XBX Benchmarking Results January 2012

Christian Wenzel-Benner[1] Jens Gräf[2] John Pham[3]
Jens-Peter Kaps[3]

[1]ITK Engineering AG, Germany
[2]LiNetCo GmbH, Germany
[3]George Mason University, USA

March 22, 2012

Table Of Contents

XBX: an extension of SUPERCOP-eBASH

XBX: Benchmarking of 'small devices' that

- can execute compiled C code
- can't run a POSIX compliant operating system
- can't run a C compiler
- are often embedded in consumer electronics

XBX: an extension of SUPERCOP-eBASH

Small devices require a different approach to benchmarking:

- Binaries have to be created on another system
- Memory footprint is an important metric
- Standardized timing services are unavailable

SUPERCOP, XBX and Hardware

XBX aims to extend SUPERCOP while retaining the most important features:

- Same source code format, same output format
- Different compilers and compiler option combinations
- Benchmarking of different input data sizes

XBX adds some new features beyond the scope of SUPERCOP:

- Amount of RAM and ROM required by a hash implementation
- Ability to run NIST SHA-3 style KATs on small devices
- Future plans: Energy consumption measurement

XBX Team SHA-3 Criteria

In order to reach a clear and simple recommendation we followed a two-step approach.
The first step, on a per-platform basis, is to:

- Define if memory footprint or speed is most important[1]
- Define if 256- or 512-bit hash results will usually be required[2]
- Apply some human judgement to balance memory and speed requirements in case of close calls
- Find the top three candidates for the platform and rank them

In the second step the individual ranking results are aggregated into a single score per candidate and an overall ranking is reached.

[1] The ARM Cortex-M3 based LM3S811 platform is considered two times, once with memory footprint and once with speed as most important criterion.

[2] This doen't matter for Skein, which is virtually the same at 256- and 512-bit

Presentation of Platform Diagrams

For every target platform the speed of the candidate hash implementations is measured as well as RAM and ROM consumption. RAM and ROM consumption are merged into an 'Area' metric.

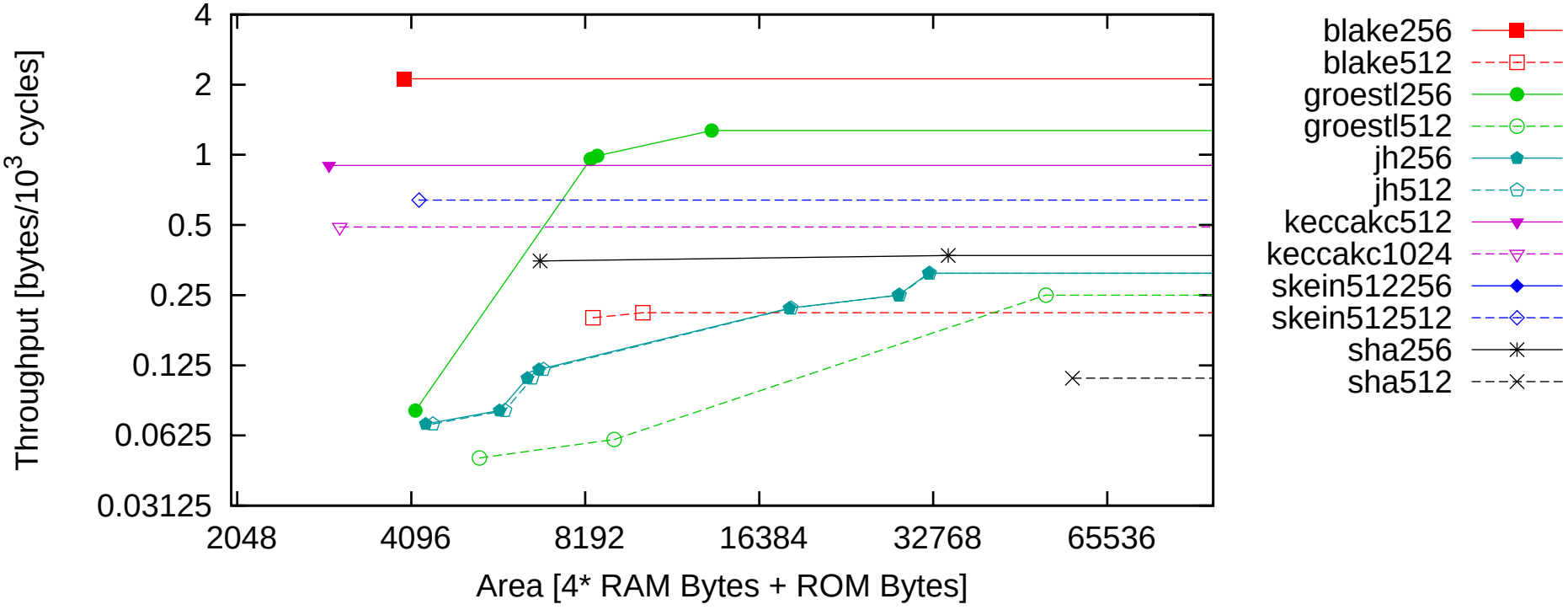
- Colour coding as in SUPERCOP shoot-out diagrams
- Solid shapes and lines for 256-bit version, dashed for 512-bit
- Both axes are scaled base-2 logarithmic
- X-Axis: $Area = 4 * RAM + ROM$, identical range for all platforms
- Y-Axis: Throughput in bytes per kilocycles

Benchmarking Results

Benchmarking results and ranking of candidates per platform.

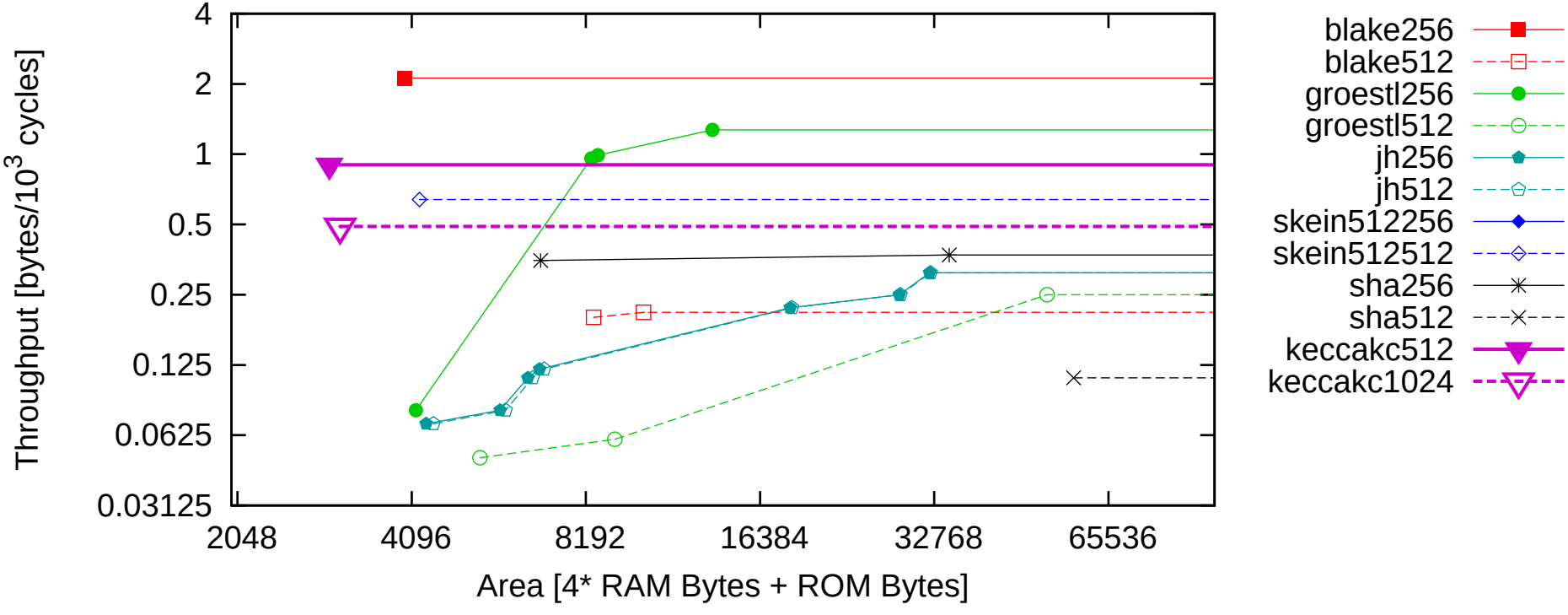
AVR (8-bit): Atmel ATmega1284P

- Best XBX platform for estimating smart card performance
- Memory footprint most important, focus on 256-bit hashes
- Detailed discussion of candidate ranking on next slide



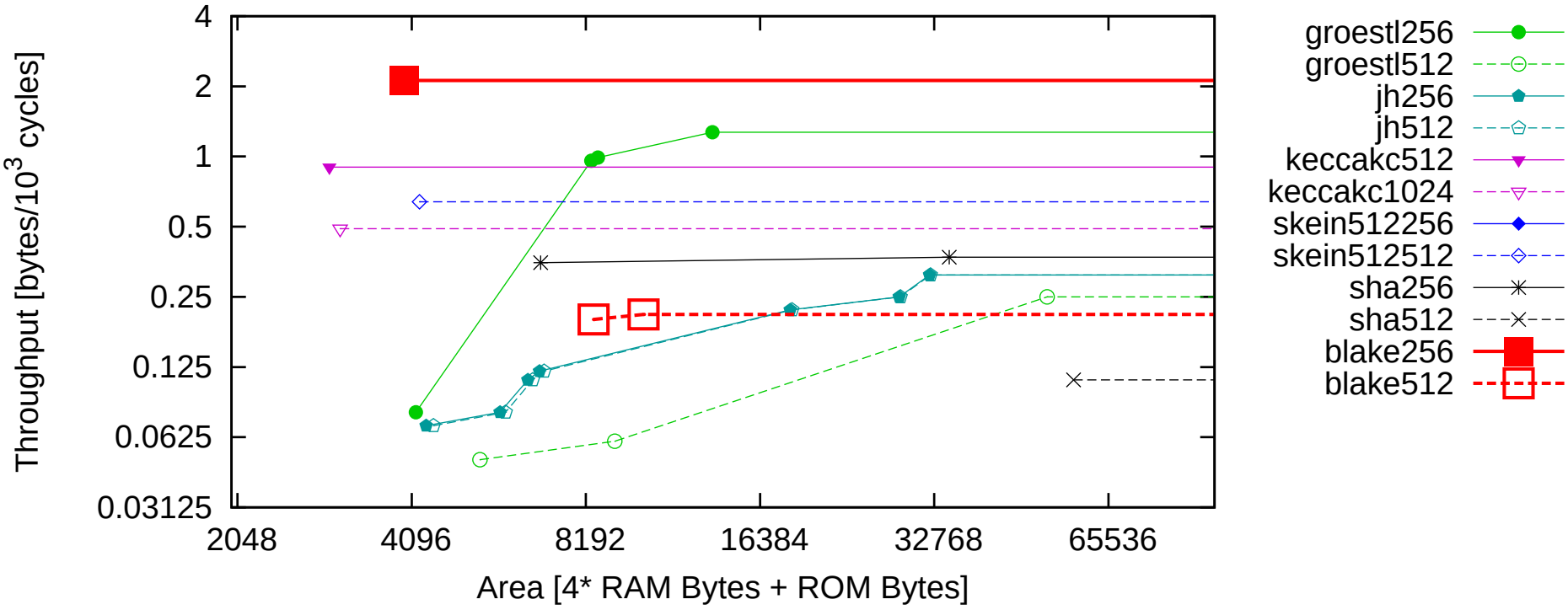
AVR (8-bit): Atmel ATmega1284P Ranking

- 1st: Keccak



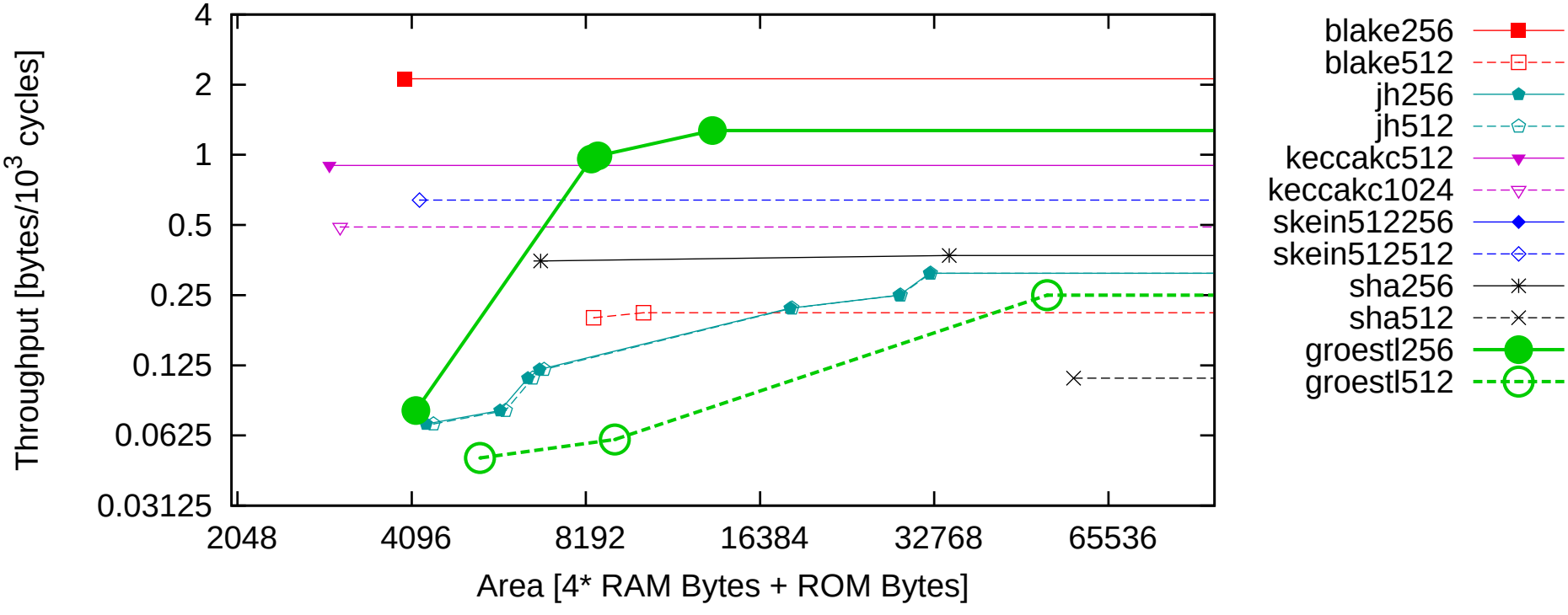
AVR (8-bit): Atmel ATmega1284P Ranking

- 1st: Keccak
- 2nd: BLAKE



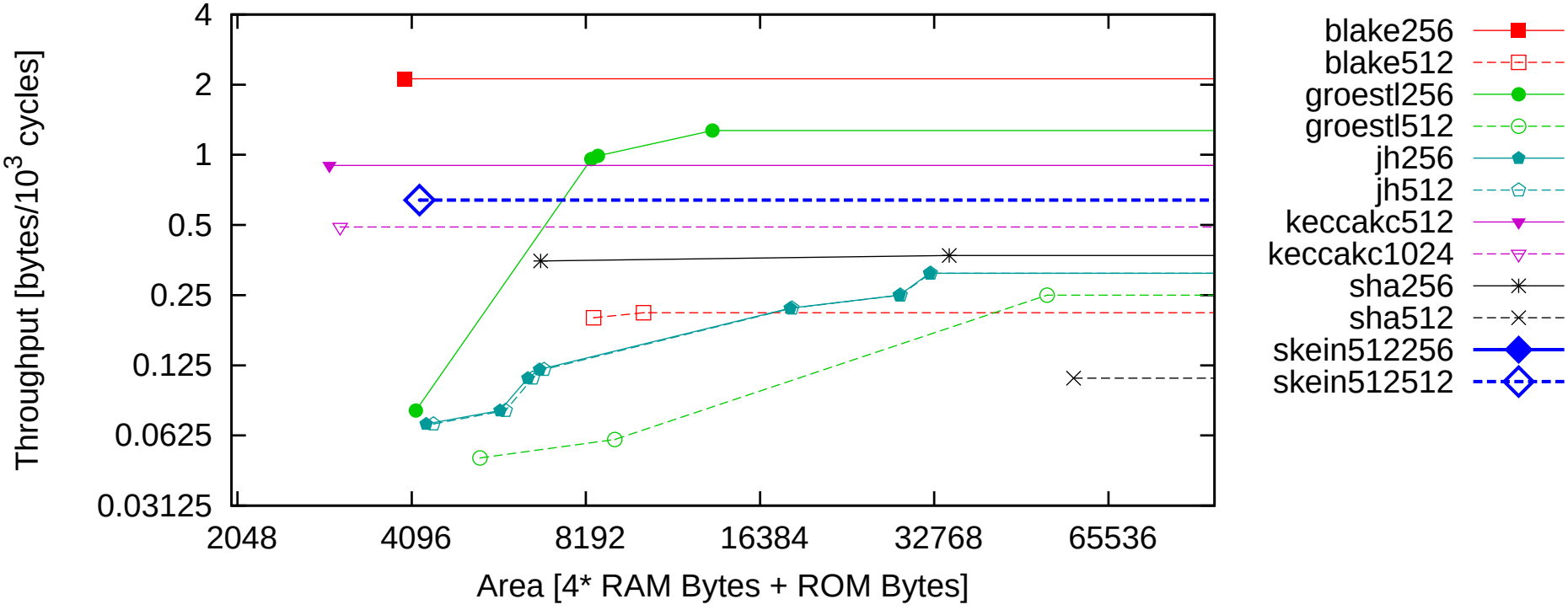
AVR (8-bit): Atmel ATmega1284P Ranking

- 1st: Keccak
- 2nd: BLAKE
- 3rd: Grøstl and Skein are tied



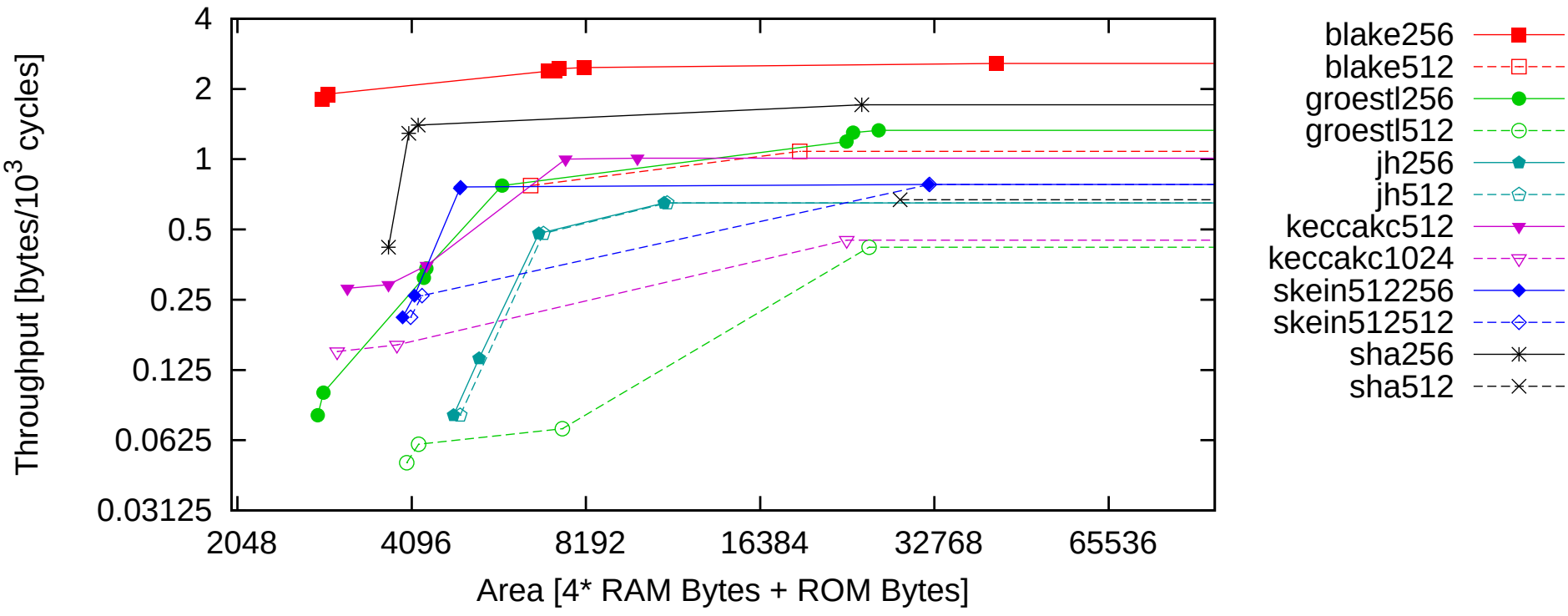
AVR (8-bit): Atmel ATmega1284P Ranking

- 1st: Keccak
- 2nd: BLAKE
- 3rd: Grøstl and Skein are tied



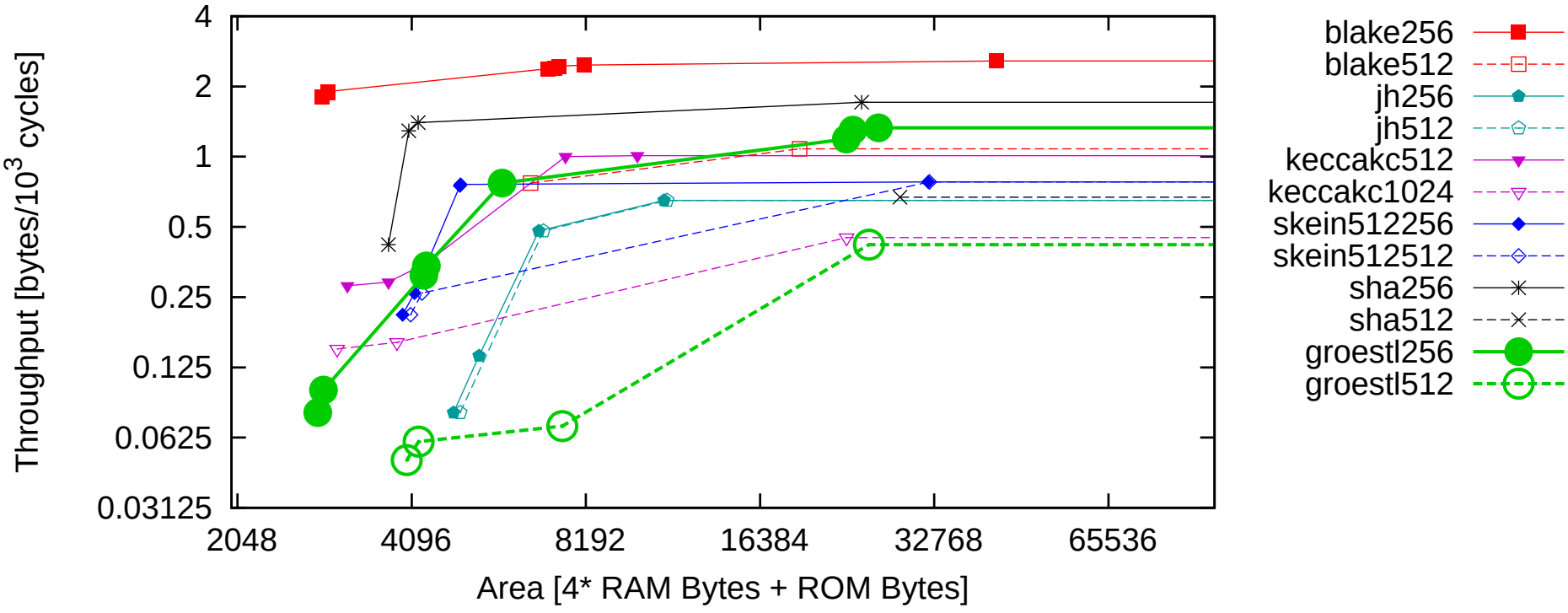
MSP430 (16-bit): Texas Instruments MSP430FG4618

- Low power platform, setup developed at GMU
- Memory footprint most important, focus on 256-bit hashes
- Detailed discussion of candidate ranking on next slide



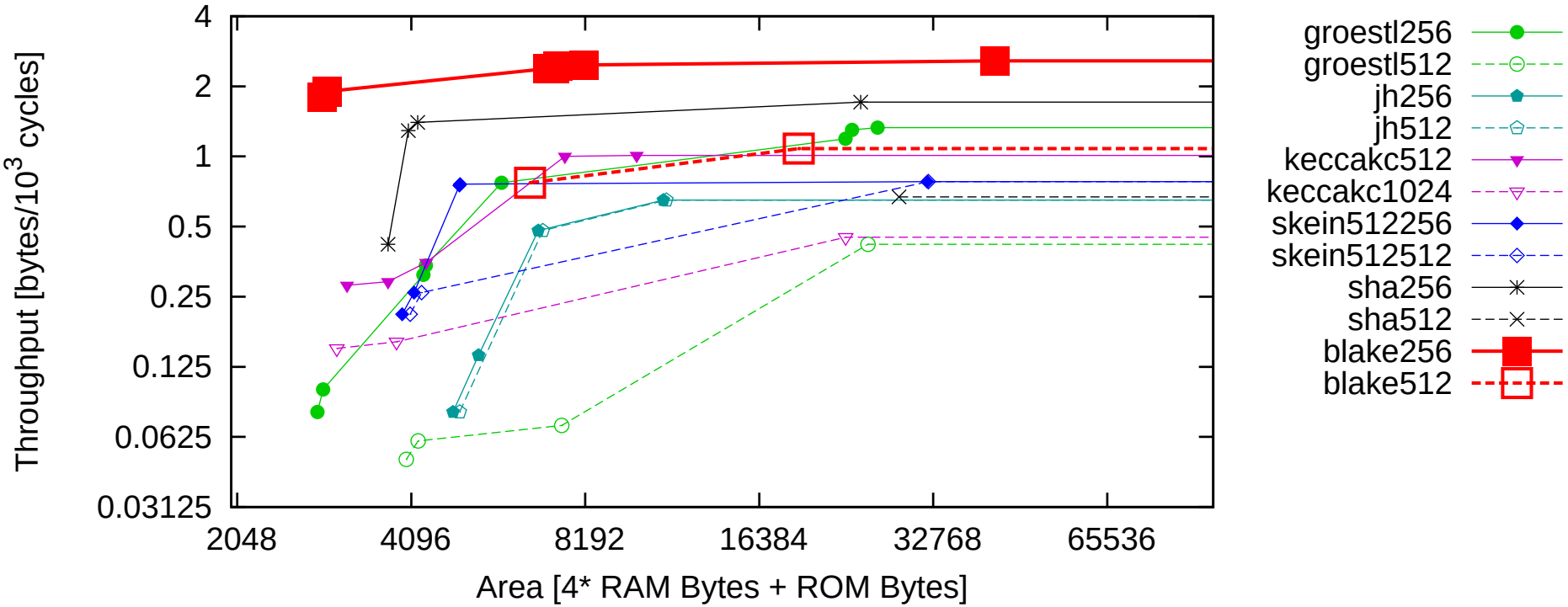
MSP430 (16-bit): MSP430FG4618 Ranking

- 1st: Grøstl and BLAKE are tied



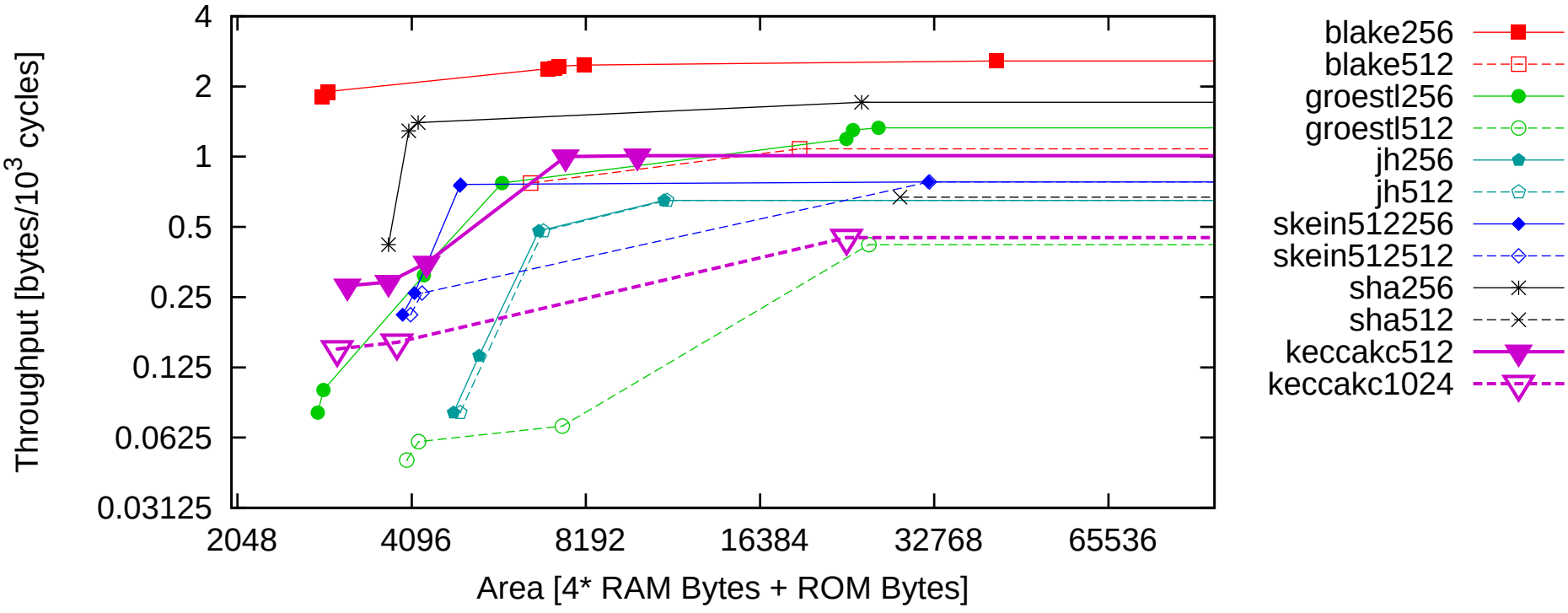
MSP430 (16-bit): MSP430FG4618 Ranking

- 1st: Grøstl and BLAKE are tied



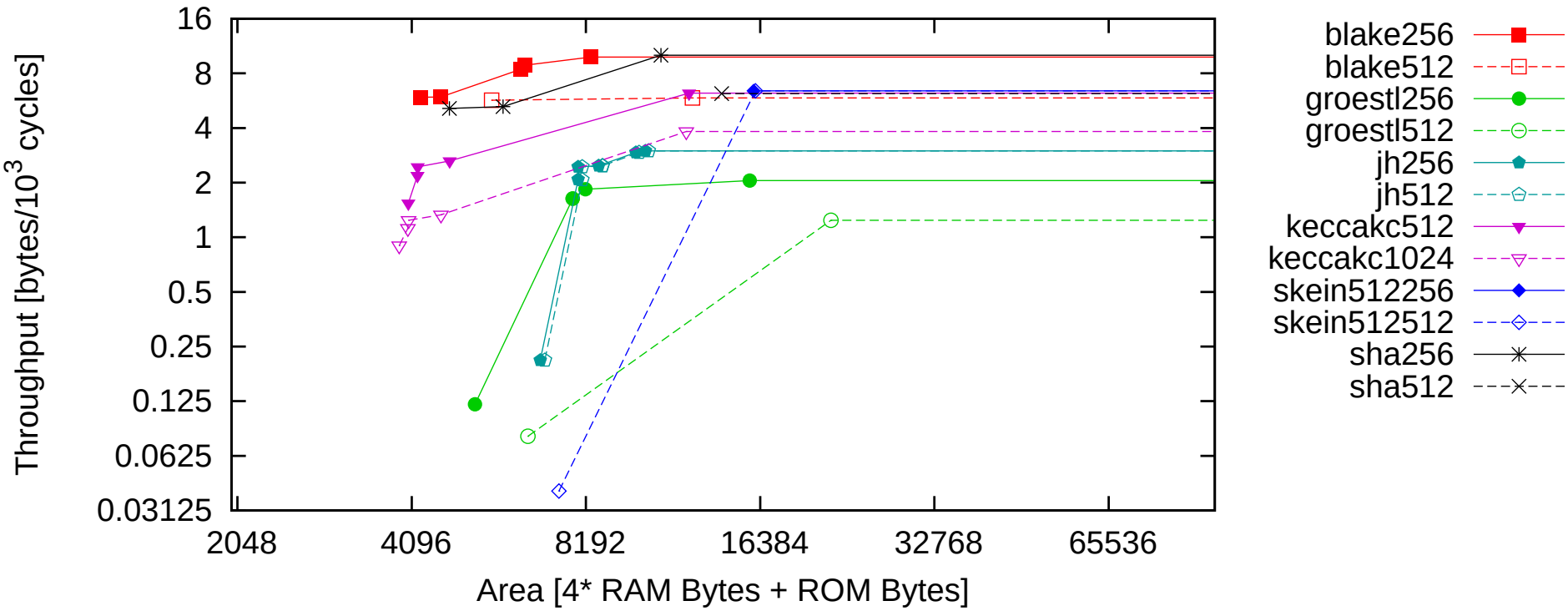
MSP430 (16-bit): MSP430FG4618 Ranking

- 1st: Grøstl and BLAKE are tied
- 3rd: Keccak



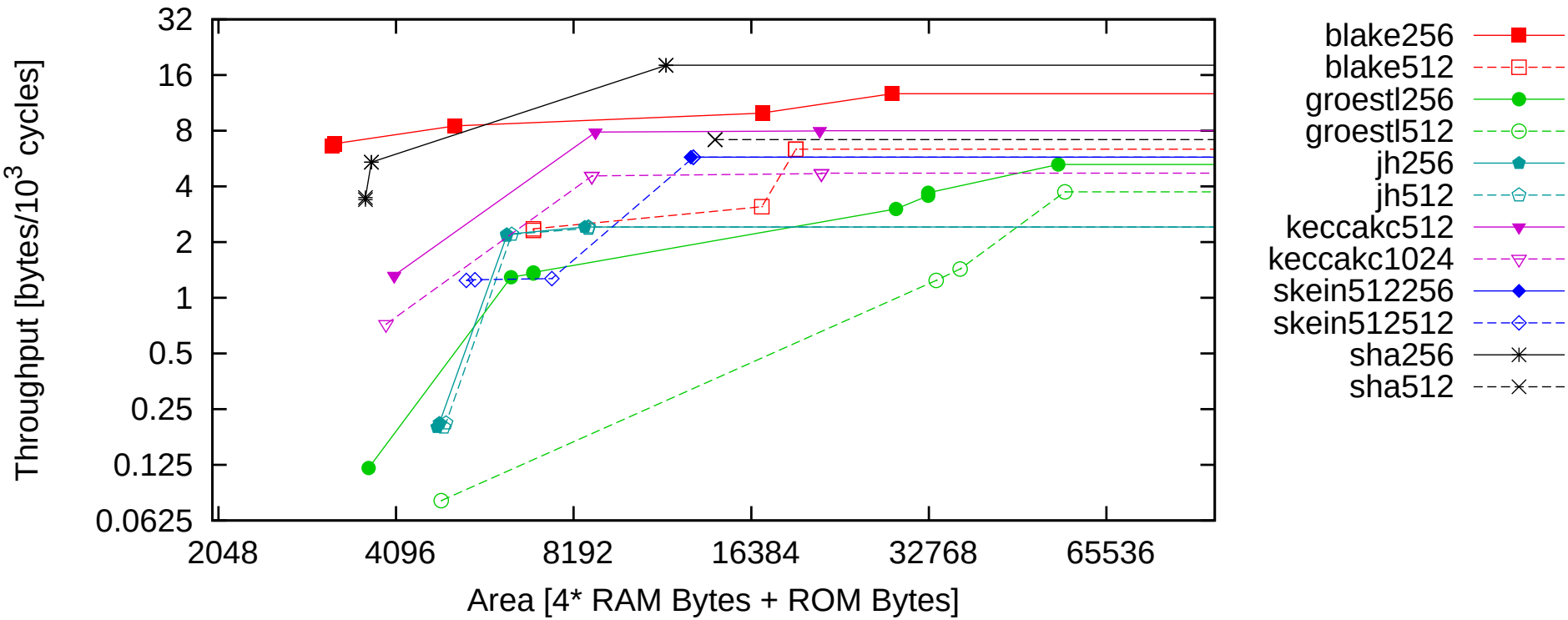
MIPS (32-bit): Texas Instruments AR7

- MIPS core, Linux based, popular in DSL routers
- Throughput most important, no output length focus
- 1st: BLAKE, 2nd: Skein, 3rd: Keccak



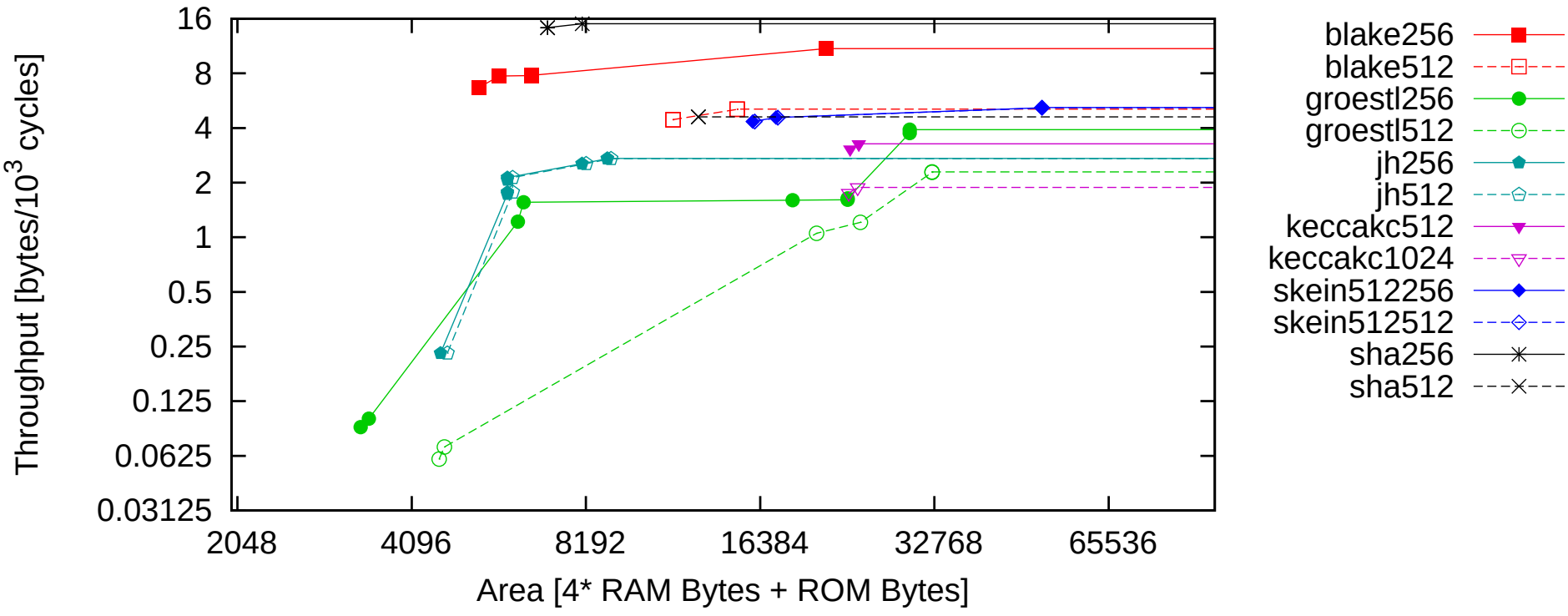
ARM 920T (32-bit): Atmel AT91RM9200

- Older ARM core, Linux based, popular in automation
- Throughput most important, no output length focus
- 1st: BLAKE, 2nd: Keccak and Skein tied



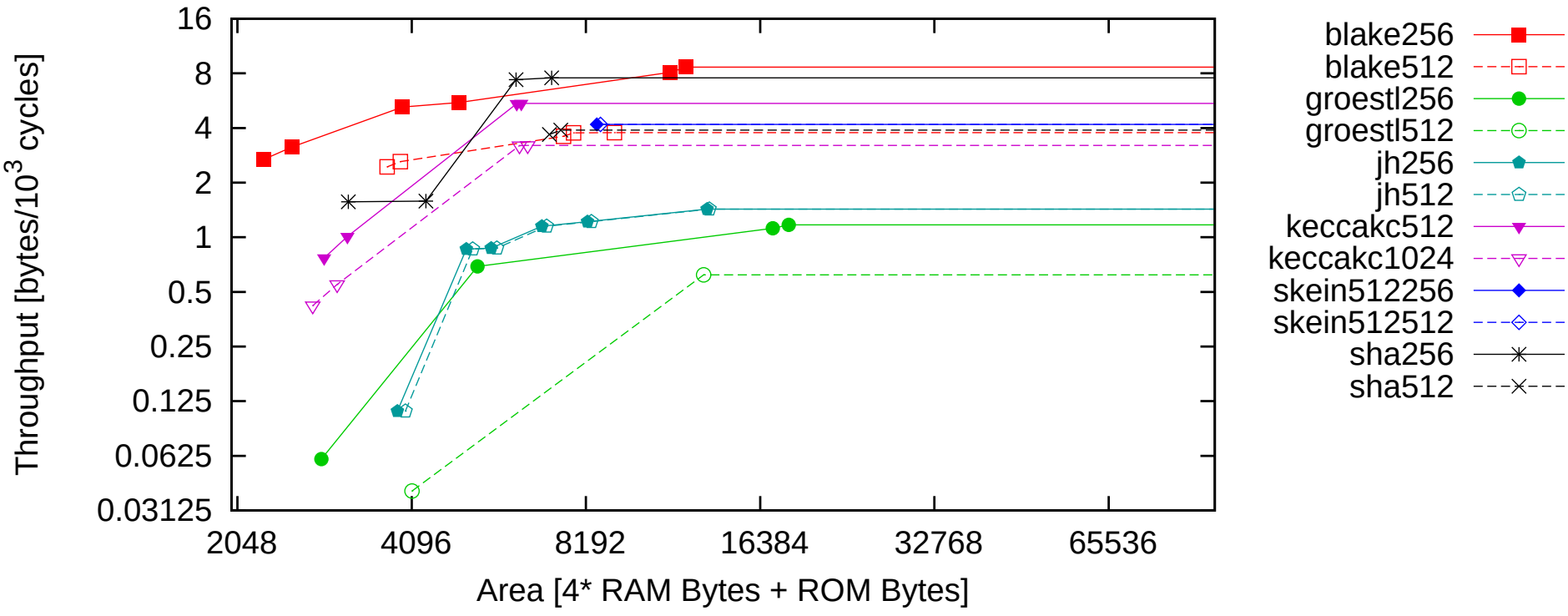
ARMv5TE (32-bit): Intel XScale IXP420

- Older ARM core, Linux based, popular in NAS appliances
- Throughput most important, no output length focus
- 1st: BLAKE, 2nd: Skein, 3rd: Grøstl



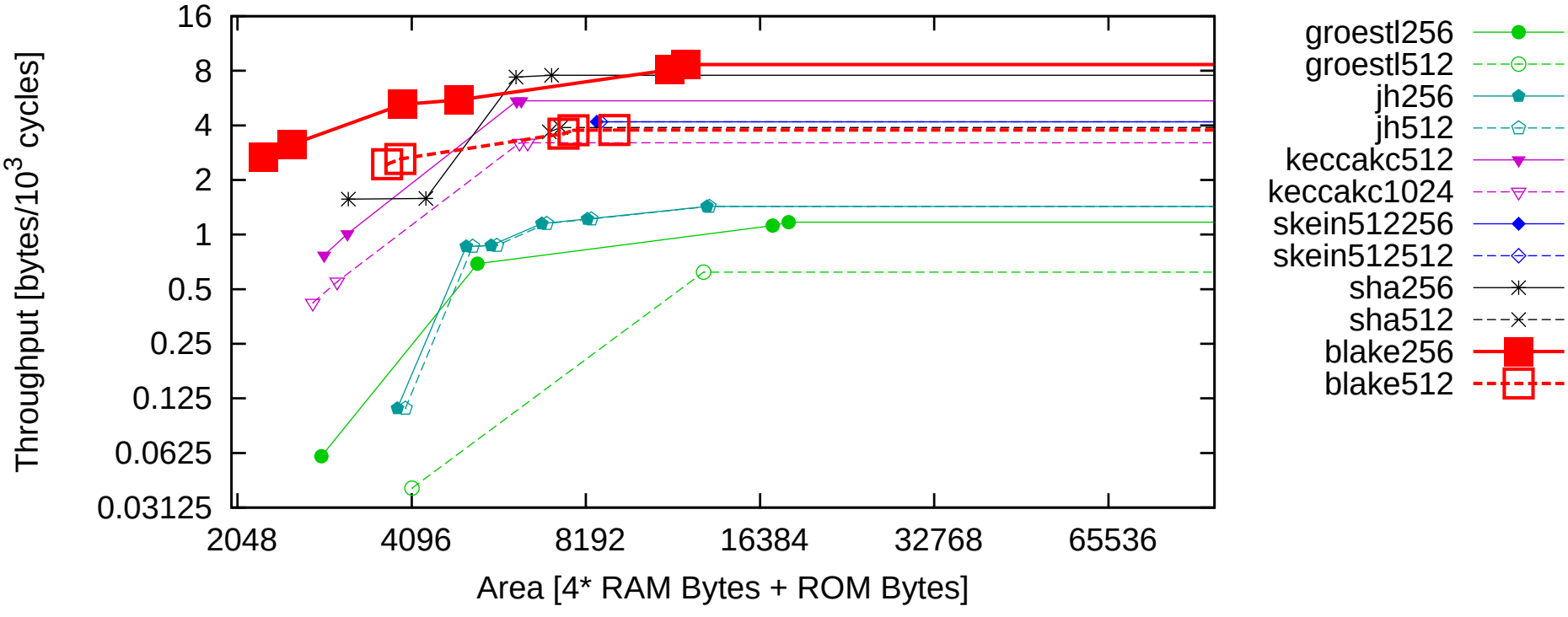
ARM Cortex-M0 (32-bit): NXP LPC1114

- Current ARM core, low cost, used in microcontrollers
- Memory footprint most important but no output length focus
- Detailed discussion of candidate ranking on next slide



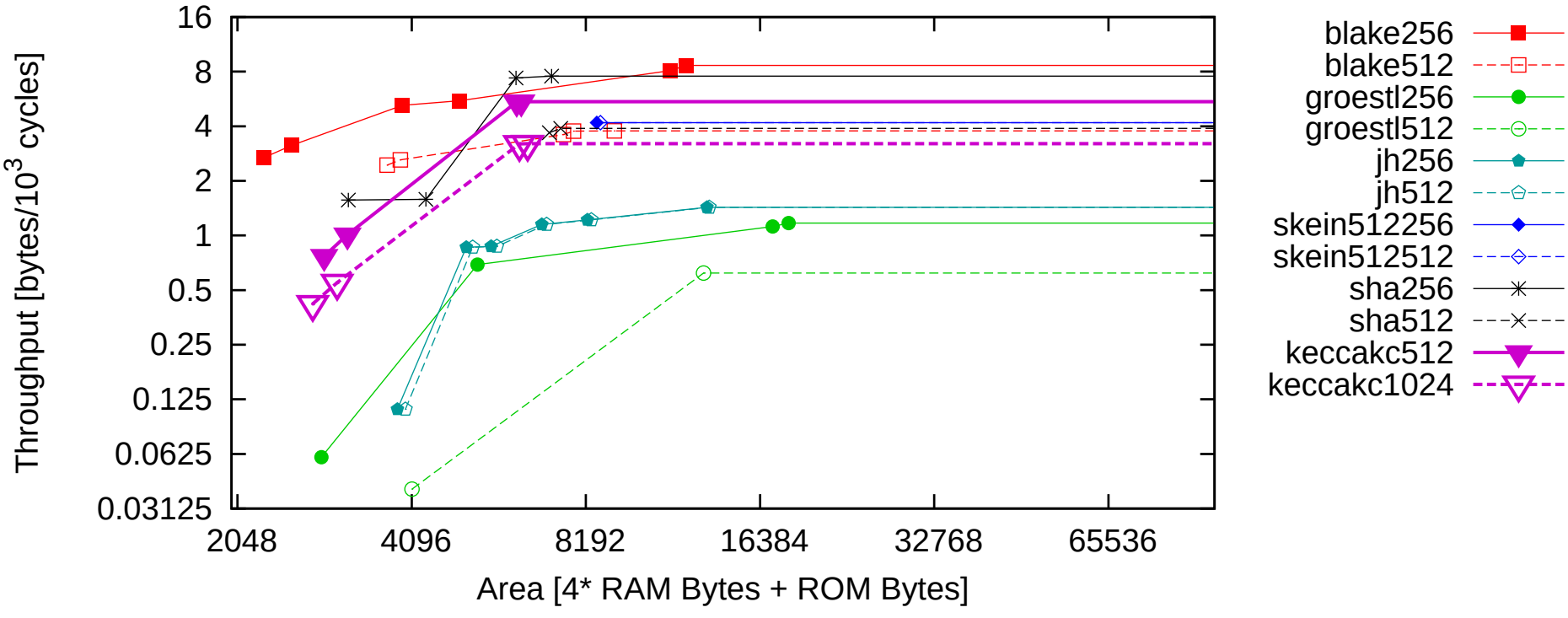
ARM Cortex-M0 (32-bit): NXP LPC1114 Ranking

- 1st: BLAKE



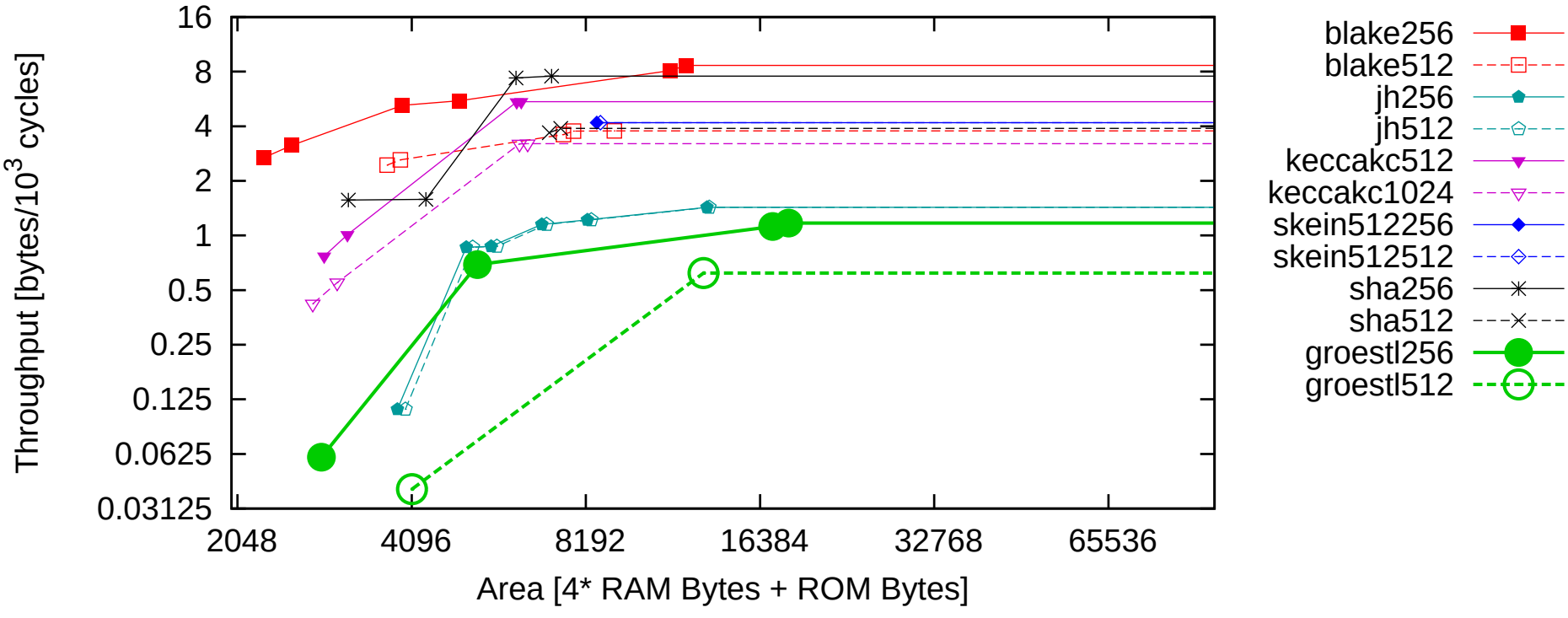
ARM Cortex-M0 (32-bit): NXP LPC1114 Ranking

- 1st: BLAKE
- 2nd: Keccak



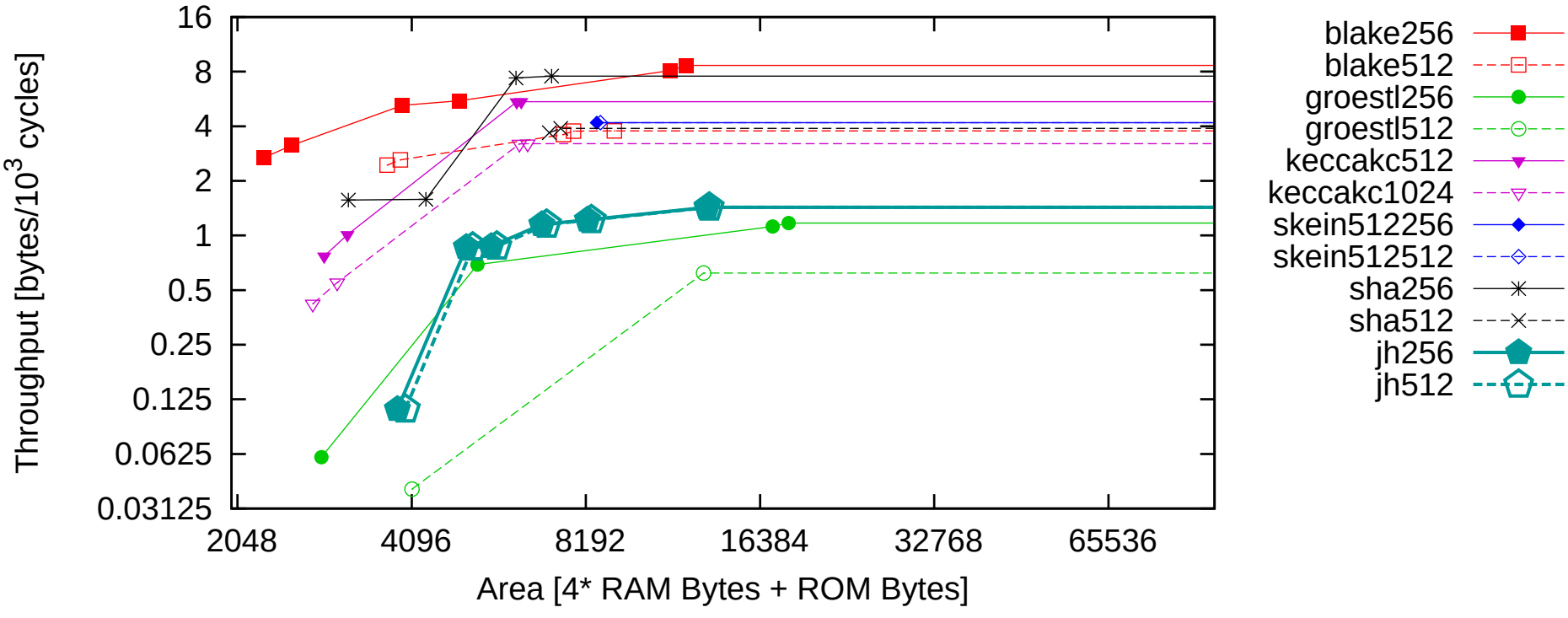
ARM Cortex-M0 (32-bit): NXP LPC1114 Ranking

- 1st: BLAKE
- 2nd: Keccak
- 3rd: Grøstl and JH are tied



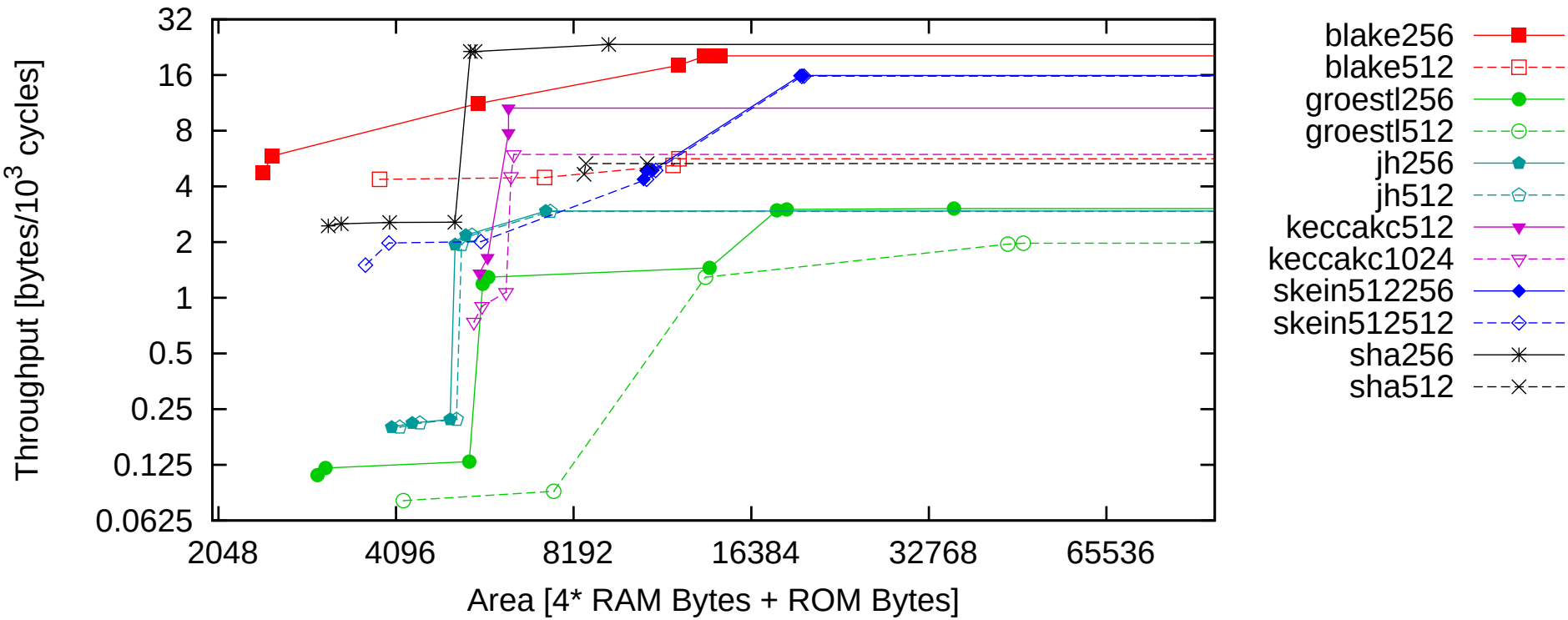
ARM Cortex-M0 (32-bit): NXP LPC1114 Ranking

- 1st: BLAKE
- 2nd: Keccak
- 3rd: Grøstl and JH are tied



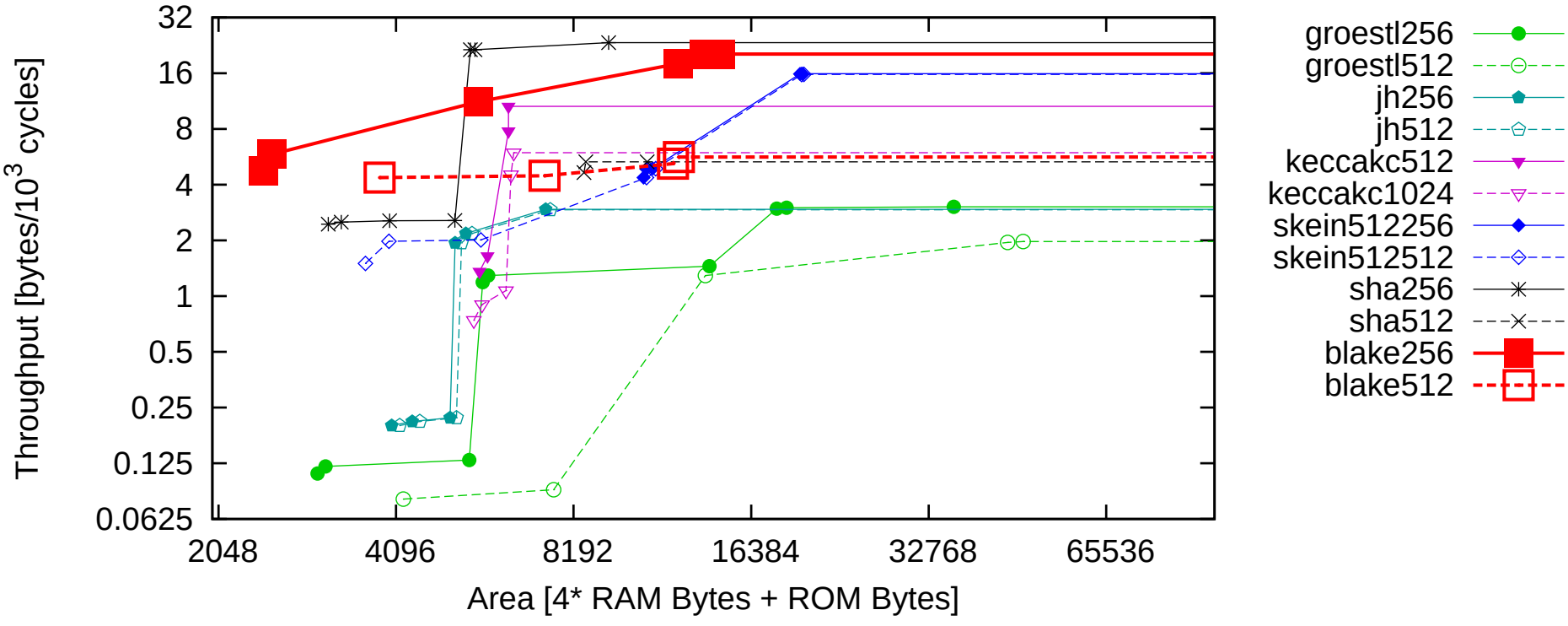
ARM Cortex-M3 (32-bit): Texas Instruments LM3S811

- Current ARM core, cost-performance balanced, two criteria
- Low cost: memory footprint but no output length focus
- Speed: throughput, no output length focus



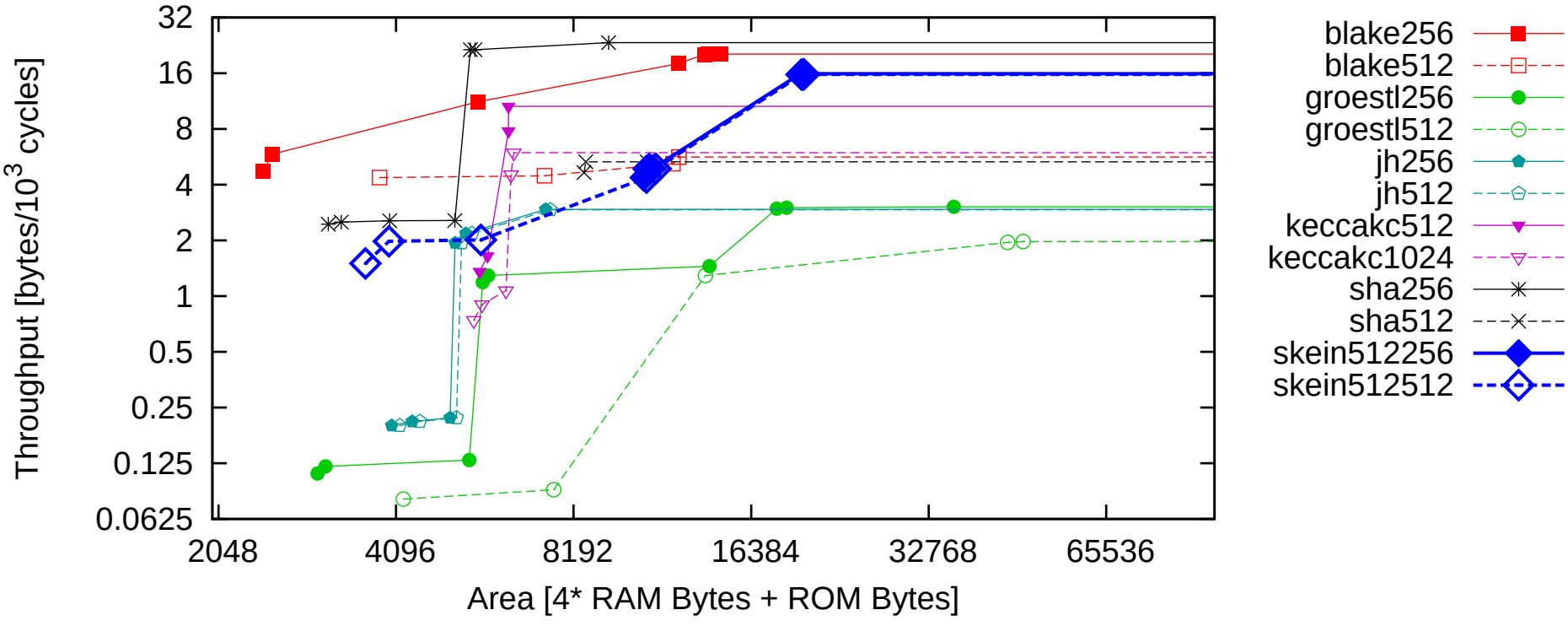
ARM Cortex-M3 (32-bit): TI LM3S811 Low Cost Ranking

- 1st: BLAKE



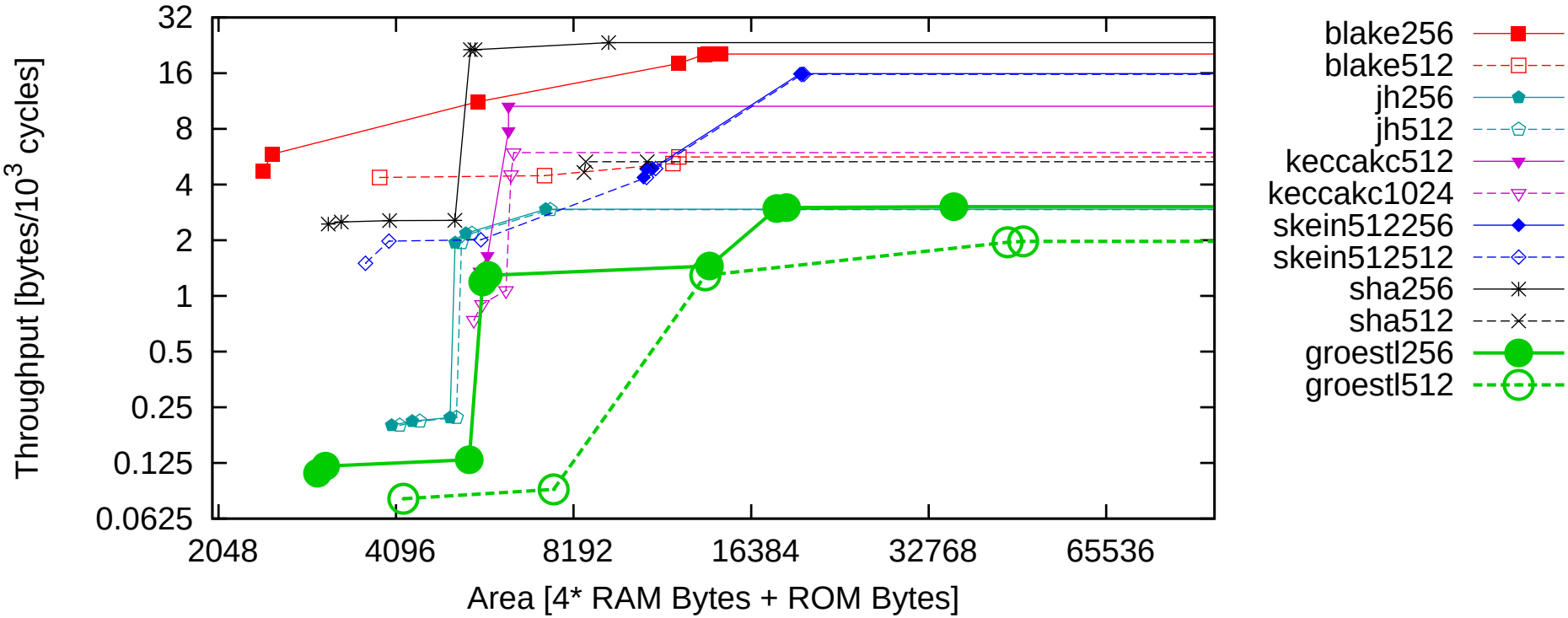
ARM Cortex-M3 (32-bit): TI LM3S811 Low Cost Ranking

- 1st: BLAKE
- 2nd: Skein and Grøstl are tied



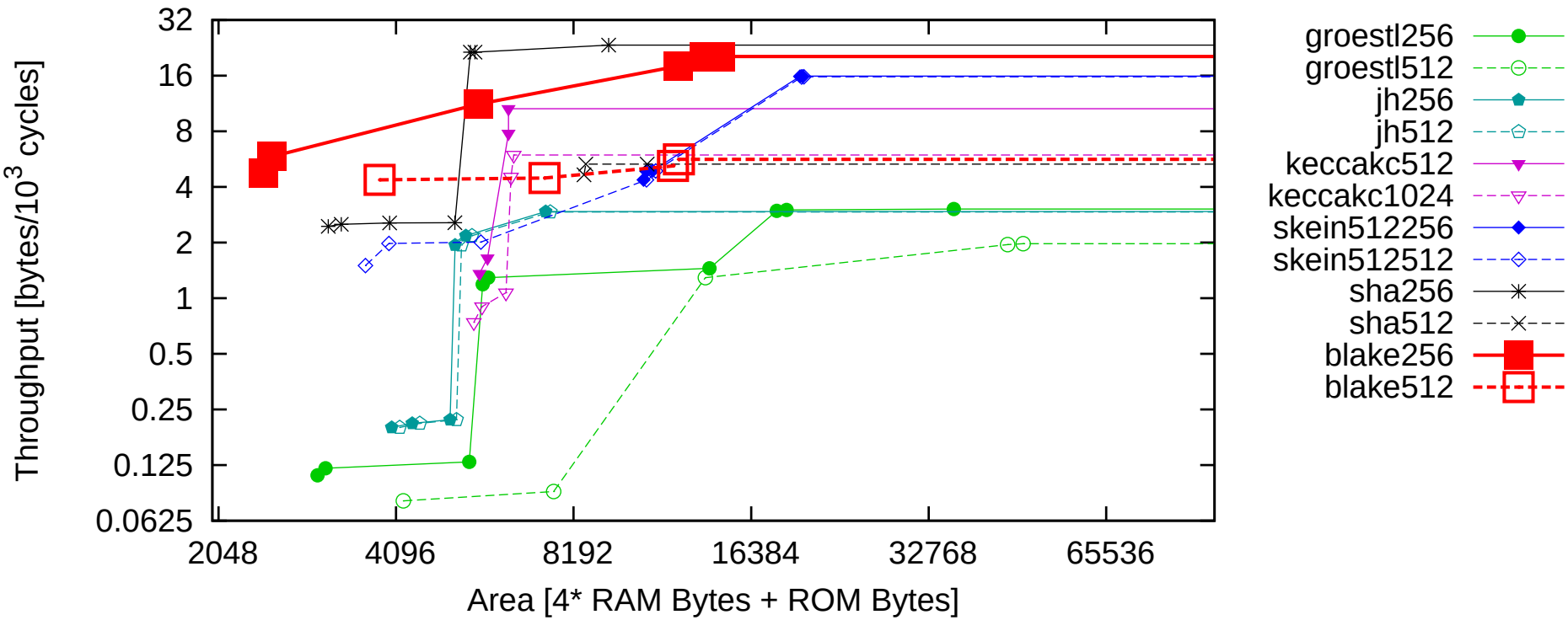
ARM Cortex-M3 (32-bit): TI LM3S811 Low Cost Ranking

- 1st: BLAKE
- 2nd: Skein and Grøstl are tied



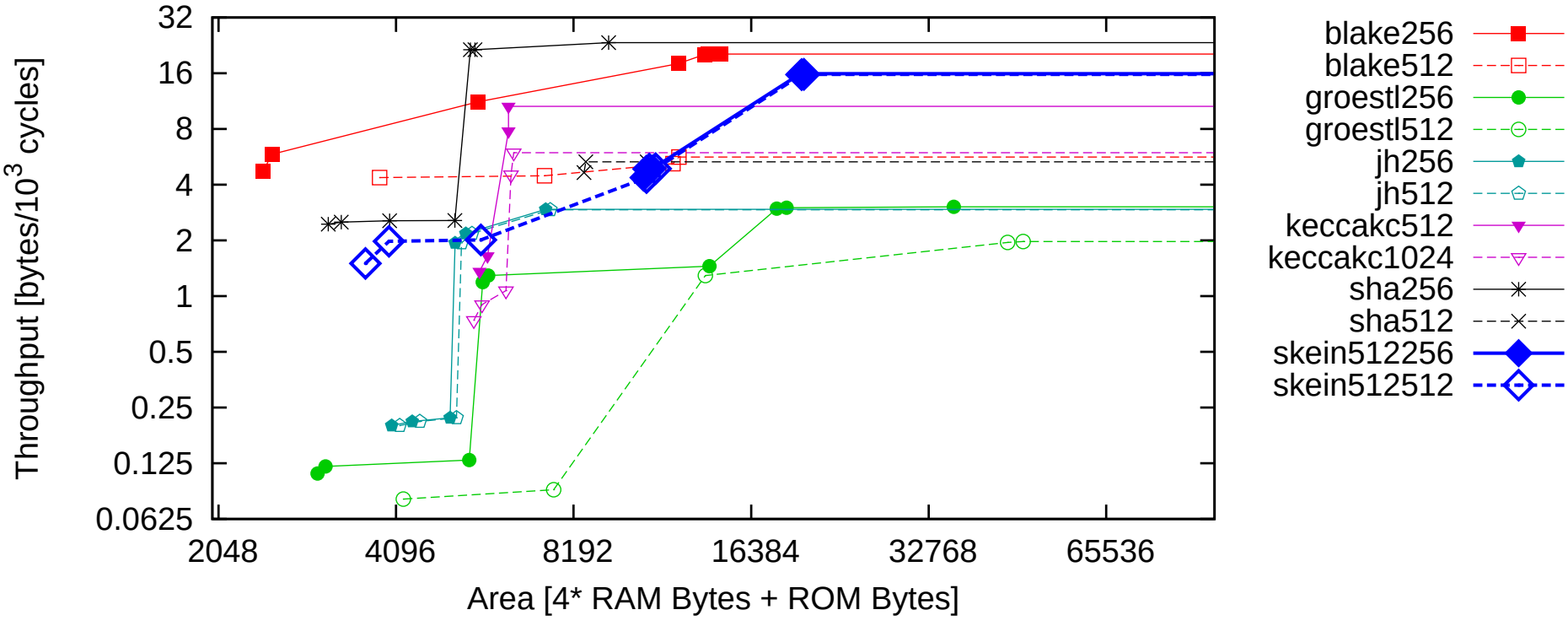
ARM Cortex-M3 (32-bit): TI LM3S811 Speed Ranking

- 1st: BLAKE and Skein are tied



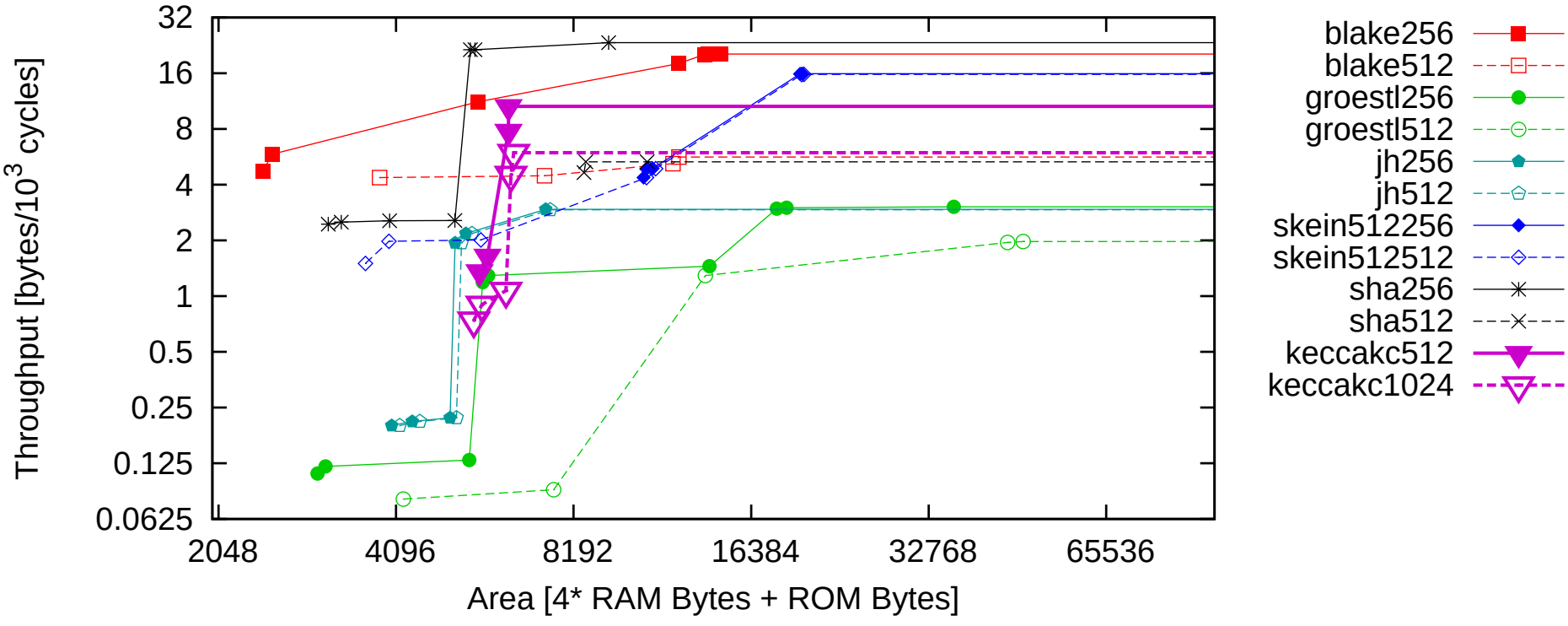
ARM Cortex-M3 (32-bit): TI LM3S811 Speed Ranking

- 1st: BLAKE and Skein are tied



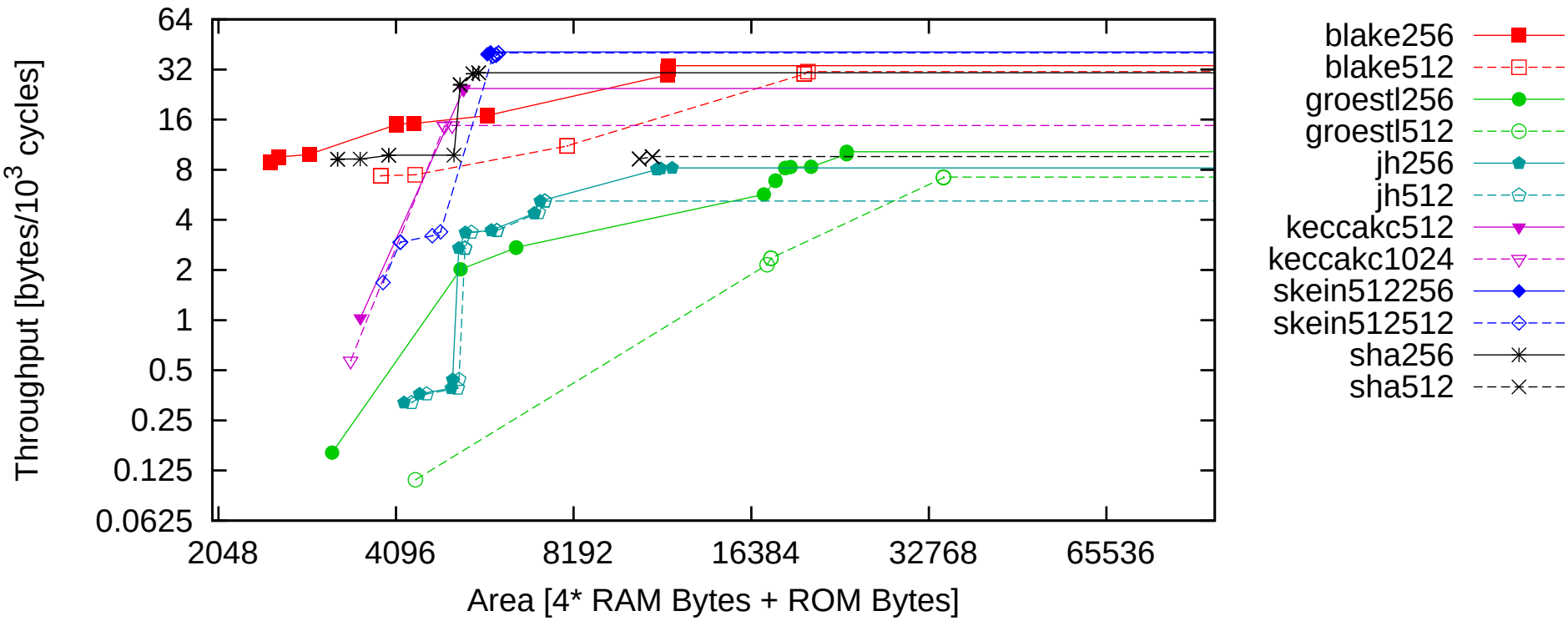
ARM Cortex-M3 (32-bit): TI LM3S811 Speed Ranking

- 1st: BLAKE and Skein are tied
- 3rd: Keccak



ARM Cortex-A8 (32-bit + SIMD): TI DM3730

- Current ARM core with vector extensions, Linux based
- Throughput most important, no output length focus
- 1st: Skein, 2nd: BLAKE, 3rd: Keccak



Conclusion

Bringing it all together:

- Summarize data from 9 (8) platforms
- Three points for a first place
- Two points for a second place
- One for third

XBX Team SHA-3 Choice

SHA-3 Candidate	Ranked 1st (3 points)	Ranked 2nd (2 points)	Ranked 3rd (1 point)	Total Score
BLAKE	7	2	0	25
Keccak	1	2	4	11
Grøstl	1	1	3	8
JH	0	0	1	1
Skein	2	4	1	15

- BLAKE is our overall first choice, balanced for most platforms

XBX Team SHA-3 Choice

SHA-3 Candidate	Ranked 1st (3 points)	Ranked 2nd (2 points)	Ranked 3rd (1 point)	Total Score
BLAKE	7	2	0	25
Keccak	1	2	4	11
Grøstl	1	1	3	8
JH	0	0	1	1
Skein	2	4	1	15

- BLAKE is our overall first choice, balanced for most platforms
- Skein is our overall second choice, strong on fast platforms

XBX Team SHA-3 Choice

SHA-3 Candidate	Ranked 1st (3 points)	Ranked 2nd (2 points)	Ranked 3rd (1 point)	Total Score
BLAKE	7	2	0	25
Keccak	1	2	4	11
Grøstl	1	1	3	8
JH	0	0	1	1
Skein	2	4	1	15

- BLAKE is our overall first choice, balanced for most platforms
- Skein is our overall second choice, strong on fast platforms
- Keccak is our overall third choice, strong on very small platforms

XBX Team SHA-3 Choice

SHA-3 Candidate	Ranked 1st (3 points)	Ranked 2nd (2 points)	Ranked 3rd (1 point)	Total Score
BLAKE	7	2	0	25
Keccak	1	2	4	11
Grøstl	1	1	3	8
JH	0	0	1	1
Skein	2	4	1	15

- BLAKE is our overall first choice, balanced for most platforms
- Skein is our overall second choice, strong on fast platforms
- Keccak is our overall third choice, strong on very small platforms

Update: Grøstl-256 AVR assembly implementation submitted on March 1st makes Grøstl the winner for the Atmel ATmega1284P platform. BLAKE, Skein and Keccak thus loose one score point each. This puts Grøstl in third position tied with Keccak in the overall ranking.

XBX Team SHA-3 Choice Update

SHA-3 Candidate	Ranked 1st (3 points)	Ranked 2nd (2 points)	Ranked 3rd (1 point)	Total Score
BLAKE	7	2 (1)	0 (1)	25 (24)
Keccak	1 (0)	2 (3)	4	11 (10)
Grøstl	1 (2)	1	3	8 (10)
JH	0	0	1	1
Skein	2	4	1 (0)	15 (14)

- BLAKE is our overall first choice, balanced for most platforms
- Skein is our overall second choice, strong on fast platforms
- Keccak and Grøstl are our overall third choice, strong on very small platforms

Update: Grøstl-256 AVR assembly implementation submitted on March 1st makes Grøstl the winner for the Atmel ATmega1284P platform. BLAKE, Skein and Keccak thus loose one score point each. This puts Grøstl in third position tied with Keccak in the overall ranking.