512	-	-	1856	1764	1720	-
skein256	**266**	**266**	**520**	**380**	1508	**356**
skein512	**427**	**427**	**704**	**492**	**972**	**540**

Visual coding	**Best – 2.5 X Best**	**2.5 X – 5 X Best**	5 X – 10 X Best	*>10X Best*

ROM

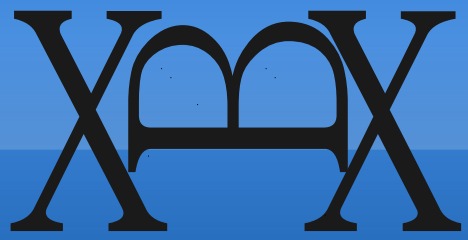
Algorithm	Atmega1281,AVR	Atmega1284,AVR	Fritzbox,AR7(MIPS)	Artila M501,ARM920T	NSLU2,ARMv5TE	LM3S811,Cortex-M3
blake32	**3528**	**3586**	**3106**	**2080**	**3736**	**1372**
blake64	**6398**	**6472**	**3618**	**5092**	7104	**1820**
bmw256	**1910**	**1910**	**6538**	**3784**	7032	**2480**
bmw512	*16724*	*16812*	**7117**	**5020**	*14076*	**3340**
cubehash1632	**1470**	**1470**	**2167**	**1260**	**1312**	**672**
echo256	**3296**	**3598**	**4598**	**3168**	7056	**1724**
echo512	**3312**	**3662**	**4550**	**3168**	7016	**1644**
echosp256	-	-	*22792*	*20900*	*20932*	*18988*
echosp512	-	-	*22792*	*20900*	*20932*	*18988*
fugue256	10212	10212	17134	*42342*	*14298*	*12632*
fugue512	10212	10212	19958	*42342*	*16766*	*14728*
groestl256	**2214**	**2214**	**2963**	**1892**	**1628**	**1212**
groestl512	**2306**	**2306**	**3310**	**1952**	**1696**	**1252**
hamsi	*46478*	*46478*	15267	*156408*	*14284*	*11556*
jh256	8760	8760	**6058**	**4284**	**4200**	**3324**
jh512	8760	8760	**6058**	**4284**	**4200**	**3324**
keccak512	**3870**	**3928**	**3755**	**2196**	*16528*	**1520**
keccak256	**3870**	**3928**	**3755**	**2196**	*16528*	**1520**
luffa256	*20380*	*20380*	**7862**	10852	**5412**	4228
luffa512	*45252*	*45252*	15205	10852	11852	*7836*
shabal256	**1900**	**1900**	**2500**	**3096**	*17840*	**952**
shabal512	**1898**	**1898**	**2500**	**3096**	*17488*	**952**
shavite3256	-	*65922*	*31480*	-	*24880*	-
simd256	*31930*	*31930*	12386	*28416*	10844	*8276*
simd512	-	-	**6846**	9794	**4570**	-
skein256	**2398**	**2398**	**4615**	**2880**	*23912*	**1372**
skein512	**2500**	**2500**	**4679**	**3148**	10868	**1472**

Visual coding				
Best – 2.5 X Best	**2.5 X – 5 X Best**	5 X – 10 X Best	*>10X Best*	



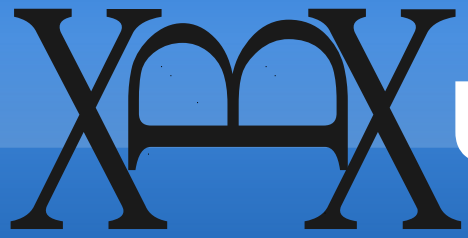
Conclusions

- Shabal, BMW and Blake are consistently fast
  - They are good with RAM and ROM usage, too
- Grøstl has small ROM, good RAM usage
  - Is fast on AVR (asm) but not (yet) ARM
- CubeHash is king of ROM, good with RAM
  - Achieves decent speed
  - Great in really constrained environments like smartcards
- Hamsi can be extremely good with RAM
  - Even though only generic implementation yet!



Caveats

- Please read the paper with the full results
- Please keep in mind that architecture aware implementations make a huge difference
  - All of the 13 smallest candidates for both RAM and ROM on AVR are avr-crypto-lib implementations
  - The four fastest candidates on AVR are assembly implementations and Skein256 should bring that number up to five, soon
  - SHAvite, JH, Luffa, Fugue, Keccak, SIMD and Hamsi suffer from a lack of embedded optimized implementations



Updates until Aug 22

Algo	Feature	Old	New	Old/New Ratio	Comment
Skein-256	cpb (long msg.)	1204	303	25.17%	Not feature complete but fast and reasonably small. http://www.syntax-k.de/projekte/fhreefish/
Keccak-256	RAM	670	627	93.58%	Assembly rotate, smaller constants. DO / CWB
Keccak-256	ROM	3928	3266	83.15%	Assembly rotate, smaller constants. DO / CWB
Keccak-512	RAM	638	595	93.26%	Assembly rotate, smaller constants. DO / CWB
Keccak-512	ROM	3928	3266	83.15%	Assembly rotate, smaller constants. DO / CWB