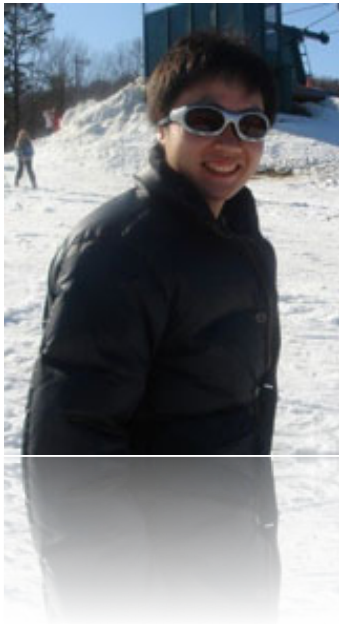


Comprehensive Evaluation of High-Speed and Medium-Speed Implementations of Five SHA-3 Finalists Using Xilinx and Altera FPGAs



**Kris Gaj,
Ekawat Homsirikamol,
Marcin Rogawski,
Rabia Shahid,
Malik Umar Sharif
George Mason University
U.S.A.**

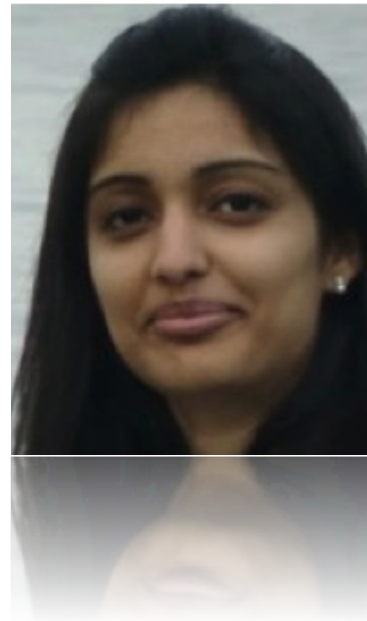
Co-Authors



**Ekawat "Ice"
Homsirikamol**



**Marcin
Rogawski**

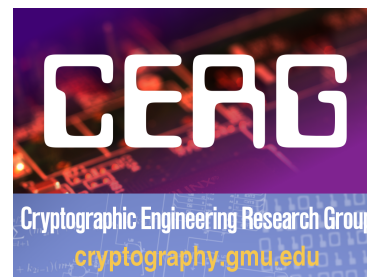


**Rabia
Shahid**



**Malik Umar
Sharif**

**PhD Students,
Members of**



Focus of This Talk

	FPGA	ASIC
High-speed	GMU Gaj et al.	
Low-area		



Motivation & Highlights

Advantages of Benchmarking using FPGAs

- Short development time
- Accurate post-place & route results
- Existence of tools for optimization of program options
- Relatively small number of vendors and device families that dominate the market



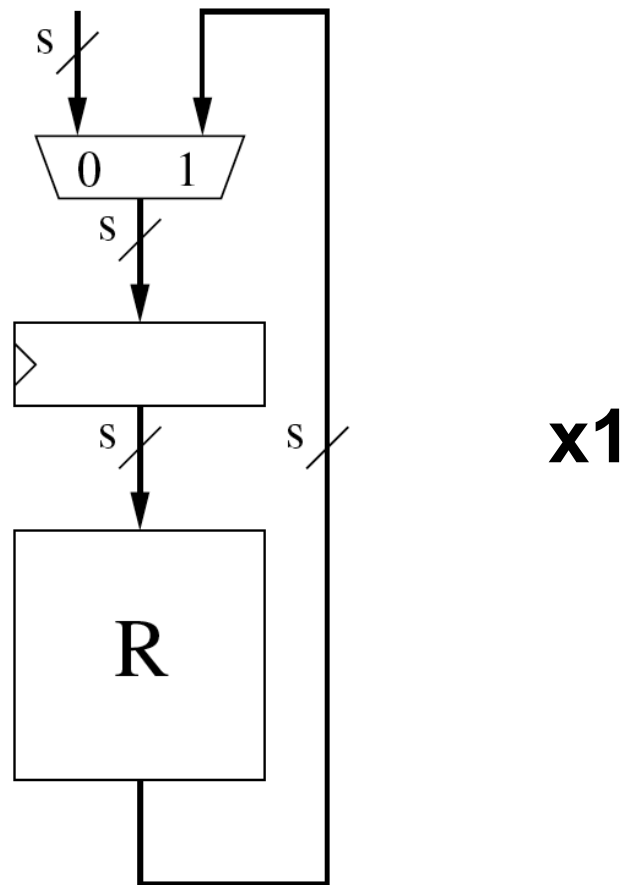
Highlights

- **5 to 10 different architectures per algorithm**
- **Two variants, with a 256-bit and a 512-bit output**
- **Realistic FIFO-based interface**
- **Padding unit for arbitrary size messages**
- **VHDL codes portable among FPGA families**
- **Two primary designers**
- **600+ results for 4 modern FPGA families**
- **Result replication scripts**
- **All source codes available for public scrutiny**

A large yellow oval with a thin blue border, centered on the slide.

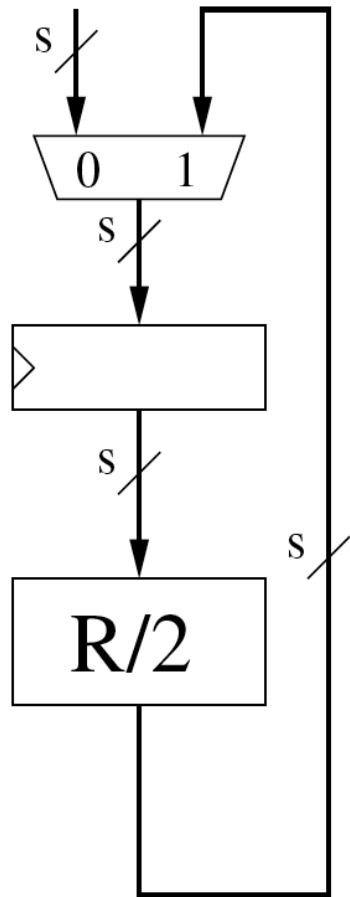
Investigated Hardware Architecture

Basic Iterative Architecture



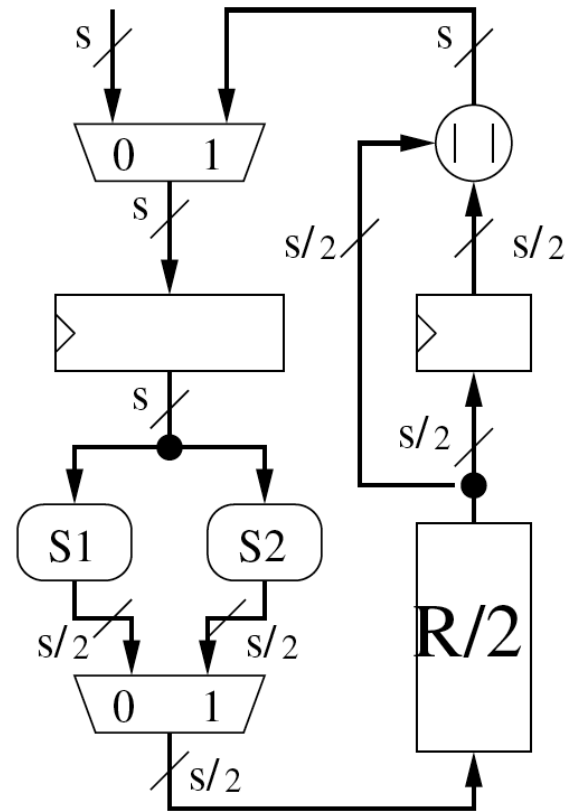
Currently, most common architecture used to implement SHA-1, SHA-2, and many other hash functions.

Folded Architectures



/2(h)

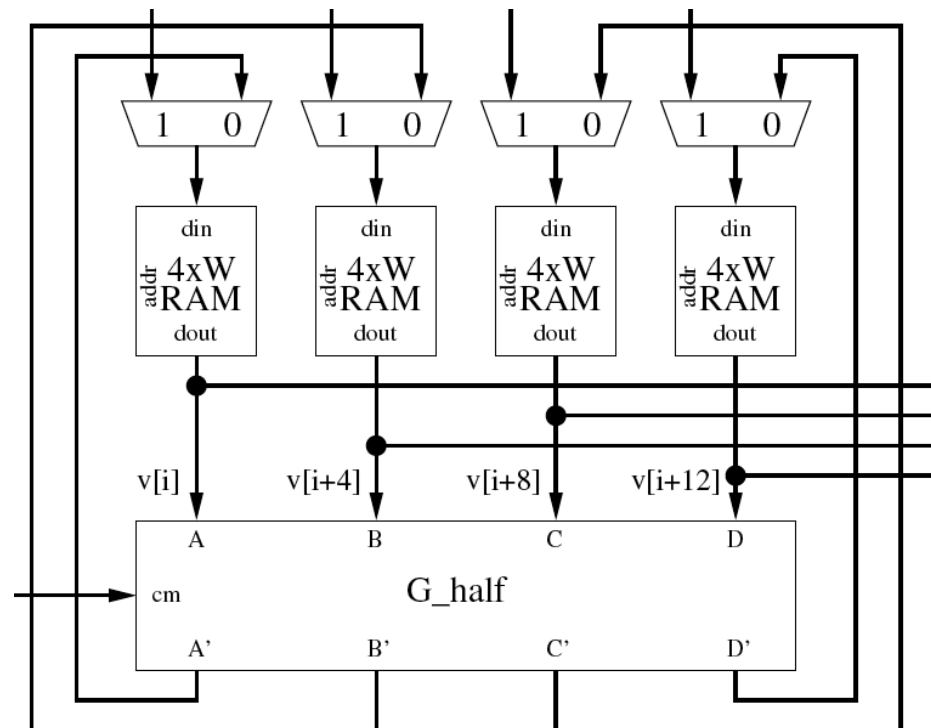
Folded Horizontally



/2(v)

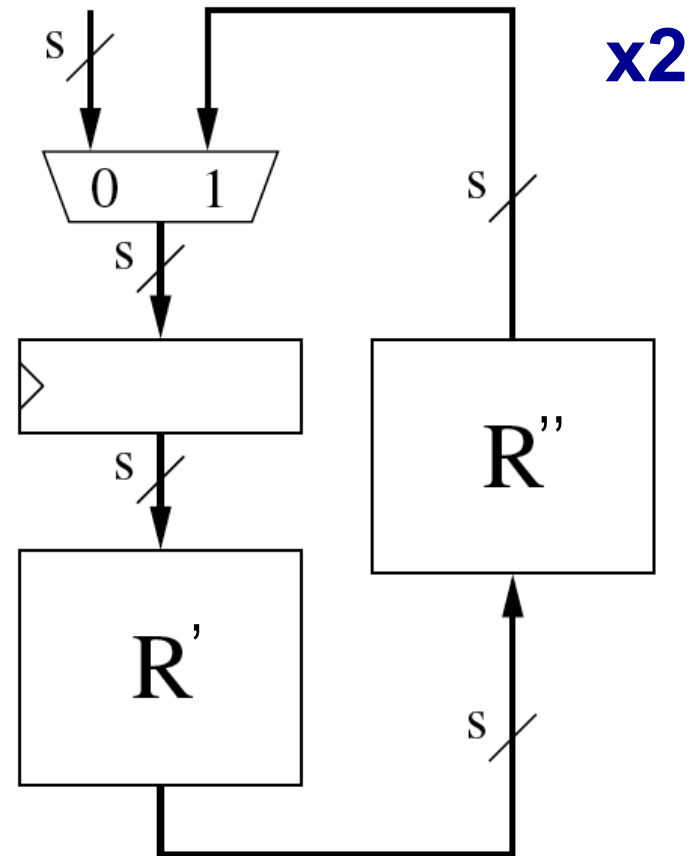
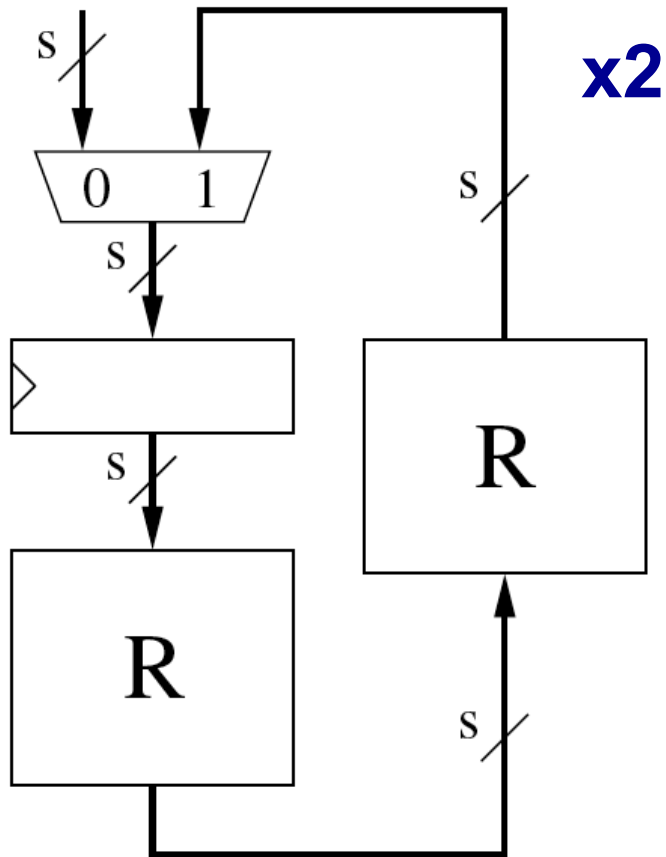
Folded Vertically

Folded Architectures with the State Kept in Memory

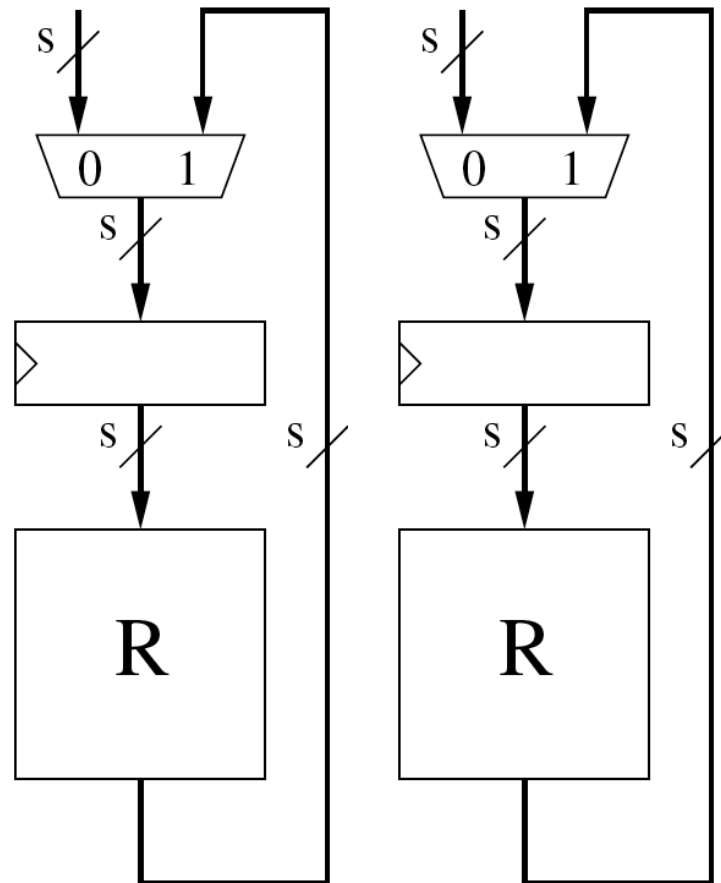


$/4(h)/4(v)-m$

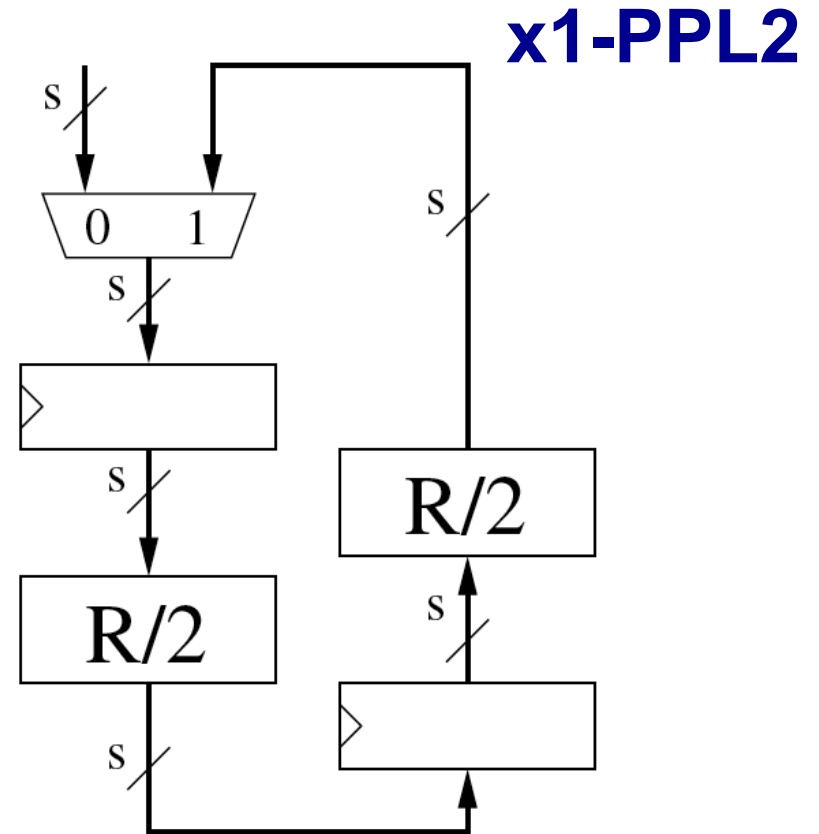
Unrolled Architectures



Multi-Unit Architecture



MU2



Basic architecture with 2 Pipeline Stages

FPGA Families

FPGA Families

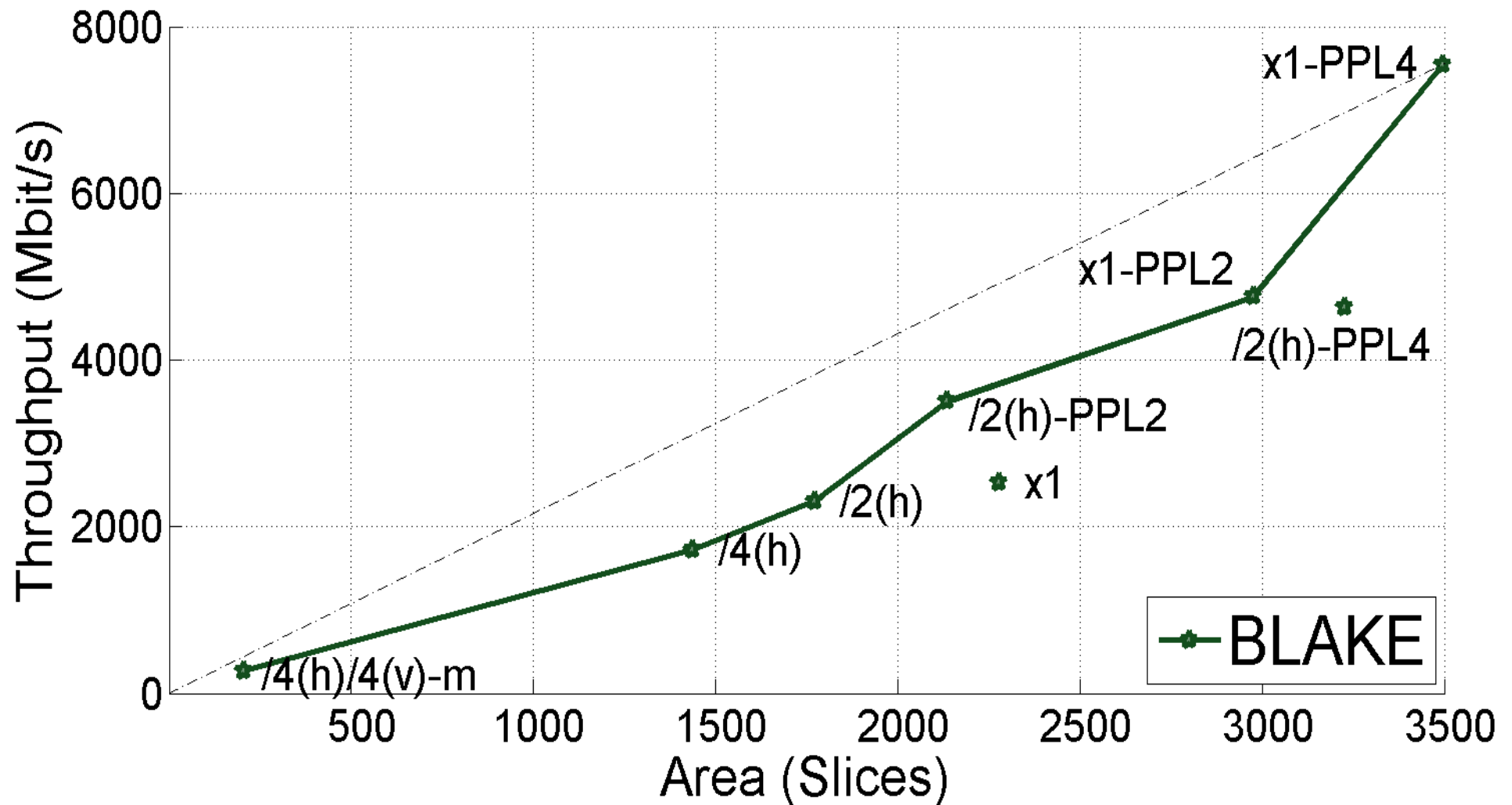
- two major vendors: Altera and Xilinx (~90% of the market)
- two most recent high-performance families

	Altera		Xilinx	
Technology	Low-cost	High-performance	Low-cost	High-performance
90 nm	Cyclone II	Stratix II	Spartan 3	Virtex 4
65 nm	Cyclone III	Stratix III		Virtex 5
40-60 nm	Cyclone IV	Stratix IV	Spartan 6	Virtex 6

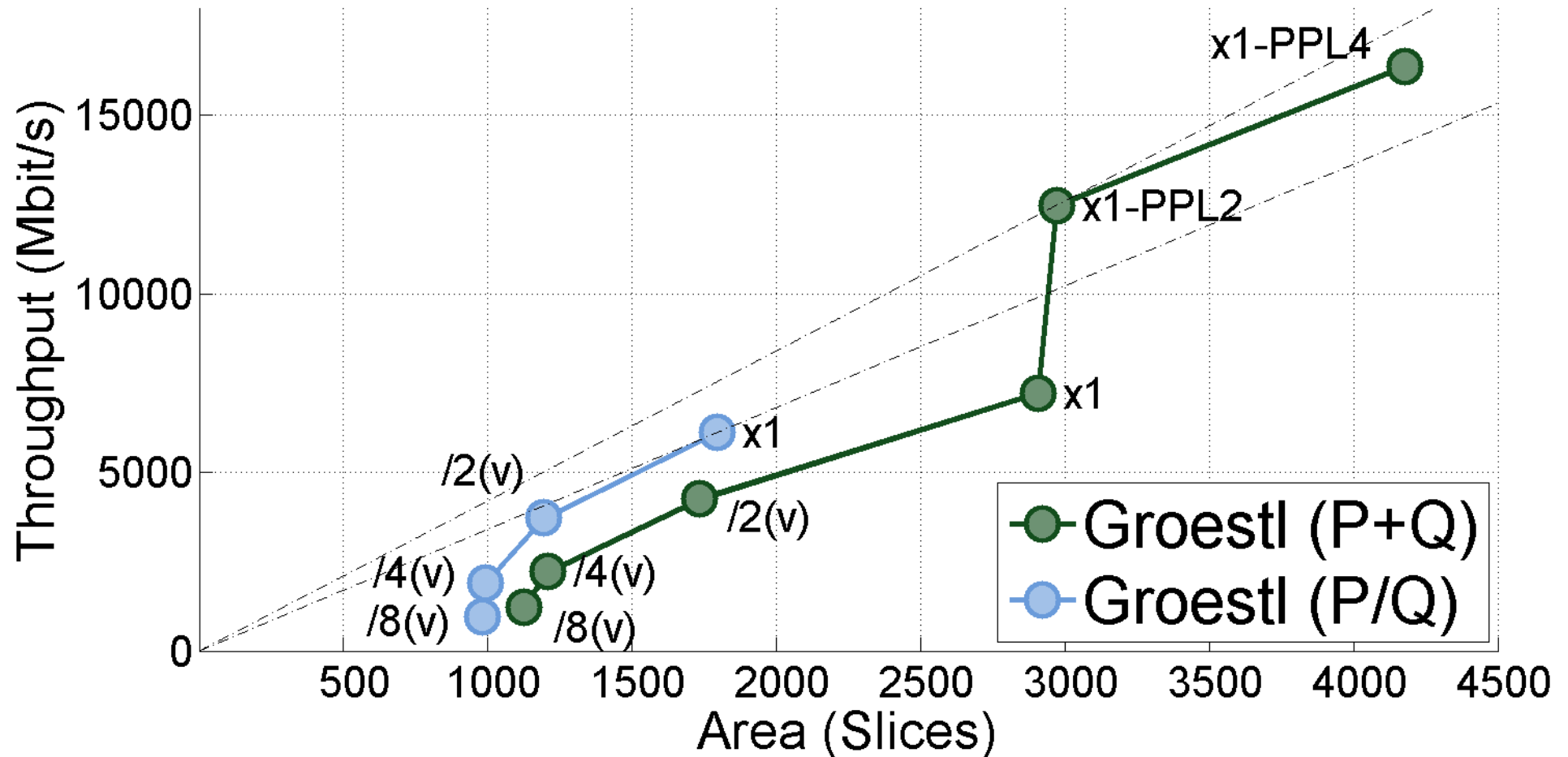


Results for Altera & Xilinx FPGAs

BLAKE-256 in Virtex 5



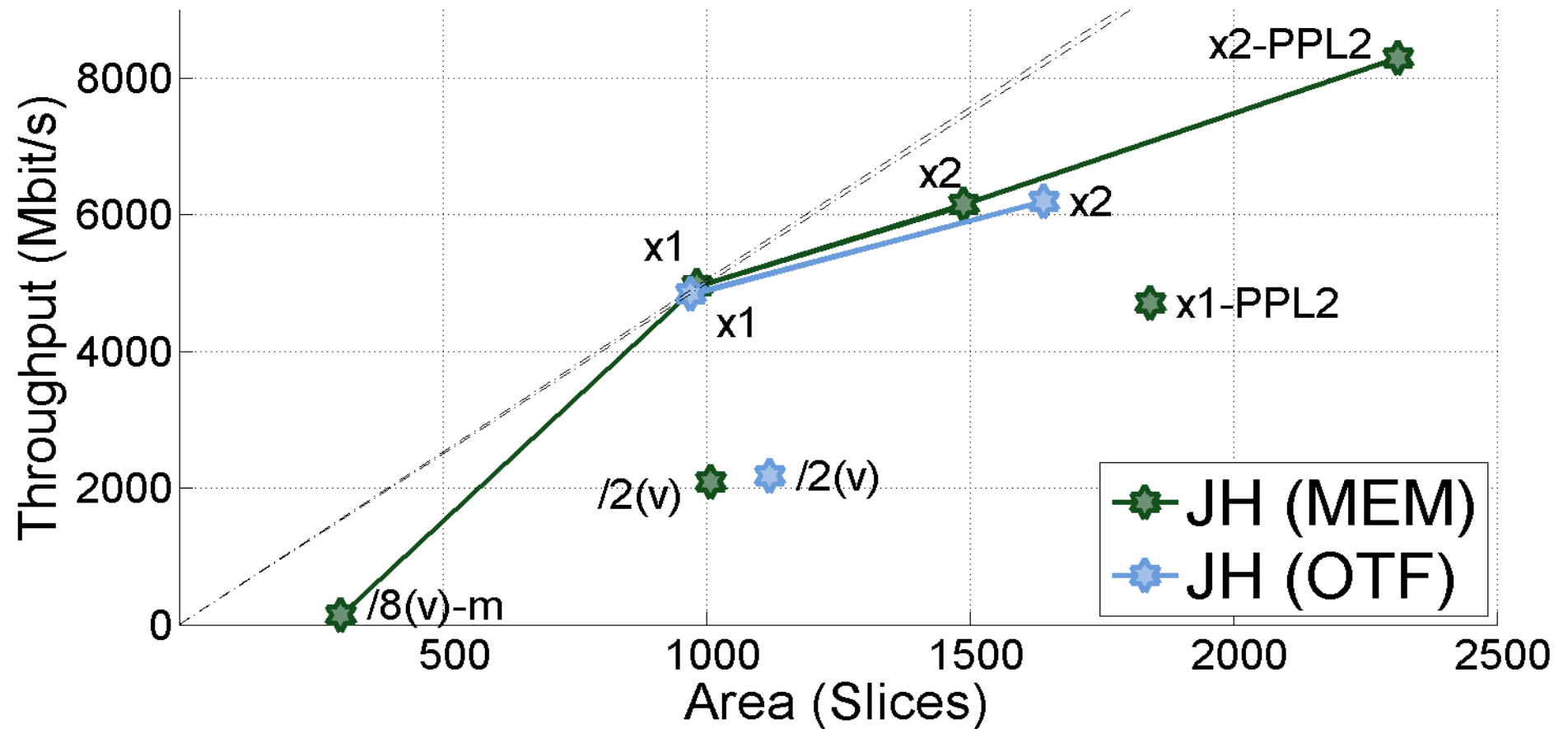
Groestl-256 in Virtex 5



Groestl P+Q – parallel architecture; two independent units for P and Q

Groestl P/Q – quasi-pipelined architecture; one unit shared between P and Q

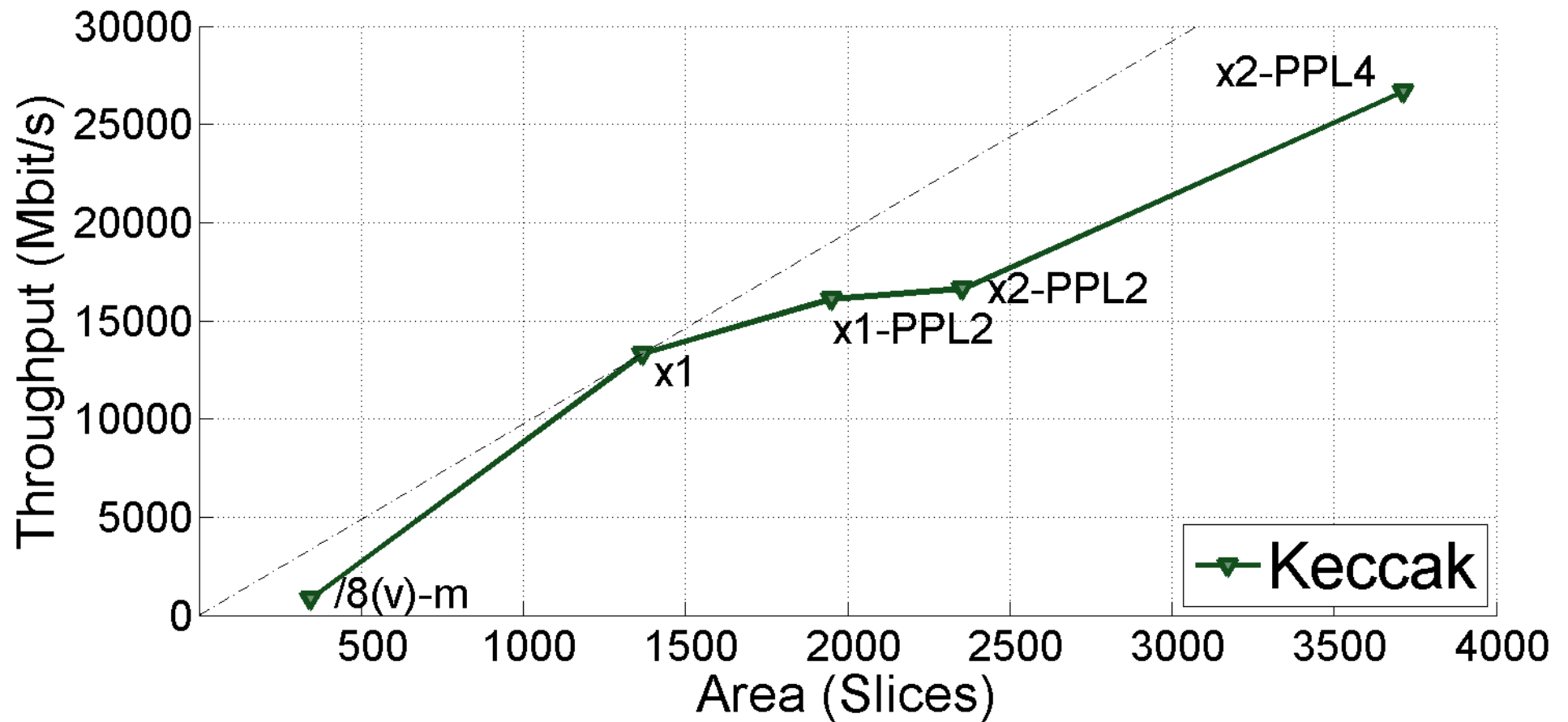
JH-256 in Virtex 5



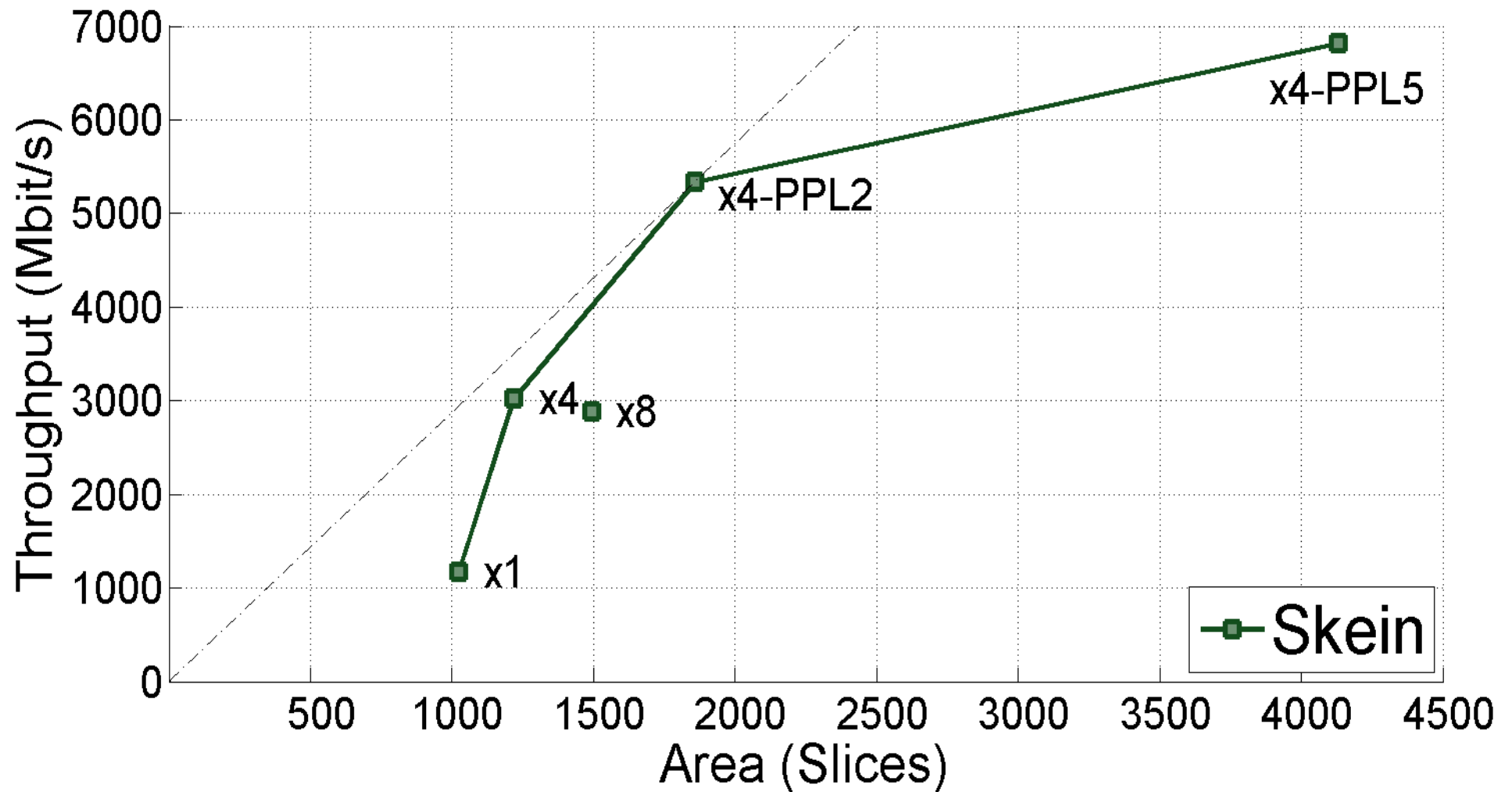
JH MEM – round constants stored in memory

JH OTF – round constants computed on-the-fly

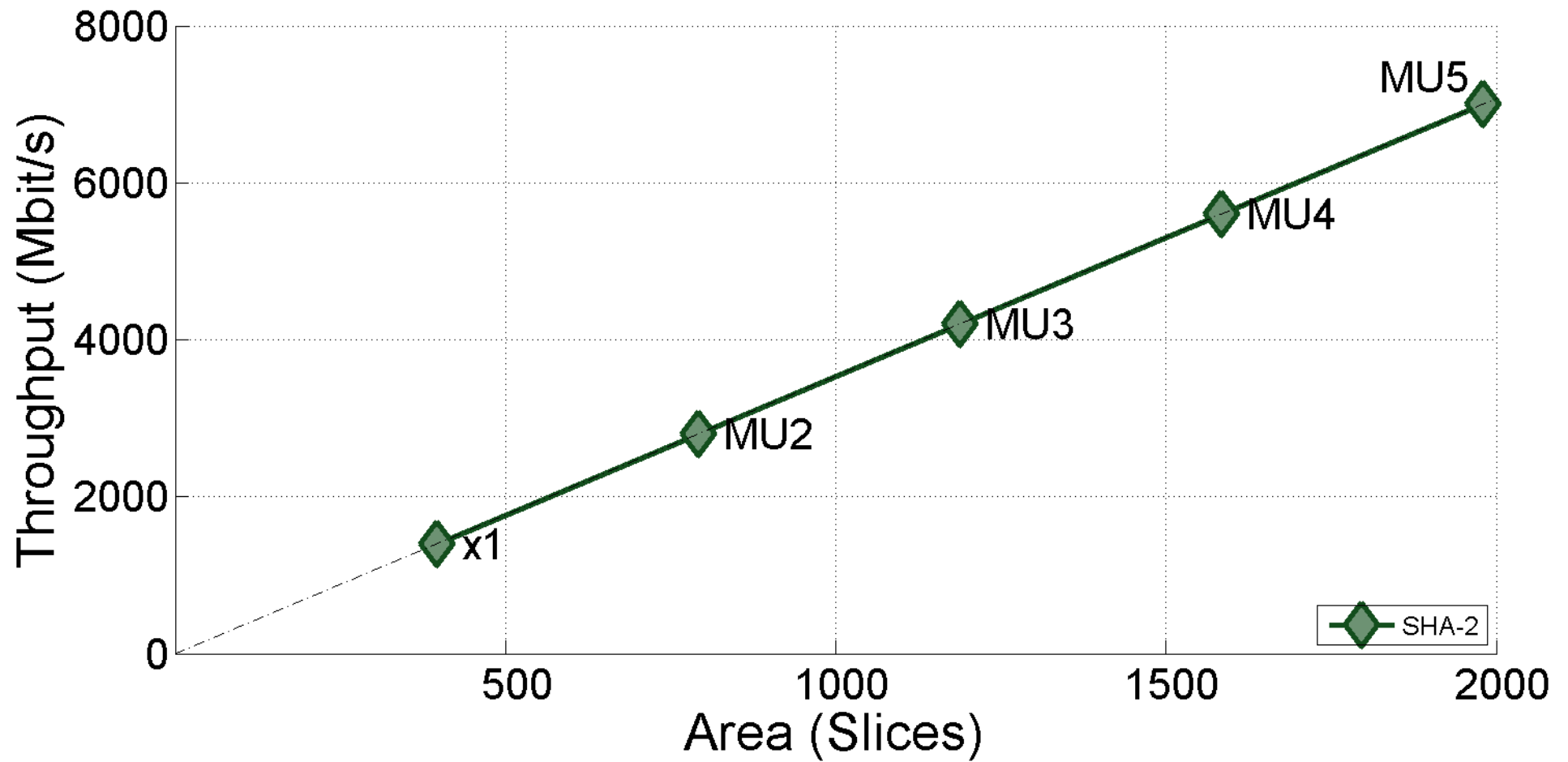
Keccak-256 in Virtex 5



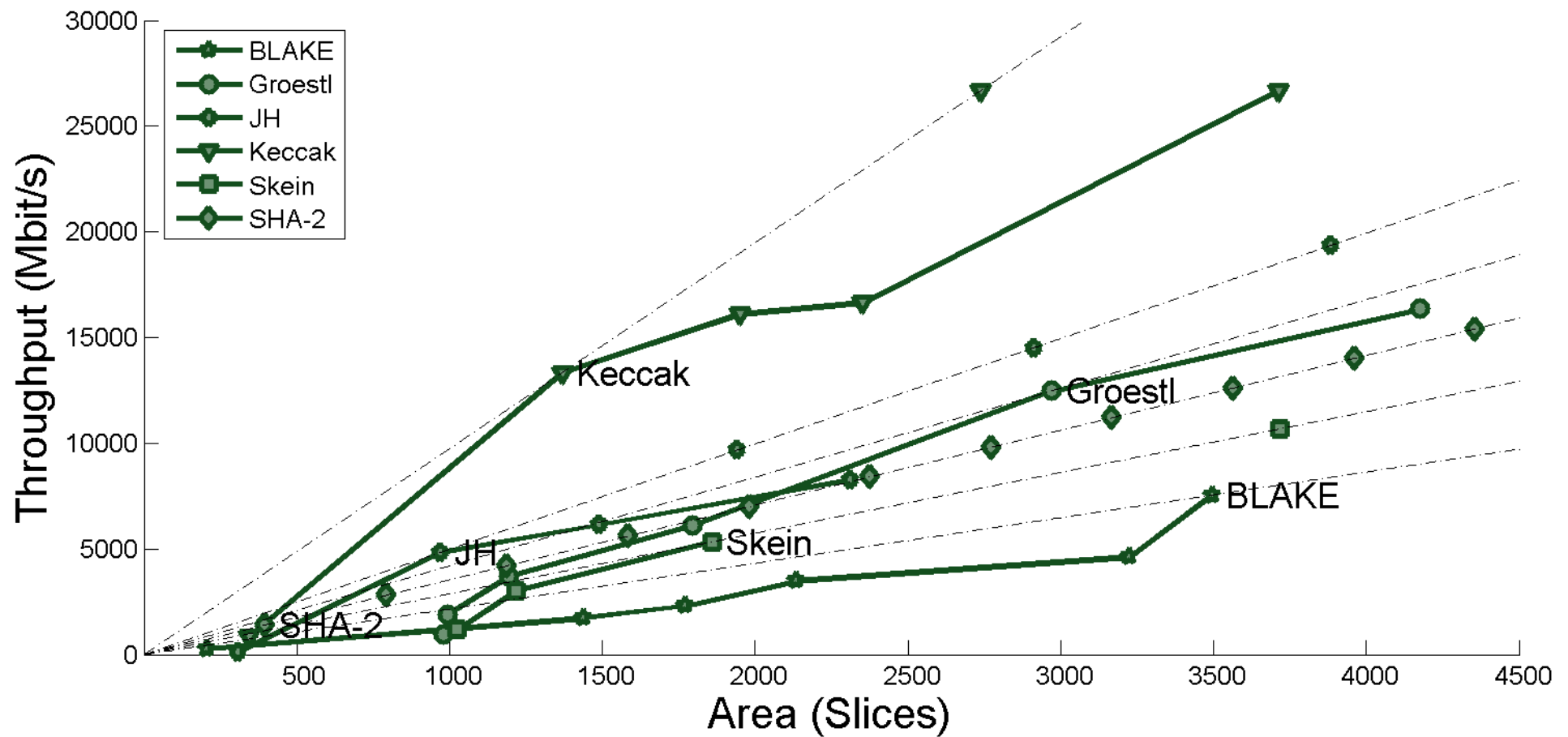
Skein-256 in Virtex 5



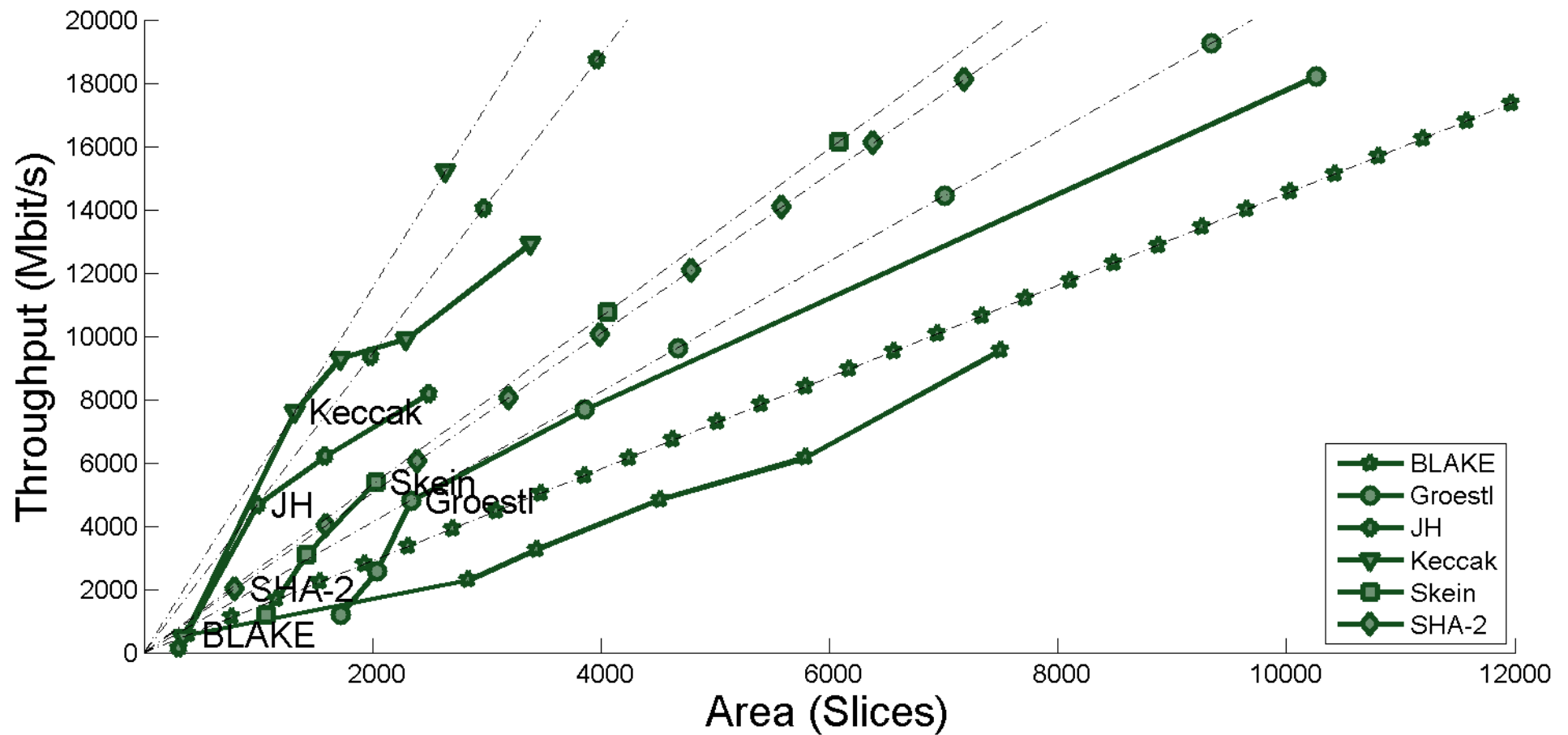
SHA-256 in Virtex 5



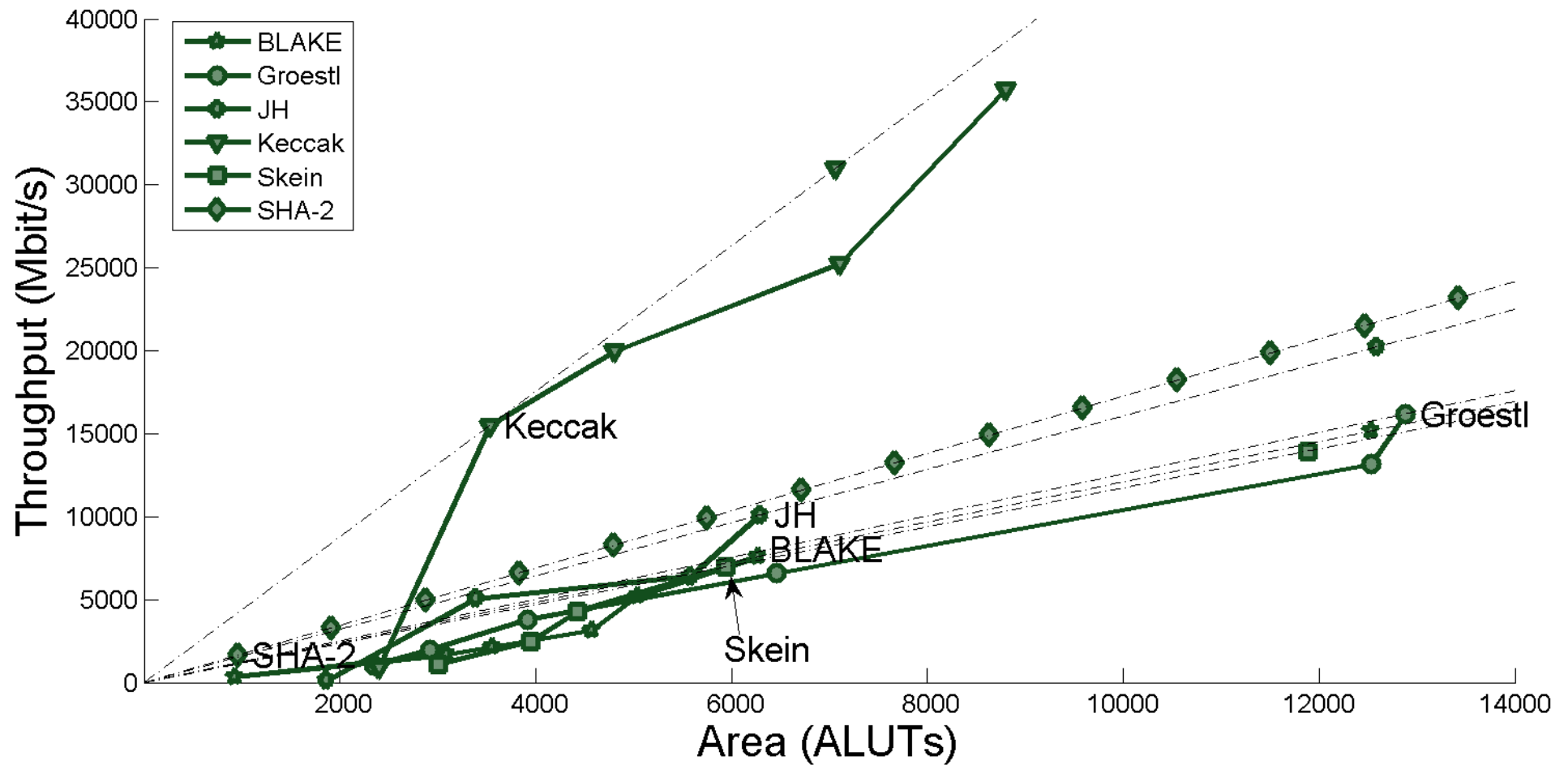
256-bit variants in Virtex 5



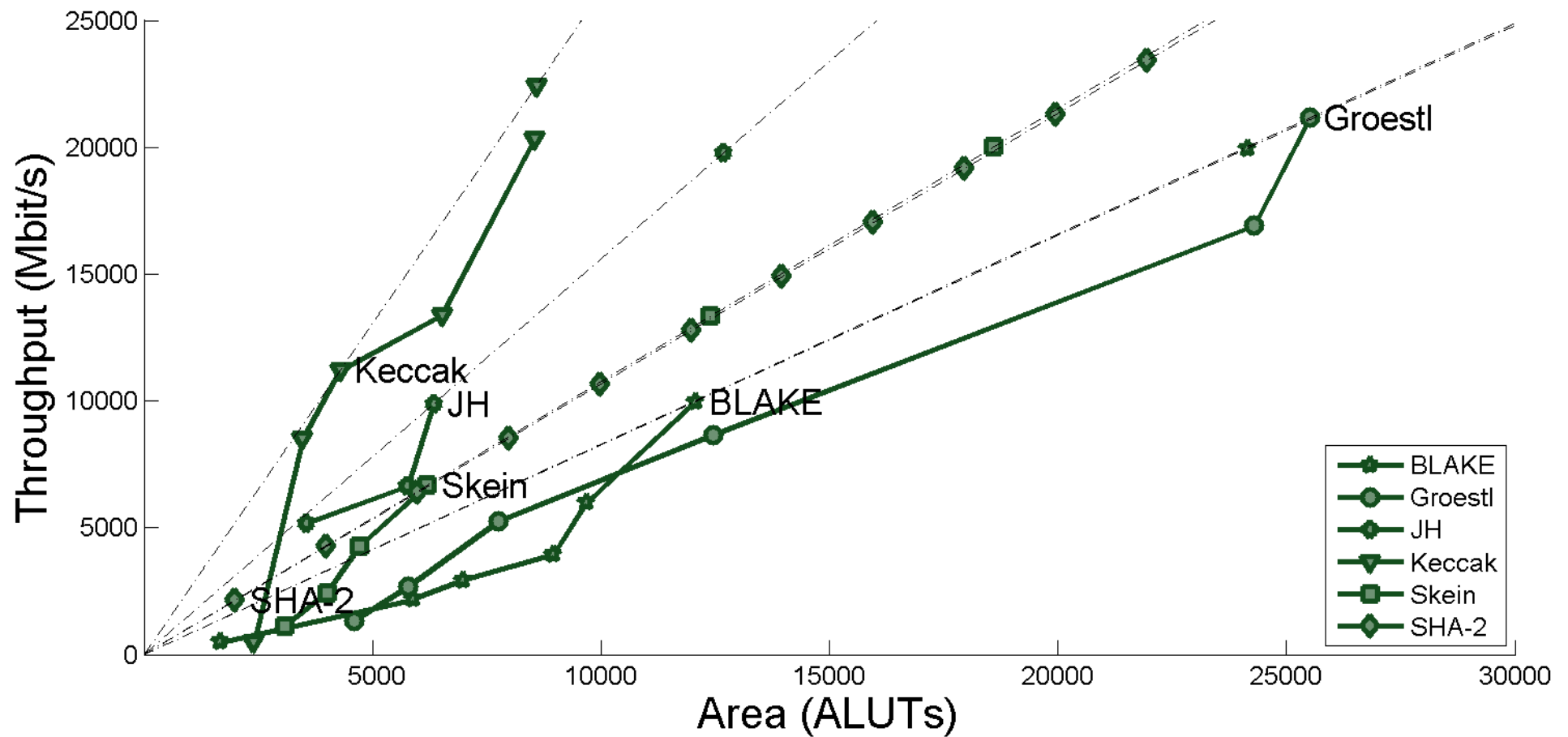
512-bit variants in Virtex 5



256-bit variants in Stratix III



512-bit variants in Stratix III



Flexibility of SHA-3 Finalists

Algorithm	Iterative	Folded			Pipelined			Efficient Unrolled
		Horizontally	Vertically	Mixed	Unrolled	Basic	Folded	
BLAKE	x1	/2(h), /4(h)		/4(h)/4(v)- m [*]		x1- PPL2, x1- PPL4	/2(h)- PPL2, /2(h)- PPL4	
Groestl	x1 [*]		/2(v), /4(v), /8(v)			x1- PPL2, x1- PPL7		
JH	x1 [*]		/2(v)	/8(v)-m	x2-PPL2			
Keccak	x1 [*]			/8(v)-m		x1- PPL2		
Skein	x1				x4- PPL2, x4-PPL5			x4 [*]

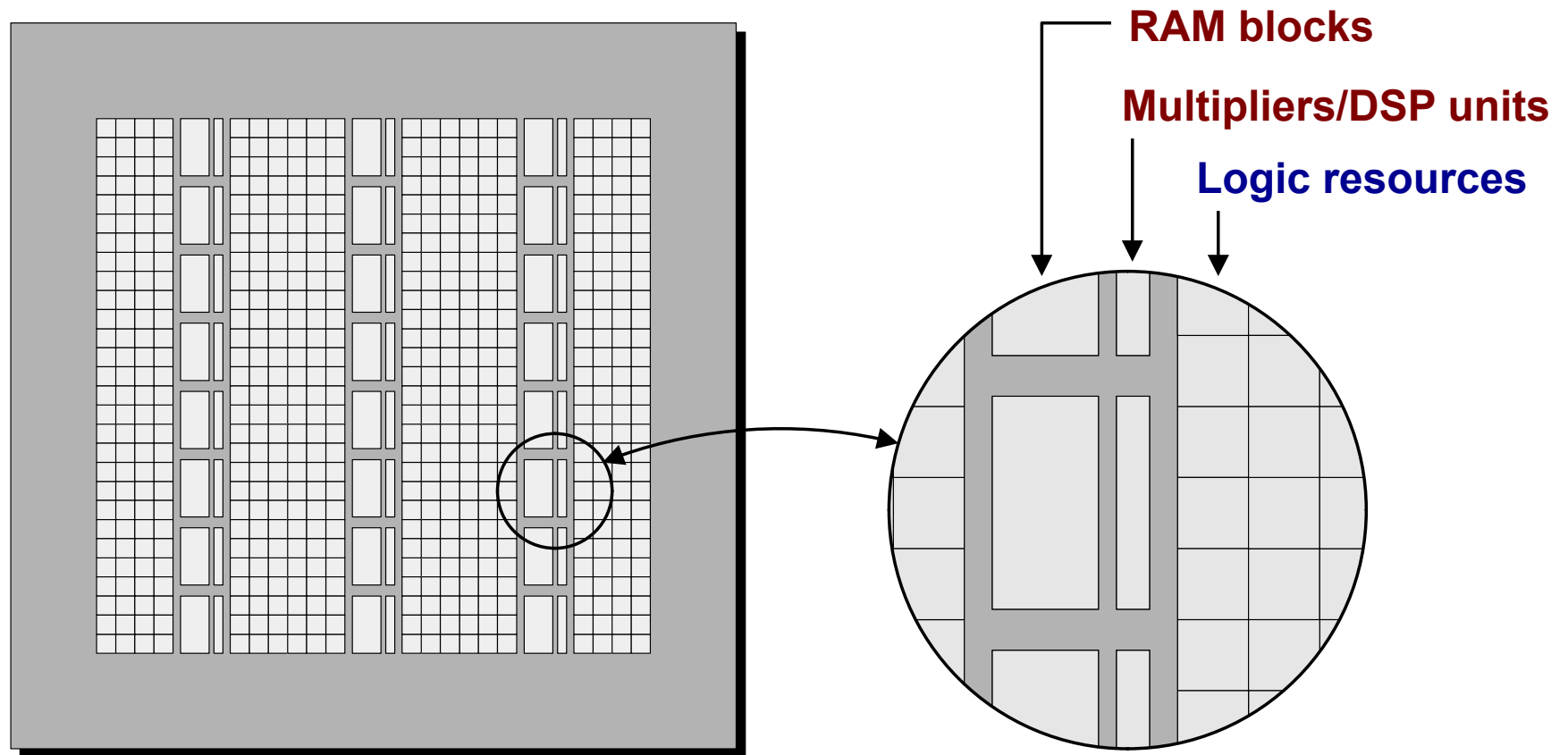
ARCH_SYMBOL* - the best non-pipelined architecture

BLAKE – most flexible, Keccak, JH – least flexible



Architectures Based on Embedded Resources

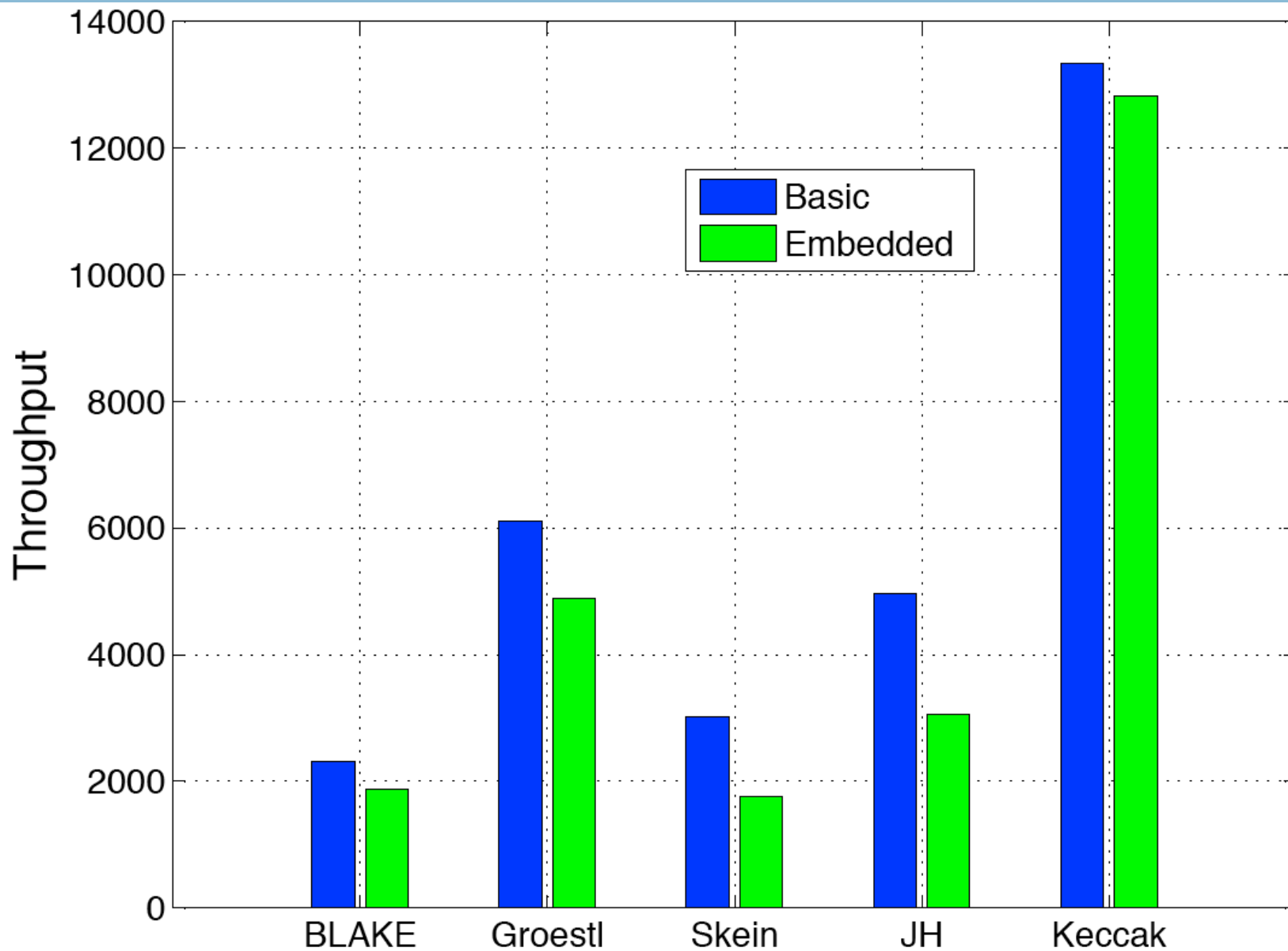
Implementations Based on the Use of Embedded Resources in FPGAs



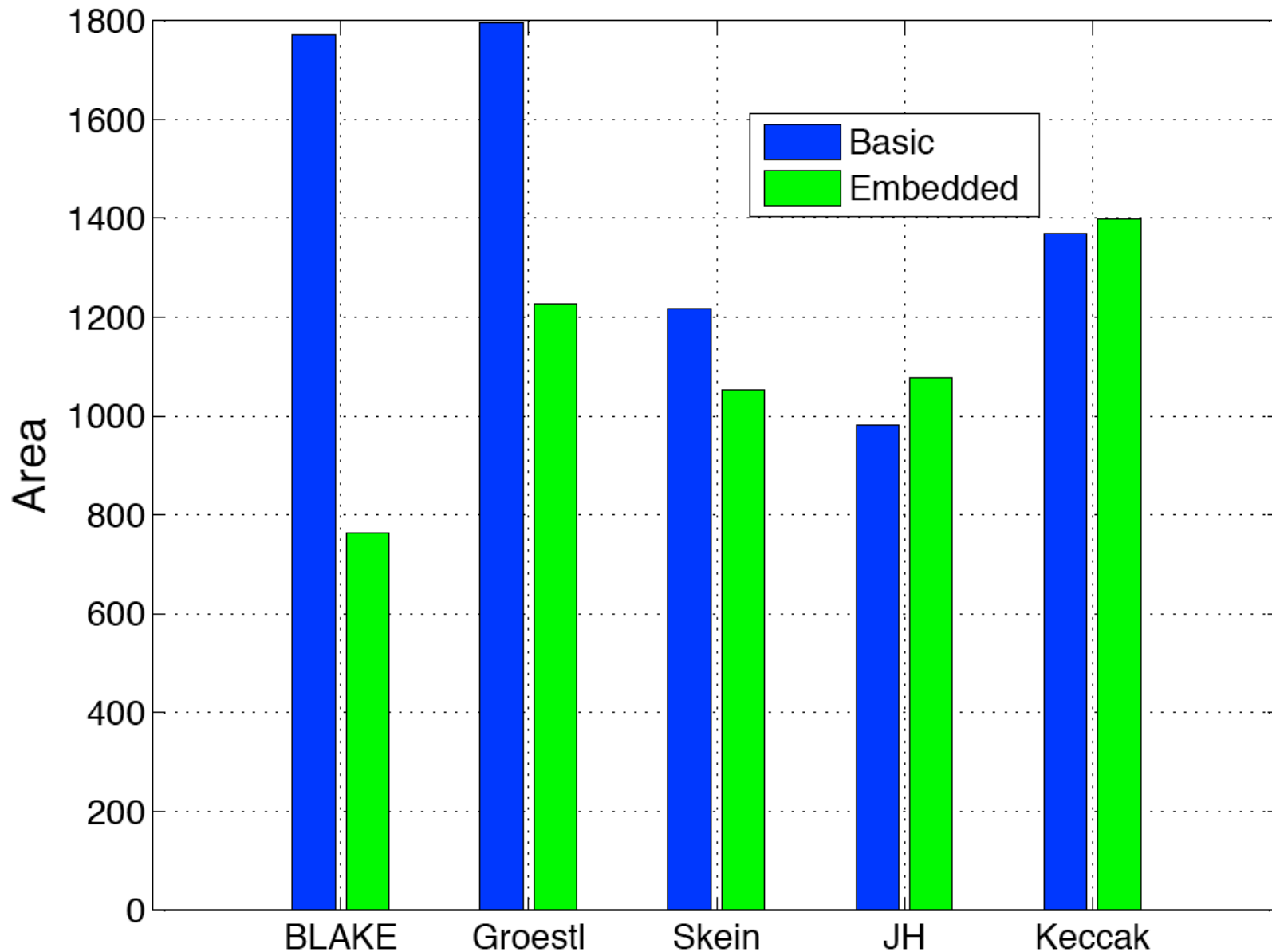
(#Logic resources, #Multipliers/DSP units, #RAM_blocks)

Throughput

Best Non-pipelined Architectures in Virtex 5

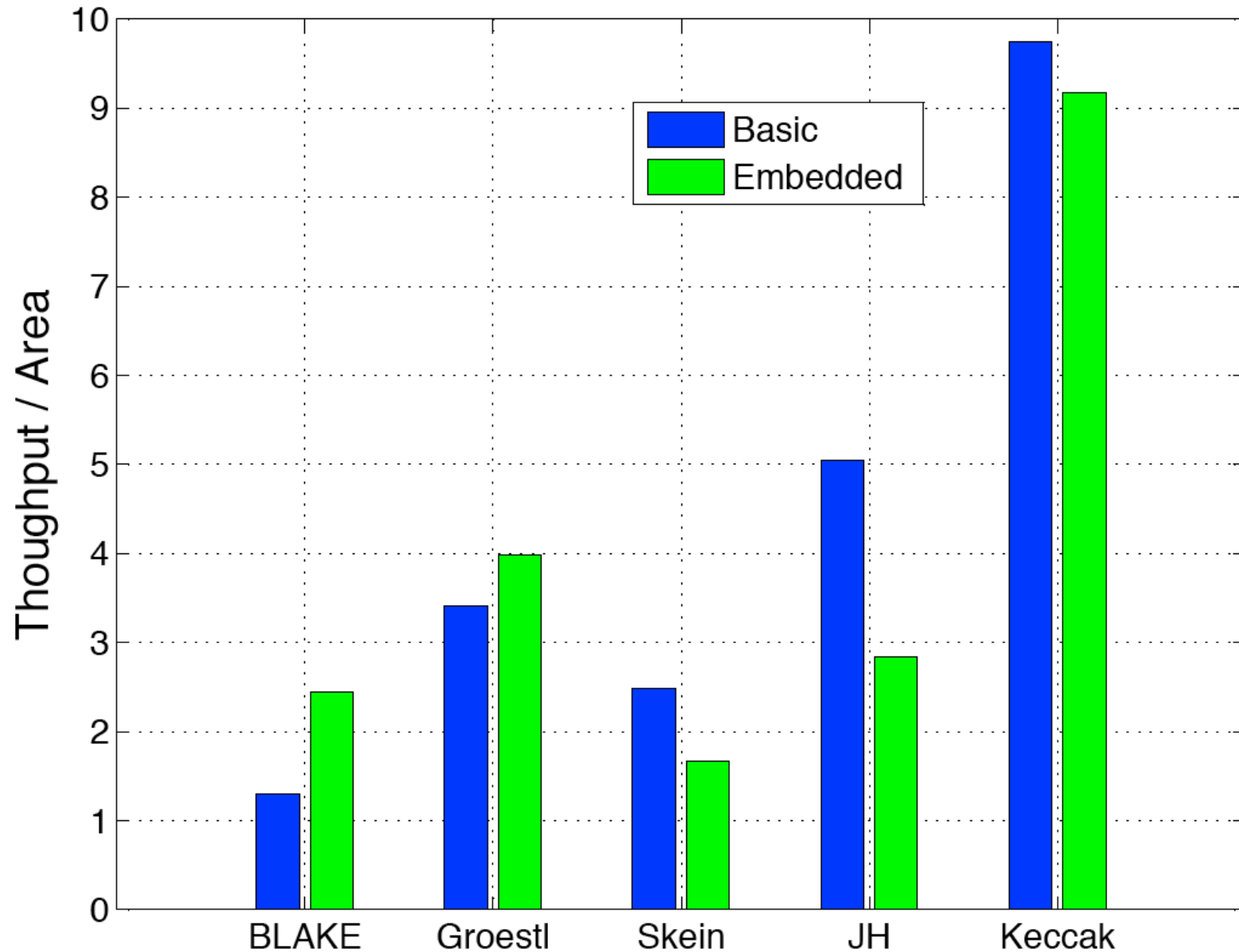


Logic Resources: Best Non-pipelined Architectures in Virtex 5




Throughput / #Logic Resources

Best Non-pipelined Architectures in Virtex 5



Architectures with Embedded Resources - Summary

- No or marginal improvement in Throughput.
- Significant savings in the amount of Logic Resources obtained for functions based on large look-up tables: **BLAKE and Groestl**
- Improvement in the Throughput to #Logic Resources ratio for **BLAKE and Groestl**
- No change in ranking based on the Throughput/#Logic Resources ratio
- Limited advantage of using DSP units

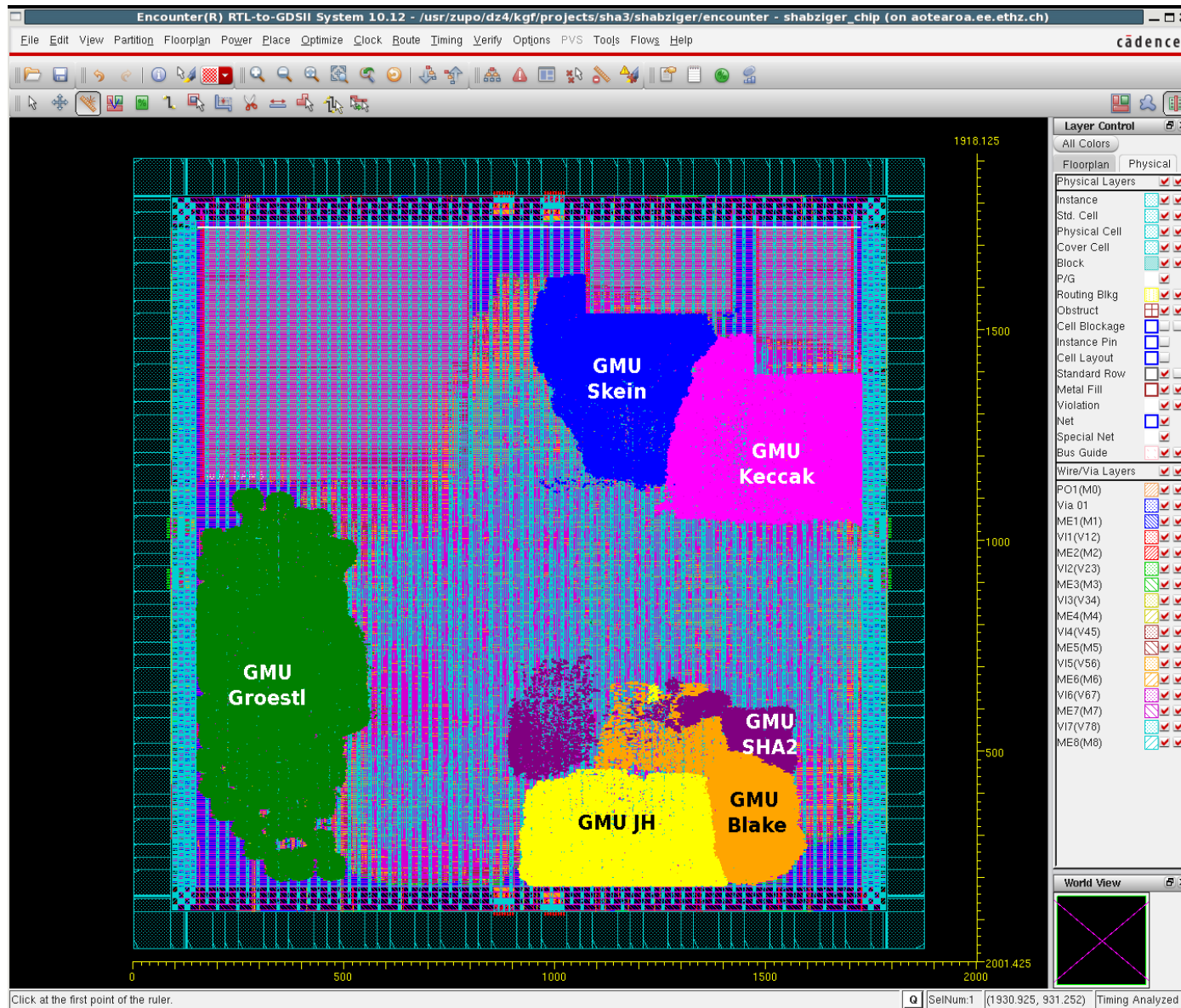


Correlation Between FPGA Results and ASIC Results

Assumptions

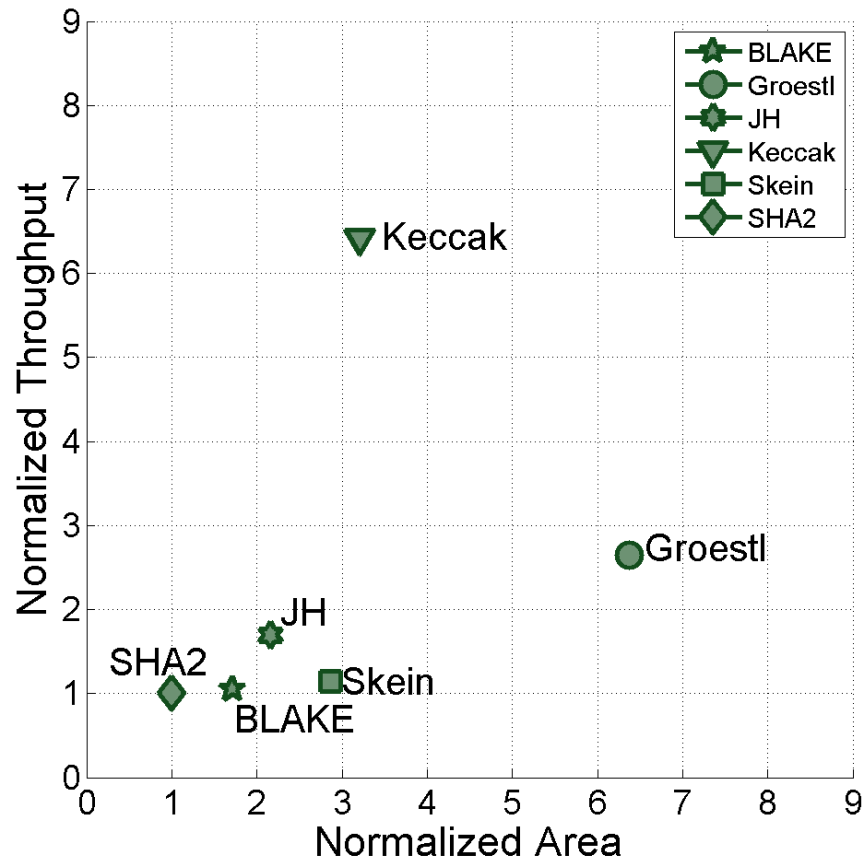
- **ASIC Chip developed in collaboration with ETHZ Zurich, including**
 - **6 GMU Cores optimized for the maximum Throughput/Area ratio for single-message (non-pipelined) architectures**
- **256-bit variants of algorithms**
- **No padding units**
- **Wide infinite bandwidth input/output interface**
- **standard-cell CMOS 65nm UMC ASIC technology (UMC65LL) offered through Europractice MPW services**
- **65nm technology used to manufacture our ASIC and Altera Stratix III FPGAs**

Layout of the GMU Cores

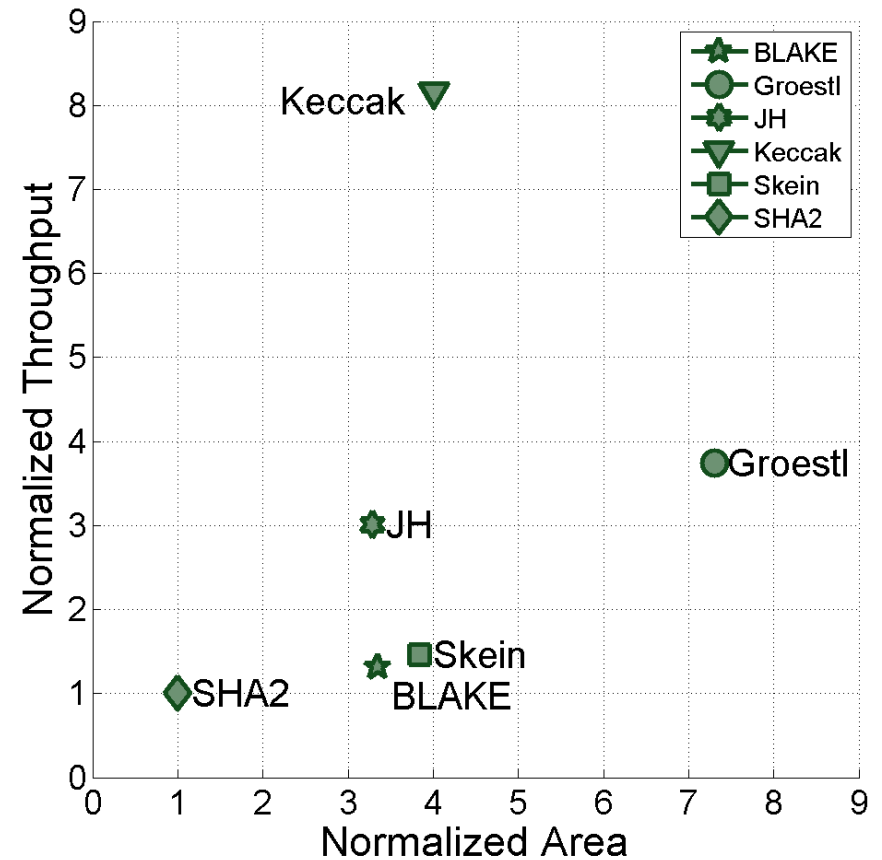


Correlation Between ASIC Results and FPGA Results

ASIC

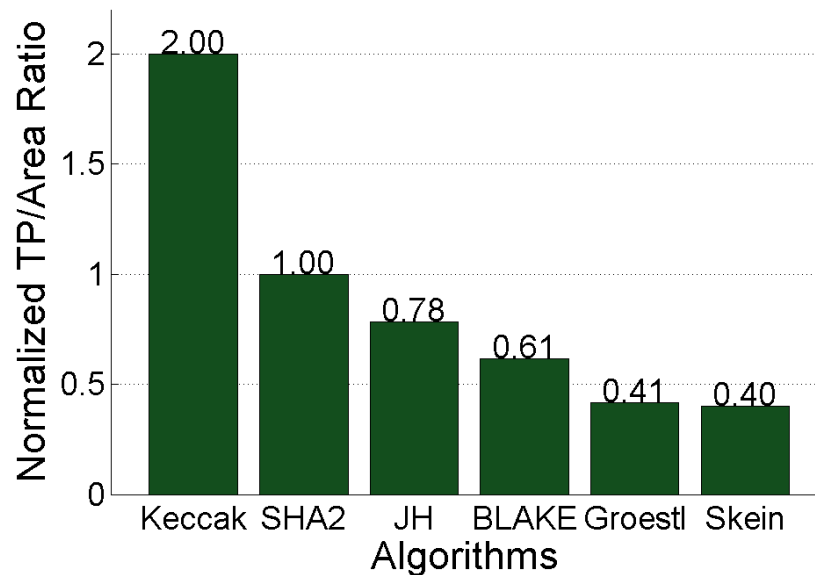


Stratix III FPGA

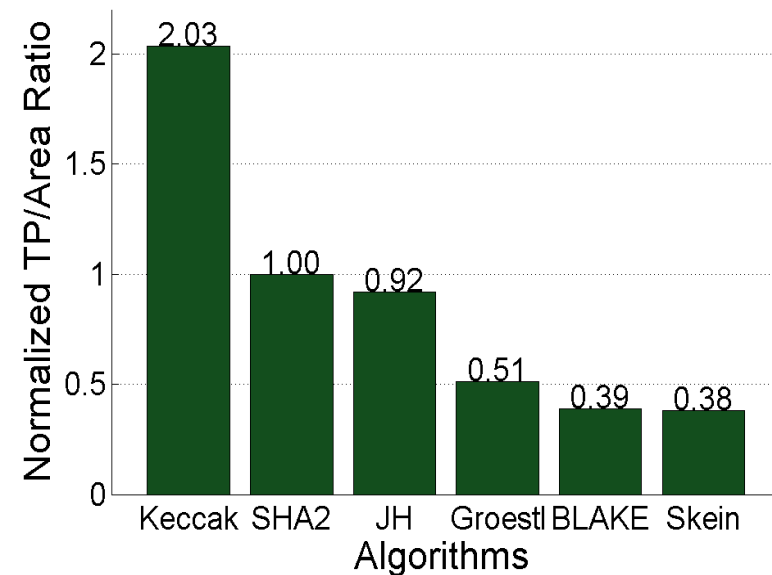


Correlation Between ASIC Results and FPGA Results

ASIC



Stratix III FPGA





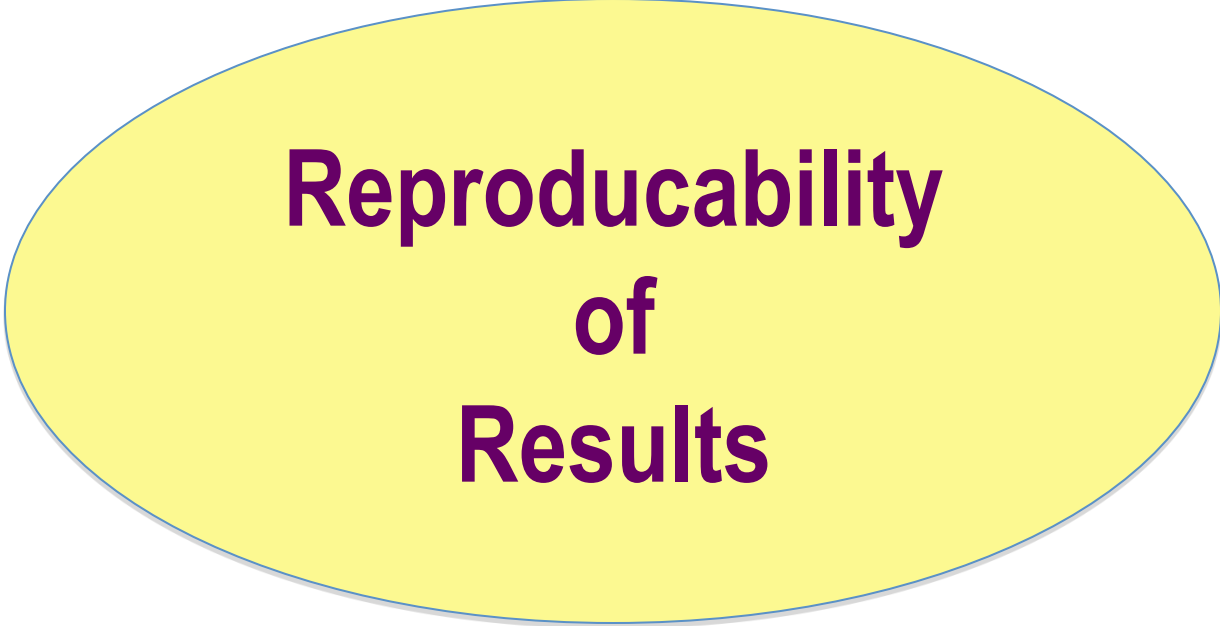
Inherent Features of all SHA-3 Finalists

Summary

- Keccak** – consistently outperforms SHA-2; front runner for high-speed implementations, but not very suitable for folding
- JH** – performs better than SHA-2 most of the time, not very suitable for folding or inner-round pipelining
- Groestl** – better than SHA-2 for only one out of four FPGA families, and only with relatively large area; suitable for vertical folding
- Skein** – the only candidate benefiting from unrolling; easy to pipeline after unrolling
- BLAKE** – most flexible; can be folded horizontally and vertically, can be effectively pipelined, however relatively slow compared to other candidates.

Conclusions

- Using multiple architectures provides a more comprehensive view of the algorithms
- Algorithms differ substantially in terms of their flexibility and suitability for folding, unrolling, and pipelining
- Optimum architecture (including an optimum number of pipeline stages) may depend on FPGA family
- **Two front-runners:** **Keccak, JH**

A large, horizontally-oriented yellow oval with a thin blue border, centered on the slide.

Reproducibility of Results

GMU Source Codes and Block Diagrams

GMU Source Codes for

all Round 3 SHA-3 Candidates & SHA-2

made available at the ATHENa website at:

<http://cryptography.gmu.edu/athena>

**Majority of codes accompanied by
hierarchical block diagrams.**

Details of Results and Replication Scripts

- Currently available in the **ATHENa database** at
<http://cryptography.gmu.edu/athena>
600+ optimized results
for
16 hash functions
50+ designs
11 FPGA families
- Scripts and configuration files sufficient to easily reproduce all results (without repeating optimizations)
- Automatically created by ATHENa and stored in ATHENa Database

A stylized illustration of a woman in a green and gold dress, holding a torch and a shield, standing against a large green circle. The woman is depicted in a classic, somewhat Art Deco style. She wears a long, flowing green dress with gold trim and a gold belt. She holds a torch in her right hand and a shield in her left. The shield is green with gold patterns. The background is a large, light green circle. The overall style is reminiscent of early 20th-century graphic design.

Show Help

<div><div>About</div><div>All Results</div><div>Compare Selected Results</div><div>Login</div></div>	Group	Algorithm	Design		Platform	Timing		Resource Utilization	
	Result ID	Algorithm Enable Unique	Hash Size [bits]	Primary Opt Target	Datapath Width [bits]	Family	Impl Freq [MHz]	TP [Mbits/s]	CLB Slices
	1127	BLAKE	512	Throughput/Area	1,024	Cyclone II	40.620	1,260	-
	1126	BLAKE	512	Throughput/Area	1,024	Cyclone III	48.070	1,492	-
	1125	BLAKE	512	Throughput/Area	1,024	Stratix II	71.910	2,231	-
	1124	BLAKE	512	Throughput/Area	1,024	Cyclone IV	48.270	1,498	-
	1123	BLAKE	512	Throughput/Area	1,024	Stratix III	92.990	2,885	-
	1122	BLAKE	512	Throughput/Area	1,024	Stratix IV GX	106.510	3,305	-
	1121	Groestl	512	Throughput/Area	1,024	Virtex 4	165.673	5,850	15,930
	1120	Groestl	512	Throughput/Area	1,024	Virtex 5	197.083	6,959	3,576
	1119	Groestl	512	Throughput/Area	1,024	Spartan 3	79.195	2,796	15,862
	1118	Groestl	512	Throughput/Area	1,024	Virtex 6	244.320	8,627	3,652
	1117	Groestl	512	Throughput/Area	1,024	Spartan 6	126.711	4,474	4,190
	1116	Groestl	256	Throughput/Area	512	Spartan 3	94.616	2,307	8,094
	1115	Groestl	256	Throughput/Area	512	Virtex 5	249.501	6,083	1,852
	1114	Groestl	256	Throughput/Area	512	Virtex 4	174.338	4,251	8,053
	1113	Groestl	256	Throughput/Area	512	Virtex 6	204.834	4,994	1,616
	1112	Groestl	256	Throughput/Area	512	Spartan 6	124.440	3,034	1,657
	1111	Keccak	512	Throughput/Area	1,600	Spartan 3	114.639	2,751	3,012
	1110	Keccak	512	Throughput/Area	1,600	Virtex 5	281.057	6,745	1,153
	1109	Keccak	512	Throughput/Area	1,600	Virtex 4	230.681	5,536	2,982
	1108	Keccak	512	Throughput/Area	1,600	Virtex 6	293.686	7,048	1,071
	1107	Keccak	512	Throughput/Area	1,600	Spartan 6	144.613	3,471	1,250
	1106	Keccak	256	Throughput/Area	1,600	Spartan 3	109.625	4,970	3,369
	1105	Keccak	256	Throughput/Area	1,600	Virtex 5	280.978	12,738	1,241
	1104	Keccak	256	Throughput/Area	1,600	Virtex 4	220.751	10,007	3,453
	1103	Keccak	256	Throughput/Area	1,600	Virtex 6	285.225	12,930	1,201

Result ID	Algorithm	Hash Size [bits]	Primary Opt Target	Datapath Width [bits]	Family	Impl Freq [MHz]	TP [Mbits/s]	CLB Slices	LE
-----------	-----------	------------------	--------------------	-----------------------	--------	-----------------	--------------	------------	----

First Previous 1 2 3 4 5 Next Last

45

Generation of Results Facilitated by ATHENa

ATHENa – Automated Tool for Hardware Evaluation
Benchmarking tool developed at GMU since 2009



- batch mode of FPGA tools



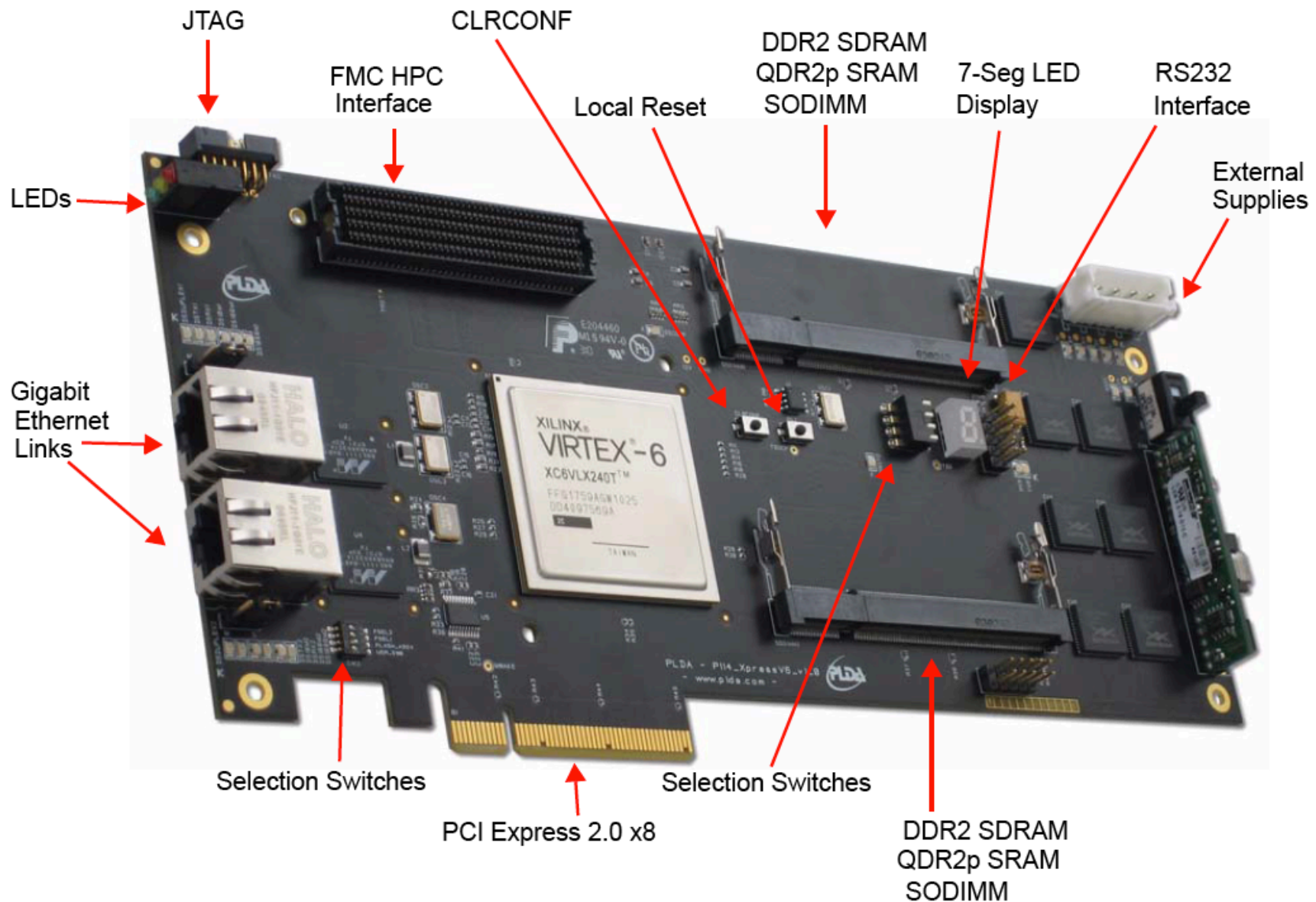
VS.



- ease of extraction and tabulation of results (Excel, CSV)
- optimized choice of tool options

Future Work

Experimental Testing using PCI Express Boards



Thank you!

Questions?



Questions?

CERG: <http://cryptography.gmu.edu>

ATHENa: <http://cryptography.gmu.edu/athena>