Design Trade-offs in the Implementations of 14 Round 2 SHA-3 Candidates using Embedded Resources of Altera and Xilinx FPGAs

Marcin Rogawski, Malik Umar Sharif,
Rabia Shahid and Kris Gaj

George Mason University, USA

Co-authors

Outline

- SHA-3 competition and benchmarking process
- Earlier results for high-speed implementations
- Methodology for using embedded resources of FPGAs
- Embedded resources and their use in SHA-3 candidates
- Results
- Conclusions

SHA-3 competition

- **Software benchmarking:**
- General CPUs - eBASH http://bench.cr.yp.to/ebash.html (Daniel J. Bernstein & Tanja Lange)
- Microcontrollers – XBX http://xbx.das-labor.org/trac

(Christian Wenzel-Benner and Jens Gräf)

- **Hardware benchmarking:** SHA-3 ZOO and ATHENaDB
- ASICs: ETH (Henzen et al.), GUT (Tillich et al.) NIICT (Matsuo et al.), VT (Guo et al.)
- FPGA Low Area: *GMU (Kaps et al.), UCL (Standaert et al.)*
- FPGA High Speed: GMU (Homsirikamol et al.), NIICT (Matsuo et al.), QUB (Baldwin et al.)
- FPGA High Speed (embedded resources) *GMU (This work)*

SHA-3 High Speed Architectures on Xilinx Virtex 5 (single stream of data)

Round 2: [SHA3 ZOO and ATHENaDB]

	Area	Bram	Throughput	Throughput/Area	Source
Blake	1623	0	3176	1.96	GMU
BMW	4350	0	8704	2.00	Matsuo et al.
BMW	5442	0	4482	0.82	GMU
Cubehash	663	0	3872	5.99	GMU
ECHO	4888	0	12094	2.47	GMU
Fugue	700	0	3414	4.88	GMU
Groestl-0	1722	N/A	10276	5.97	Gauravaram et al.
Groestl-0	1381	17	7552	5.46	Jungk et al.
Groestl-0	1597	0	7885	4.94	GMU
Hamsi	788	0	2997	3.85	GMU
JH	1056	0	5874	5.56	GMU
Keccak	1272	0	12817	10.08	GMU
Luffa	1023	0	9513	9.30	GMU
SHAvite-3	1104	0	3751	3.40	GMU
SIMD	8922	0	3121	0.35	GMU
Shabal	153	0	2051	13.41	Detrey et al.
Shabal	283	0	1719	6.08	GMU
Skein	1306	0	2565	1.96	GMU

Methodology

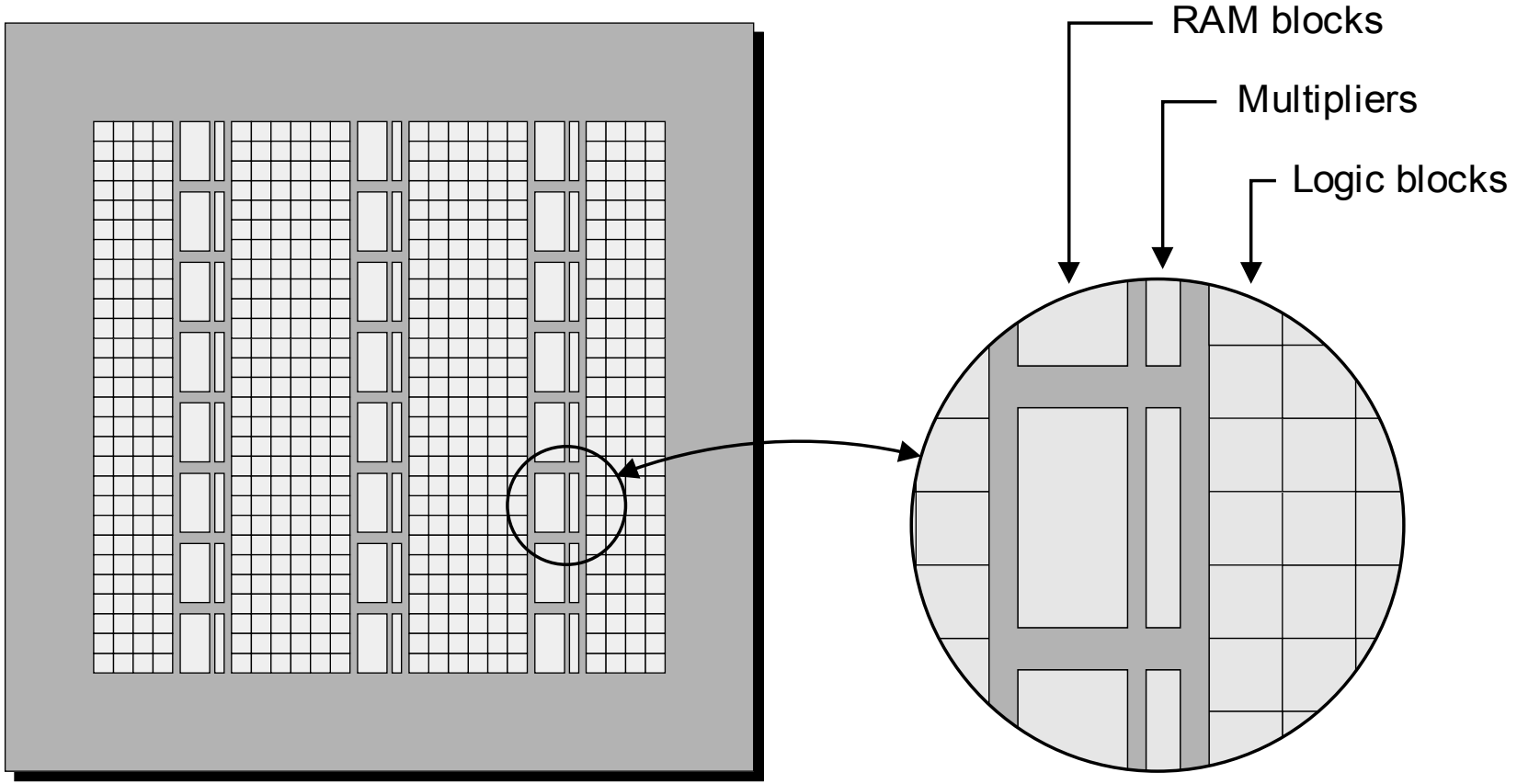
- Top level architectures from GMU basic designs
- Starting point: high-speed GMU designs optimized for the best throughput to area ratio http://eprint.iacr.org/2010/445
- Architectures modified, if needed, to support the use of embedded resources (e.g. round constants stored in memory vs. computed on the fly, T-box vs. S-box based AES units, etc.)
- Use of multiple FPGAs:

90nm low cost: Altera Cyclone II, Xilinx Spartan 3, and

65nm high performance: Altera Stratix III and Xilinx Virtex5

- Clear performance metrics
- Uniform and practical interface
- Uniform optimization criteria
- Use of ATHENa for generation, optimization and comparative analysis of results

RAM Blocks and Multipliers in Xilinx FPGAs



The Design Warrior's Guide to FPGAs
Devices, Tools, and Flows. ISBN 0750676043

Performance metrics

Vendor	Family	Resource Utilization Vector
Xilinx	Spartan 3	(#CLB_slices, #BRAMs, #multipliers)
	Virtex 5	(#CLB_slices, #BRAMs, #DSP48s)
Altera	Cyclone II	(#LEs, #Mem-bits, #multipliers)
	Stratix III	(#ALUTs, #Mem-bits, #DSP_18s)

$$Throughput = \frac{block\_size}{T \cdot (HTime(N+1) - HTime(N))}$$

T - clock period
N - message block number
Htime(N) - time for hashing N blocks of message

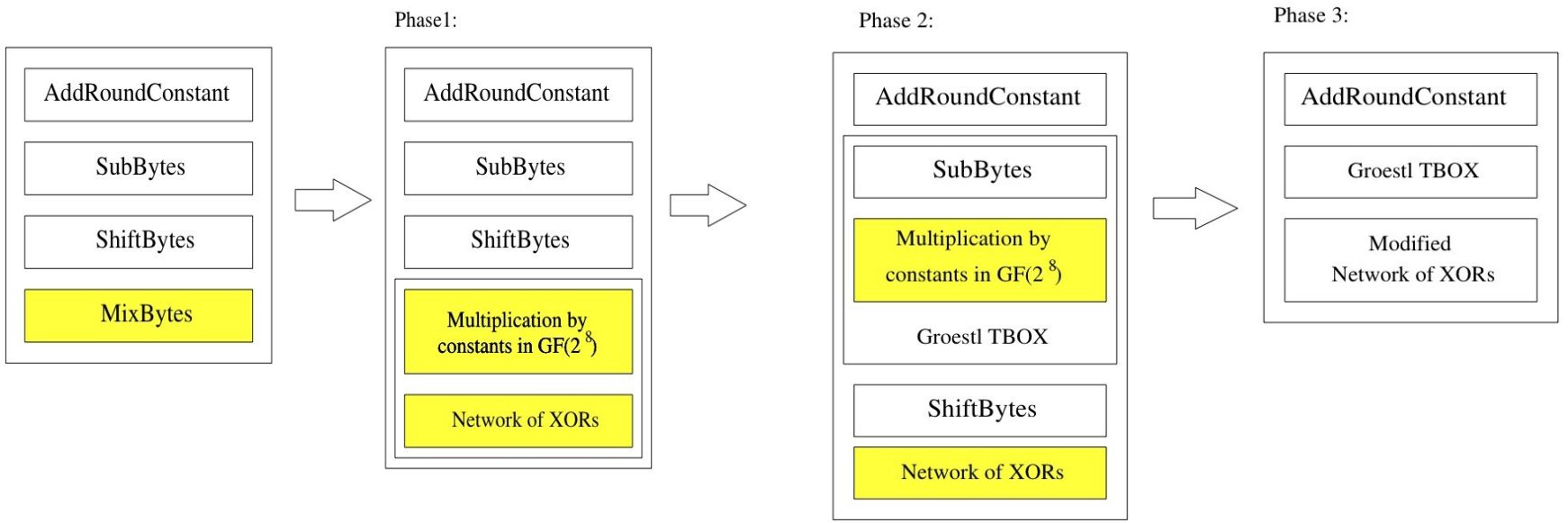
Basic operations of SHA-3 candidates and SHA-2

	S-box	GF Mul	MUL	mADD	ADD/SUB	Additional Memories
Blake				mADD3	ADD	Expansion tables
BMW				mADD17	ADD/SUB	
Cubehash					ADD	
ECHO	AES 8x8	x02, x03				
Fugue	AES 8x8	x04-x07				
Groestl	AES 8x8	x02-x07				
Hamsi						Expansion tables
JH	4x4	x02, x05				Round constants
Keccak						Round constants
Luffa						
SHAvite-3	AES 8x8	x02, x03				
SIMD			x185, x233	mADD3	ADD	
Shabal			x3, x5		ADD/SUB	
Skein					ADD-64	
SHA-2				mADD5	ADD	Round constants

Use of embedded resources to implement basic operations of SHA-3 candidates and SHA-2

	S-box	GF Mul	MUL	mADD	ADD/SUB	Additional Memories
Blake				DSP	DSP	BRAM
BMW				DSP	DSP	
Cubehash					DSP	
ECHO	BRAM	BRAM				
Fugue	BRAM	BRAM				
Groestl	BRAM	BRAM				
Hamsi						BRAM
JH	BRAM					BRAM
Keccak						BRAM
Luffa						
SHAvite-3	BRAM	BRAM				
SIMD			DSP	DSP	DSP	
Shabal			DSP		DSP	
Skein					DSP	
SHA-2				DSP	DSP	BRAM

T-box implementations (Groestl-0/Groestl example)



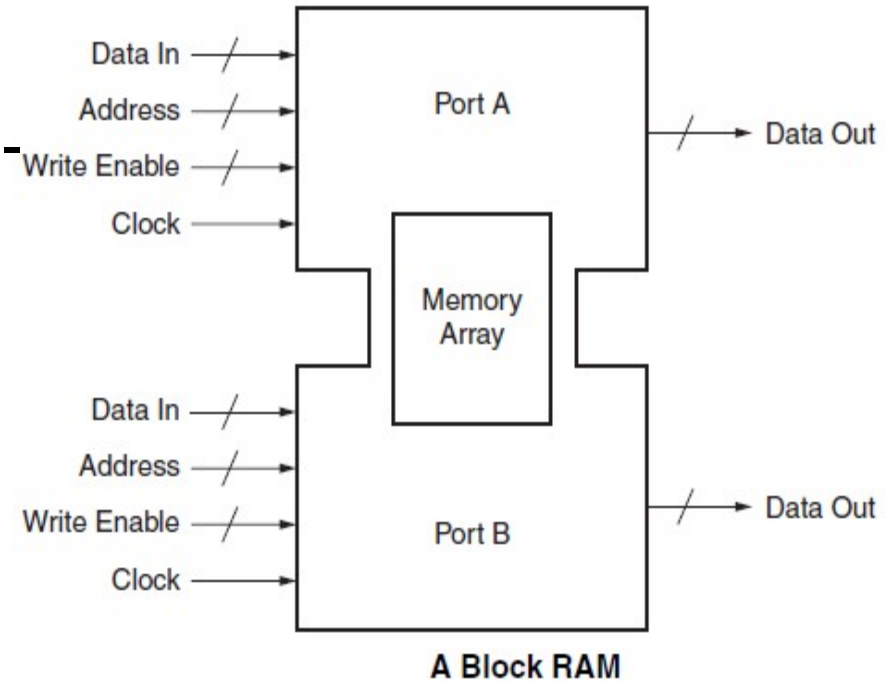
Groestl T-box: 256x40 bits, Fugue T-box: 256x24 and 256x32 bits,

ECHO and SHAvite-3 – AES T-boxes 256x32 bits

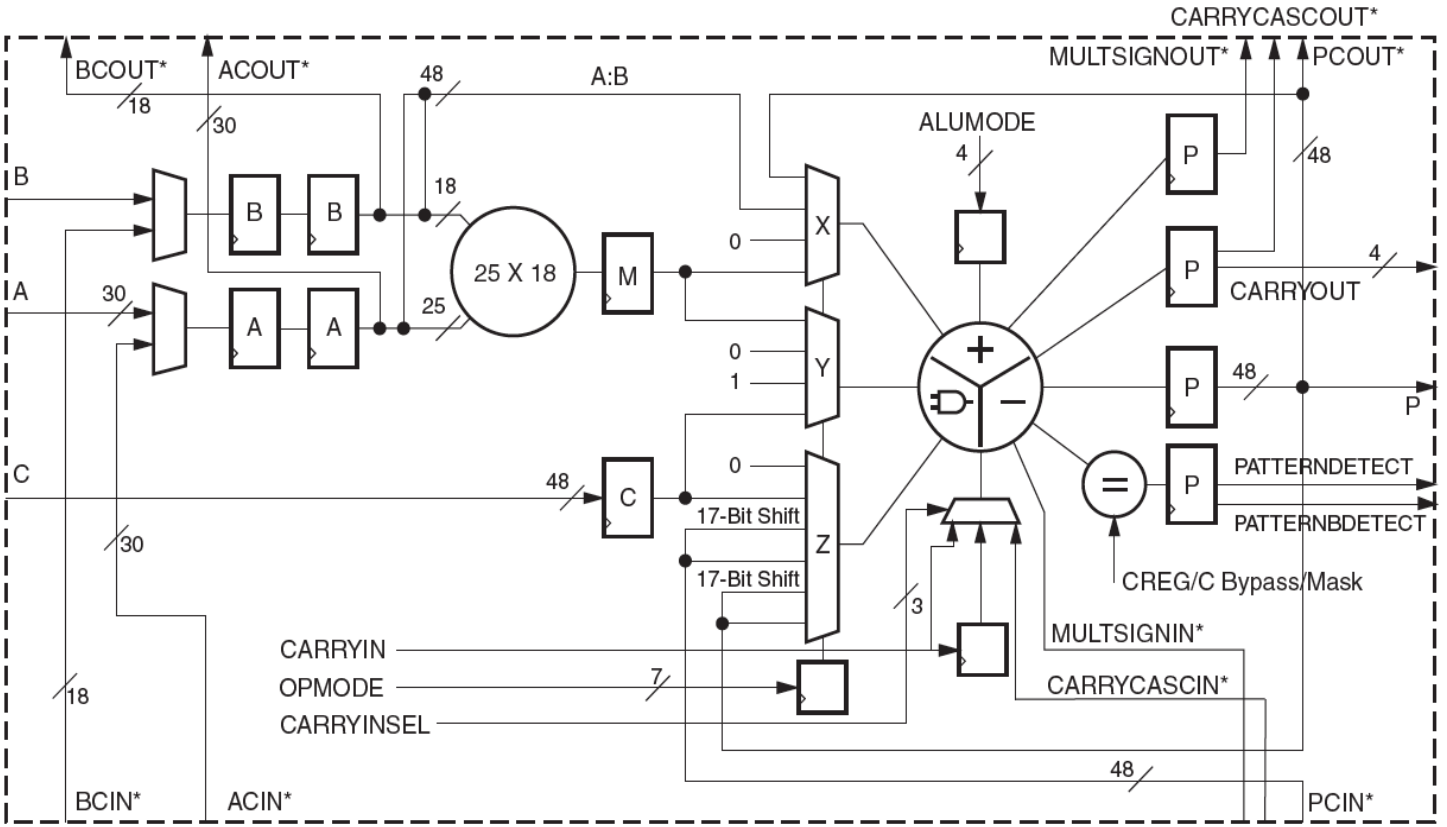
Block Memories

- Cyclone II (M4k), Stratix III (M9k, M144k), Spartan 3 (RAM18k), Virtex 5 (RAM36k)
- Aspect ratio (up to 32 bit words)
- 2xAES S-box/T-box: Spartan 3 BRAM - configured as dual port ROM (2kx8/512x32)
- 2xGroestl T-box: in 2xSpartan 3 BRAMs - configured as dual port ROM (2kx8 and 512x32)

Xilinx Virtex 5 - RAM36k



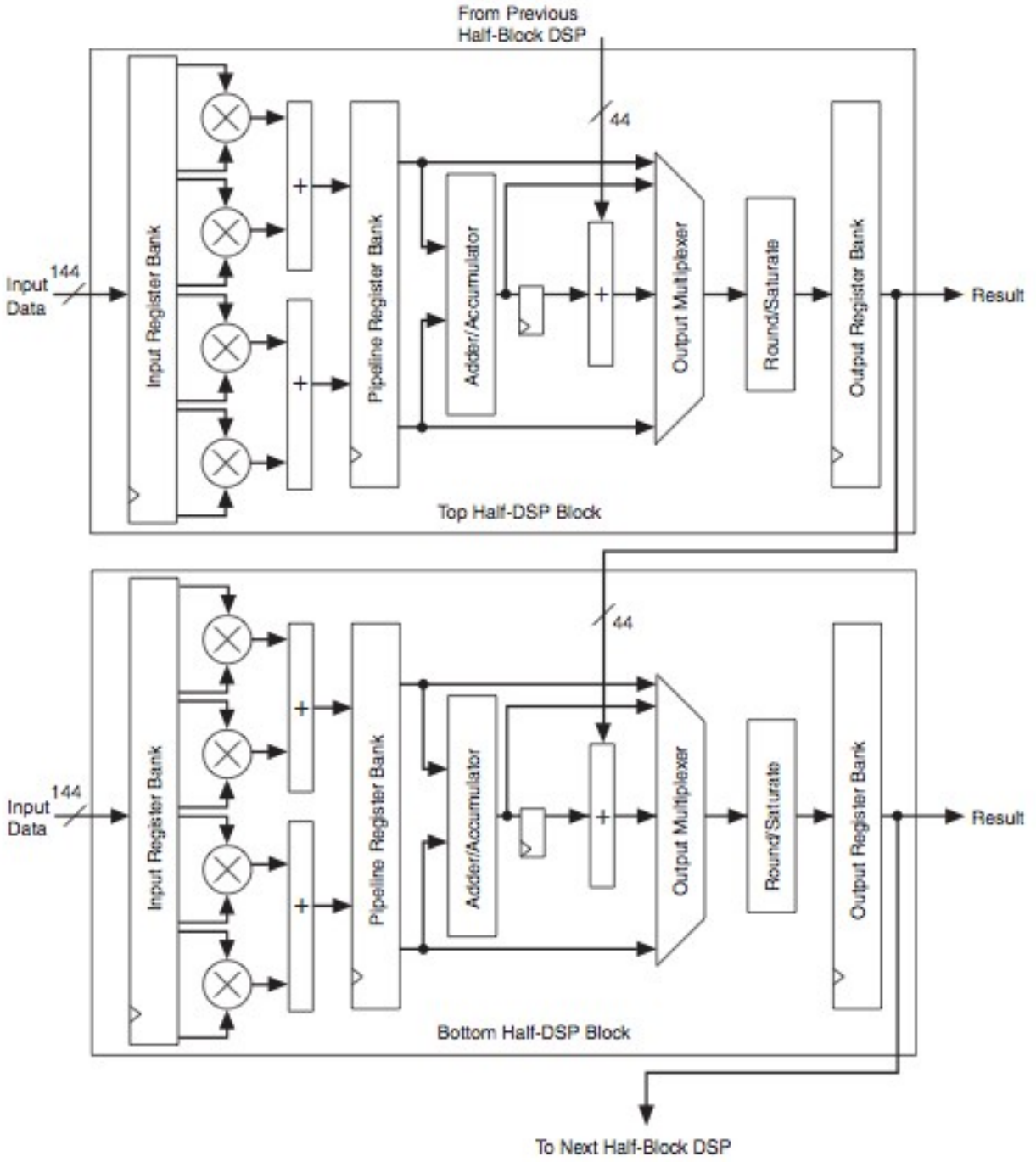
DSP48E Slice : Xilinx Virtex5



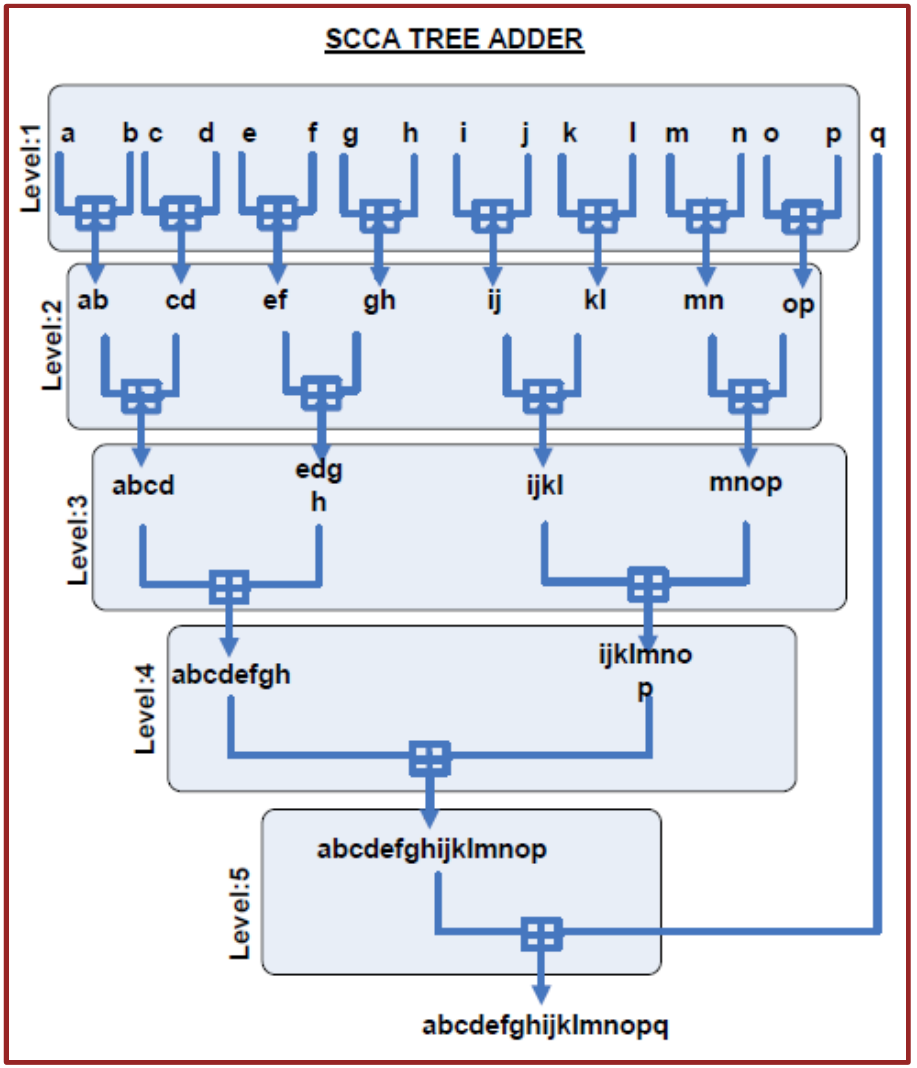
*These signals are dedicated routing paths internal to the DSP48E column. They are not accessible via fabric routing resources.

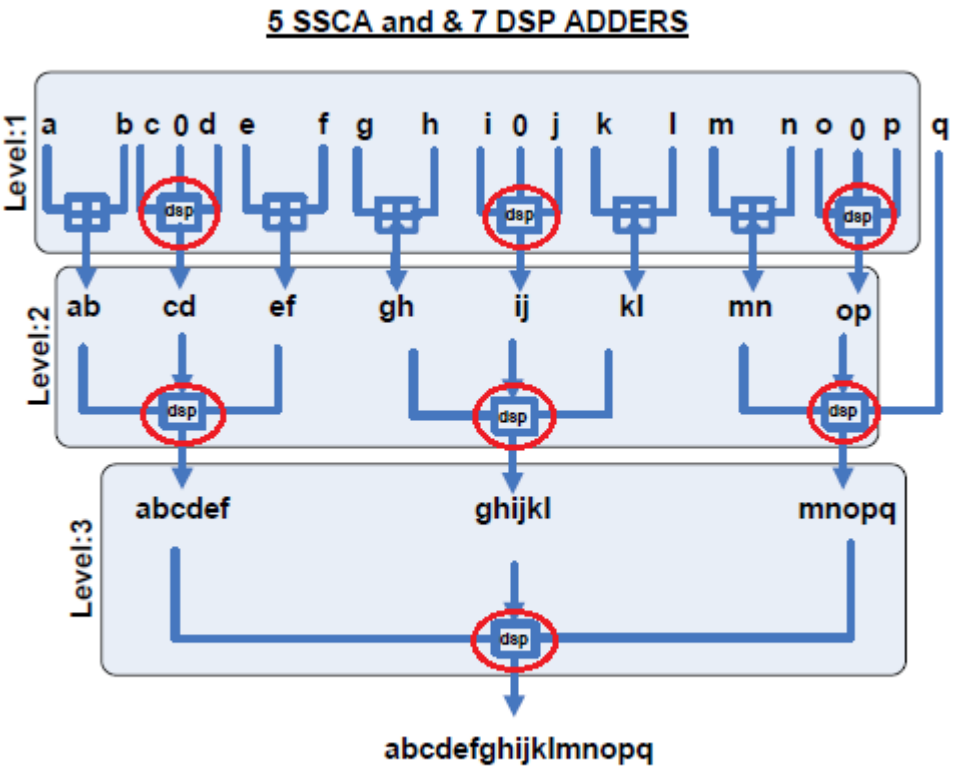
UG193_c1_01_032806

Full DSP Block
Altera Stratix III



Multi-operand addition (BMW example)





Dsp – DSP based adder
+ - Simple Carry Chain Adder
(inferred by “+” in VHDL)

Xilinx Virtex 5 results

Algorithm	Architecture	Throughput	Resource utilization	Tp/#CLB
		Mb/s	#CLB_slice, #BRAMs, #DSPs	(Mb/s)/#CLB_slice
DSP Units				
BMW	Basic	4482	5442,0,0	0.82
	Embedded	3870	3436,0,112	1.12
Cubehash	Basic	3872	633,0,0	5.99
	Embedded	3150	626,0,16	5.03
Skein	Basic	2565	1306,0,0	1.96
	Embedded	2359	1264,0,32	1.86
Shabal	Basic	1719	283,0,0	6.08
	Embedded	1337	279,0,5	4.79
SIMD	Basic	3121	8922,0,0	0.35
	Embedded	2349	4748,0,96	0.49
DSP Units and Memory Blocks				
Blake	Basic	3176	1623,0,0	1.96
	Embedded	2119	622,12,8	3.20
Sha-2	Basic	1675	418,0,0	4.01
	Embedded	1719	320,1,5	5.37

Xilinx Virtex 5 results

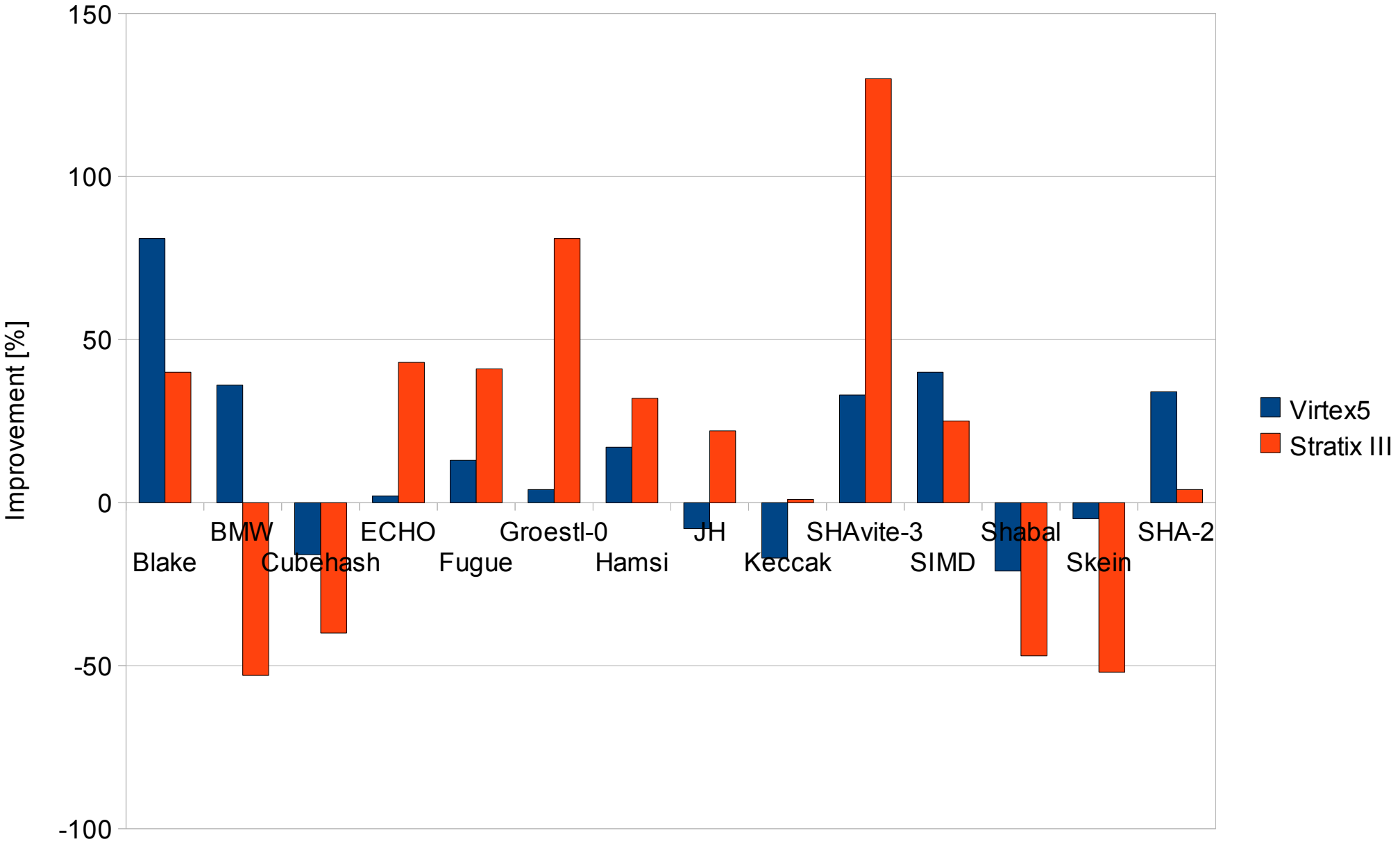
Algorithm	Architecture	Throughput	Resource utilization	Tp/#CLB
		Mb/s	#CLB_slice, #BRAMs, #DSPs	(Mb/s)/#CLB_slice
	Memory Blocks			
Blake	Basic	3176	1623,0,0	1.96
	Embedded	2572	726,13,0	3.54
ECHO	Basic	12094	4888,0,0	2.47
	Embedded	9748	3856,69,0	2.53
Fugue	Basic	3414	700,0,0	4.88
	Embedded	3165	574,8,0	5.51
Groestl-0	Basic	7885	1597,0,0	4.94
	Embedded	6098	1188,48,0	5.13
Hamsi	Basic	2997	788,0,0	3.85
	Embedded	2619	582,32,0	4.50
JH	Basic	5874	1056,0,0	5.56
	Embedded	5045	985,4,0	5.12
Keccak	Basic	12817	1272,0,0	10.08
	Embedded	11252	1338,1,0	8.41
SHA-2	Basic	1675	418,0,0	4.01
	Embedded	1591	381,1,0	4.17
SHAvite-3	Basic	3751	1104,0,0	3.40

Round 2: Throughput/area changes when embedded resources used (High Performance devices)

Virtex 5	basic	embedded	%
Blake	1.96	3.54	81
BMW	0.82	1.12	36
Cubehash	5.99	5.03	-16
ECHO	2.47	2.53	2
Fugue	4.88	5.51	13
Groestl-0	4.94	5.13	4
Hamsi	3.85	4.50	17
JH	5.56	5.12	-8
Keccak	10.08	8.41	-17
Luffa	9.30	NA	NA
SHA-2	4.01	5.37	34
SHAvite-3	3.40	4.52	33
SIMD	0.35	0.49	40
Shabal	6.08	4.79	-21
Skein	1.96	1.86	-5

Stratix III	basic	embedded	%
Blake	0.59	0.83	40
BMW	0.51	0.24	-53
Cubehash	1.94	1.17	-40
ECHO	0.67	0.96	43
Fugue	1.36	1.92	41
Groestl-0	1.12	2.03	81
Hamsi	1.33	1.75	32
JH	1.50	1.83	22
Keccak	3.28	3.30	1
Luffa	2.82	NA	NA
SHA-2	1.67	1.74	4
SHAvite-3	1.12	2.58	130
SIMD	0.12	0.15	25
Shabal	2.17	1.14	-47
Skein	0.55	0.26	-52

Round 2: High Performance FPGAs throughput/area improvement when embedded resources used

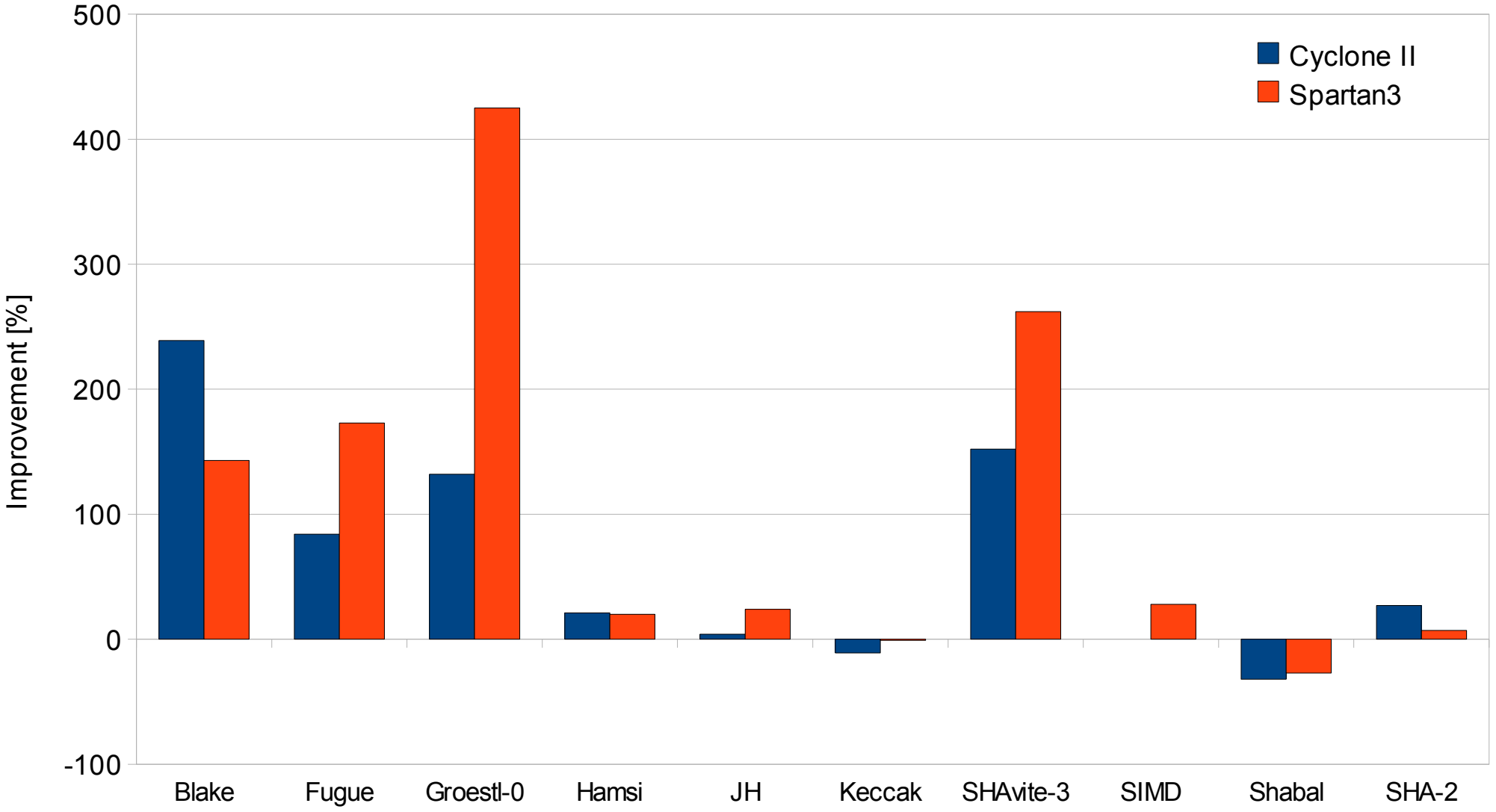


Round 2: Throughput/area changes when embedded resources used (Low Cost devices)

Spartan 3	basic	embedded	%
Blake	0.18	0.61	239
BMW	NA	NA	NA
Cubehash	0.93	NA	NA
ECHO	0.14	NA	NA
Fugue	0.49	0.9	84
Groestl-0	0.31	0.72	132
Hamsi	0.58	0.7	21
JH	0.51	0.53	4
Keccak	1.46	1.3	-11
Luffa	1.5	NA	NA
SHA-2	0.74	0.79	7
SHAvite-3	0.27	0.68	152
SIMD	NA	NA	NA
Shabal	1.13	0.77	-32
Skein	0.32	NA	NA

Cyclone II	basic	embedded	%
Blake	0.14	0.34	143
BMW	NA	NA	NA
Cubehash	0.59	NA	NA
ECHO	NA	0.31	NA
Fugue	0.26	0.71	173
Groestl-0	0.16	0.84	425
Hamsi	0.49	0.59	20
JH	0.33	0.41	24
Keccak	0.99	0.98	-1
Luffa	1.13	NA	NA
SHA-2	0.41	0.52	27
SHAvite-3	0.13	0.47	262
SIMD	0.04	0.05	28
Shabal	0.22	0.16	-27
Skein	0.22	NA	NA

Round 2: Low Cost FPGAs throughput/area improvement when embedded resources used



Round 3: Xilinx Virtex 5 results

Algorithm	Architecture	Throughput	Resource utilization	Tp/#CLB
		Mb/s	#CLB slice, #BRAMs, #DSPs	(Mb/s)/#CLB
DSP Units				
Skein	Basic	2565	1306,0,0	1.96
	Embedded	2359	1264,0,32	1.86
DSP Units and Block RAMs				
Blake	Basic	2252	1702,0,0	1.32
	Embedded	1534	662,12,8	2.31
SHA-2	Basic	1504	418,0,0	3.6
	Embedded	1719	320,1,5	5.37
Block RAMs				
Blake	Basic	2252	1854,0,0	1.32
	Embedded	1861	726,13,0	2.56
Groestl	Basic	6083	1852,0,0	3.28
	Embedded	5858	1255,50,0	4.67
JH	Basic	4917	1056,0,0	4.65
	Embedded	3120	1066,4,0	2.92
Keccak	Basic	13536	1352,0,0	10.01
	Embedded	11252	1338,1,0	8.41

Round 3: Throughput/area changes after embedded resources used

Virtex 5

	basic	embedded	%
Blake	1.32	2.56	94
Groestl	3.28	4.67	42
JH	4.65	2.92	-37
Keccak	10.01	8.41	-16
Skein	1.96	1.86	-5

Stratix III

	basic	embedded	%
Blake	0.43	0.94	118
Groestl	0.78	2.18	179
JH	1.39	1.70	22
Keccak	3.25	3.30	2
Skein	0.55	0.26	-52

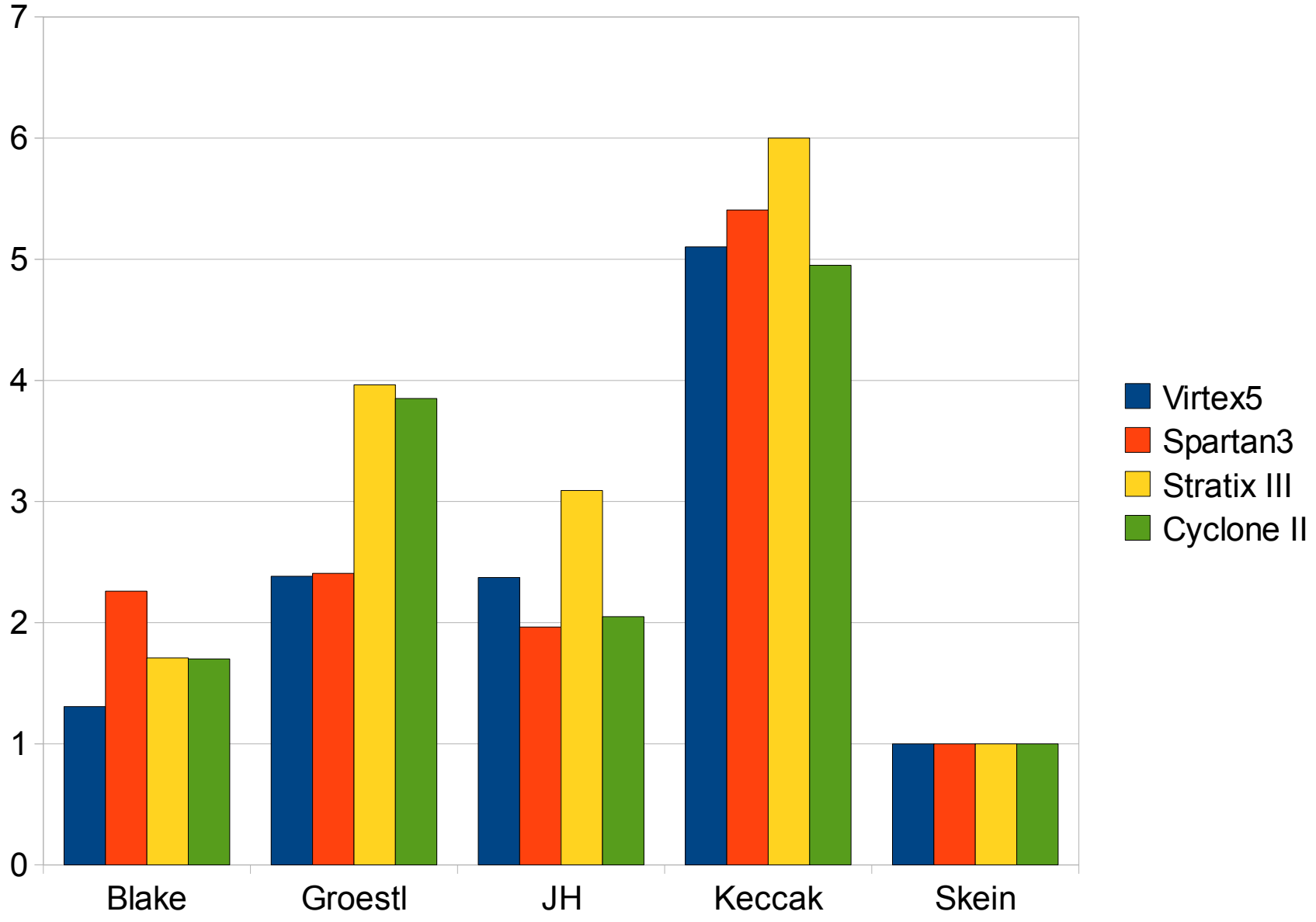
Spartan 3

	basic	embedded	%
Blake	0.25	0.61	144
Groestl	0.24	0.65	171
JH	0.41	0.53	29
Keccak	1.46	1.33	-9
Skein	0.27	N/A	N/A

Cyclone II

	basic	embedded	%
Blake	0.13	0.34	162
Groestl	0.15	0.77	413
JH	0.36	0.41	14
Keccak	0.99	0.98	-1
Skein	0.20	N/A	N/A

Round 3: Normalized Throughput/Area of the Best Results out of Basic and Embedded Architectures



Conclusions

- Basic Architectures of SHA-3 candidates were enhanced with embedded resources – results were collected for both Altera and Xilinx low cost and high performance devices.
- The drop in frequency (throughput) was caused by the interconnect delays between reconfigurable logic and embedded resources.
- DSP units and multipliers have limited importance for selected hash functions - majority of investigated algorithms use addition only.
- Except Skein on Altera Stratix III, significant portion of logic was shifted to embedded resources.
- Embedded memories helped improve throughput/area for all AES based functions and Blake on all selected devices.
- SHA3 Round 3 - the biggest improvement noted for Blake and Groestl FPGA architectures with hard-wired components.
- SHA-3 Round 3 candidates - ranking changes for High Speed implementations on FPGAs: 1. Keccak, 2. Groestl, 3. JH, 4. Blake, 5. Skein.