Use of Embedded FPGA Resources in Implementations of Five Round Three SHA-3 Candidates

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

George Mason University, USA

Agenda

- SHA-3 High Speed Implementations – results summary
- SHA-3 candidates high speed architectures with embedded resources methodology
- Hardwired resources in FPGAs
- Results
- Conclusions

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
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
Keccak	1272	0	12817	10.08	GMU
JH	1056	0	5874	5.56	GMU
Skein	1306	0	2565	1.96	GMU

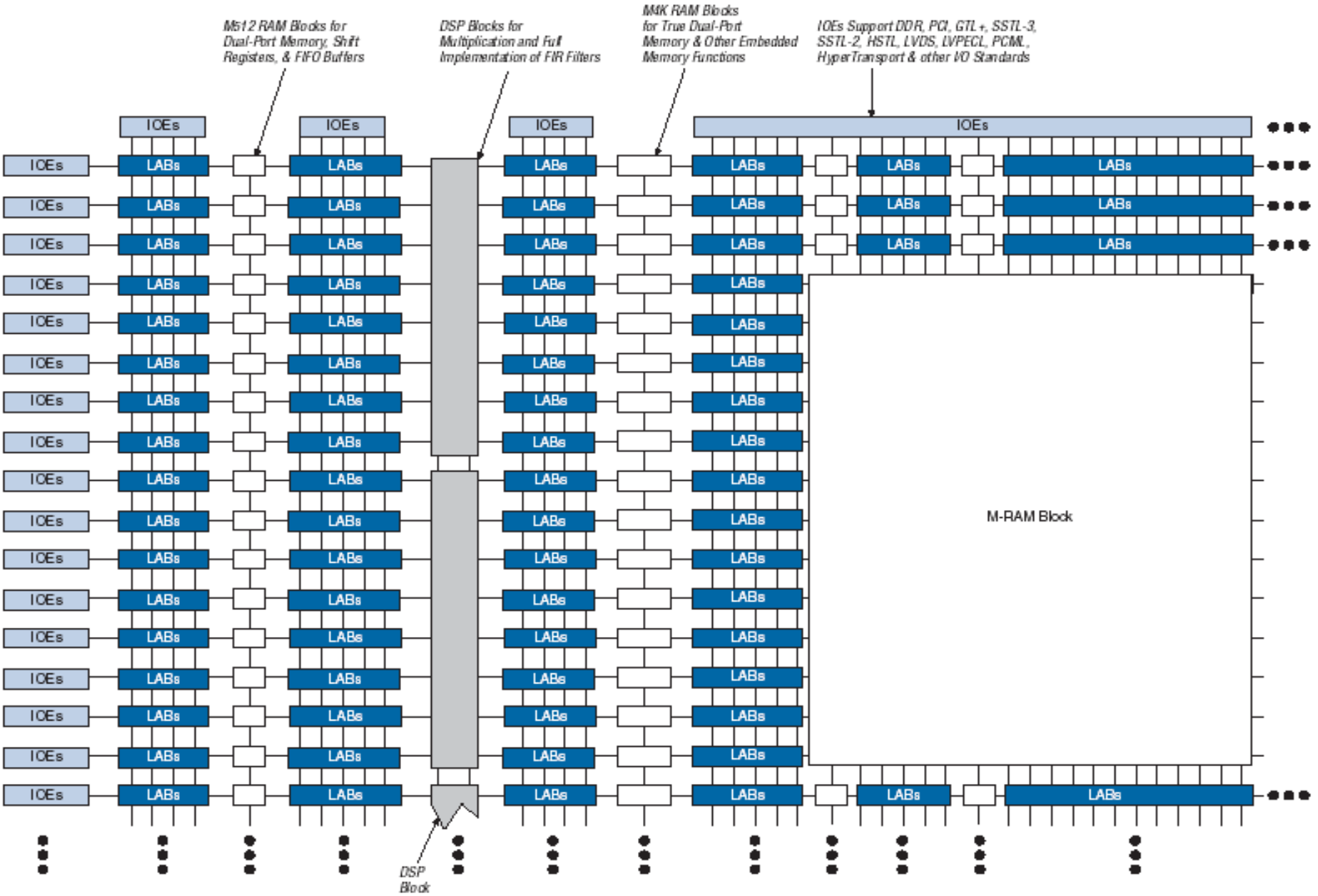
Round 3:

	Area	Bram	Throughput	Throughput/Area	Source
Blake	1702	0	2275	1.32	GMU
Groestl	1852	0	6083	3.28	GMU
Keccak	1272	0	12817	10.08	GMU
JH	1056	0	4917	4.65	GMU
Skein	1306	0	2565	1.96	GMU

Methodology

- Top level architectures from GMU basic designs,
- http://eprint.iacr.org/2010/445
- Uniform and practical Interface,
- 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 optimization criteria,
- Use of ATHENa for generation, optimization and comparative analysis of results,

Altera Stratix II



Performance metrics

Area:

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)

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

SHA-3 candidates operations and FPGA embedded resources

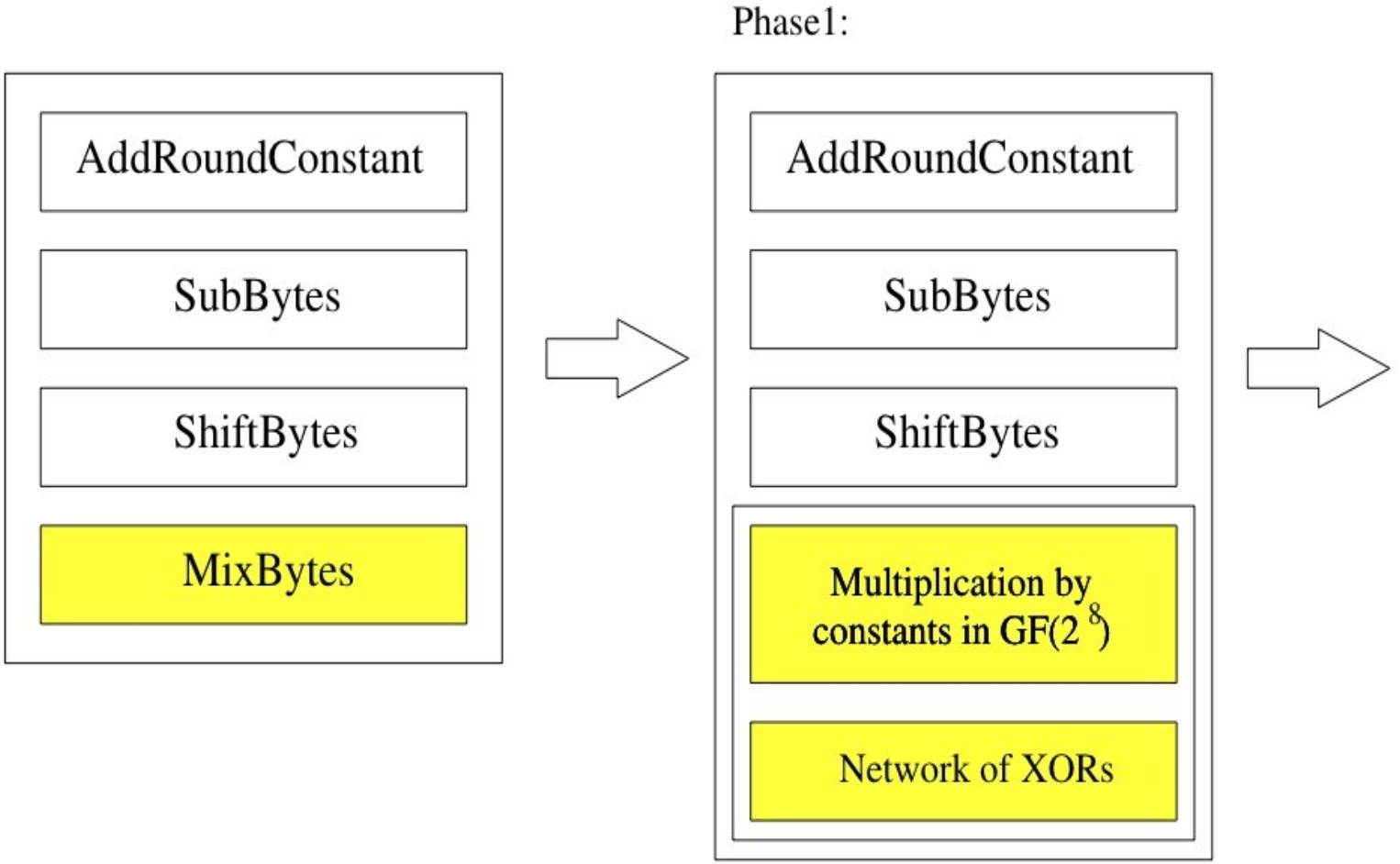
	S-box	GF Mul	mADD	ADD/SUB	Additional Memories
Blake			mADD3	ADD	Message expansion tables
Groestl	AES 8x8	x02-x07			
JH	4x4	x02, x05			Round constants
Keccak					Round constants
Skein				ADD-64	

SHA-3 candidates operations and FPGA embedded resources

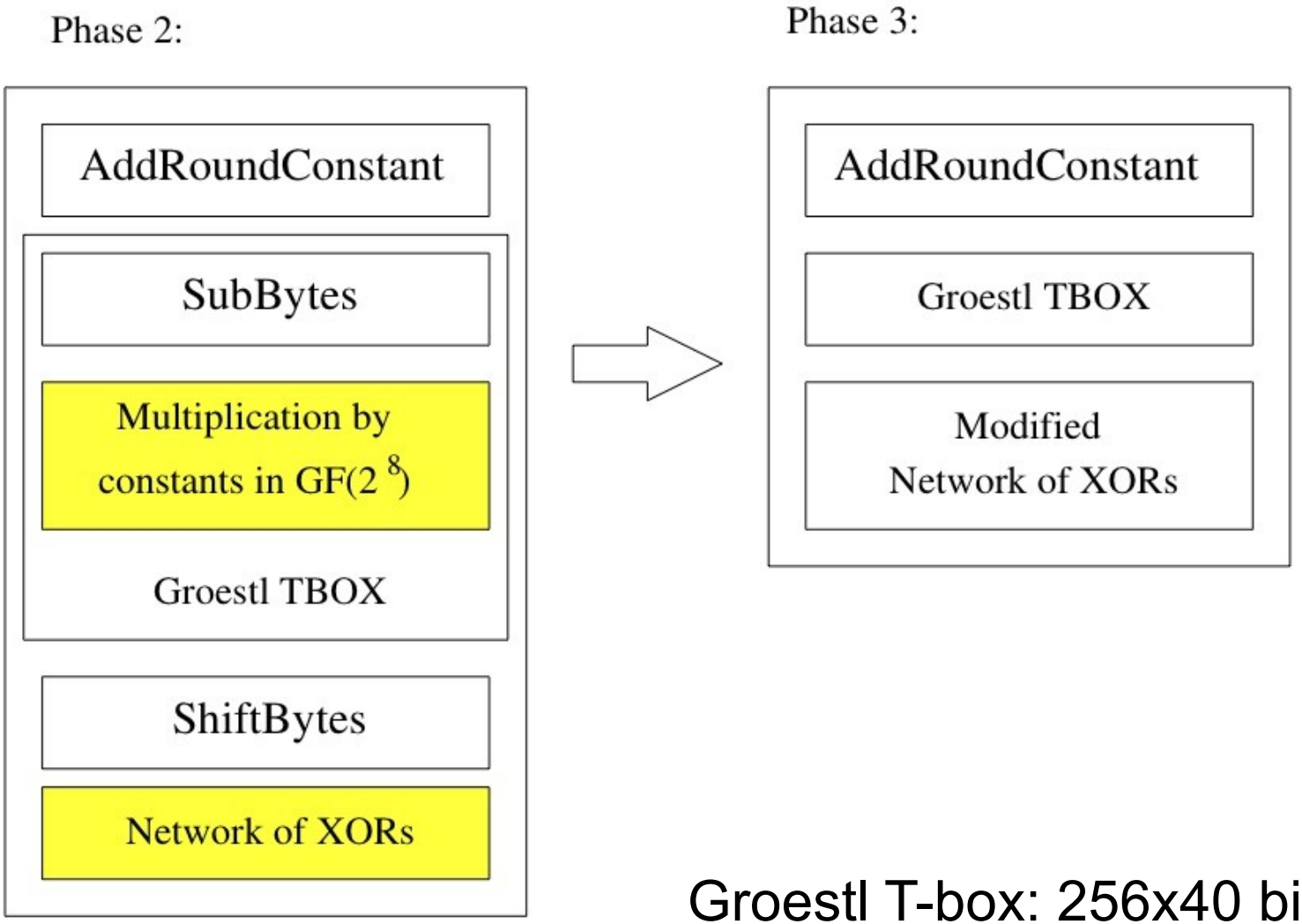
	S-box	GF Mul	mADD	ADD/SUB	Additional Memories
Blake			mADD3	ADD	Message expansion tables
Groestl	AES 8x8	x02-x07			
JH	4x4	x02, x05			Round constants
Keccak					Round constants
Skein				ADD-64	

	S-box	GF Mul	mADD	ADD/SUB	Additional Memories
Blake			DSP	DSP	BRAM
Groestl	BRAM				
JH	BRAM				BRAM
Keccak					BRAM
Skein				DSP	

Groestl-0/Groestl T-box



Groestl-0/Groestl T-box

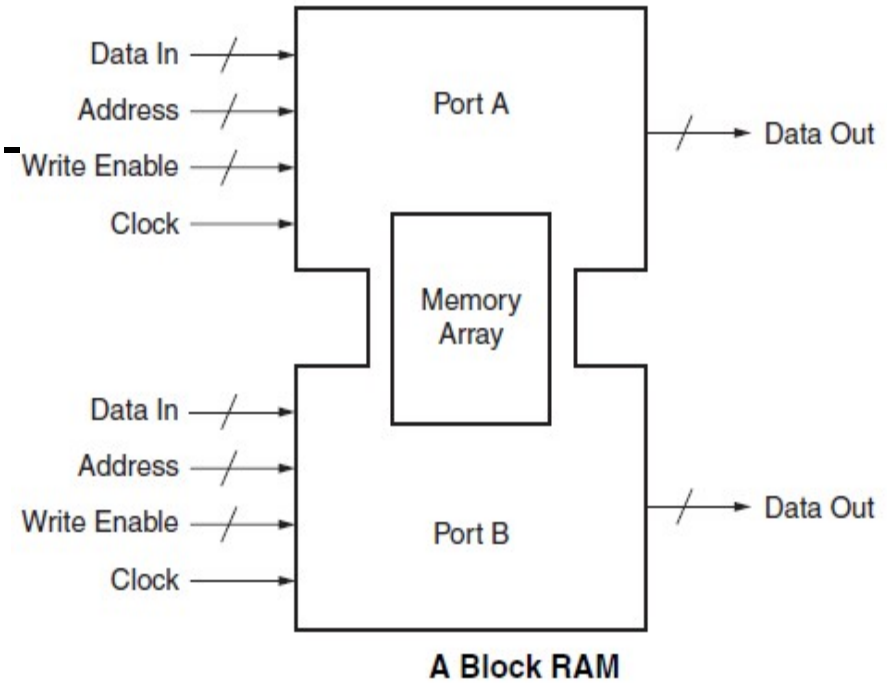


Groestl T-box: 256x40 bits

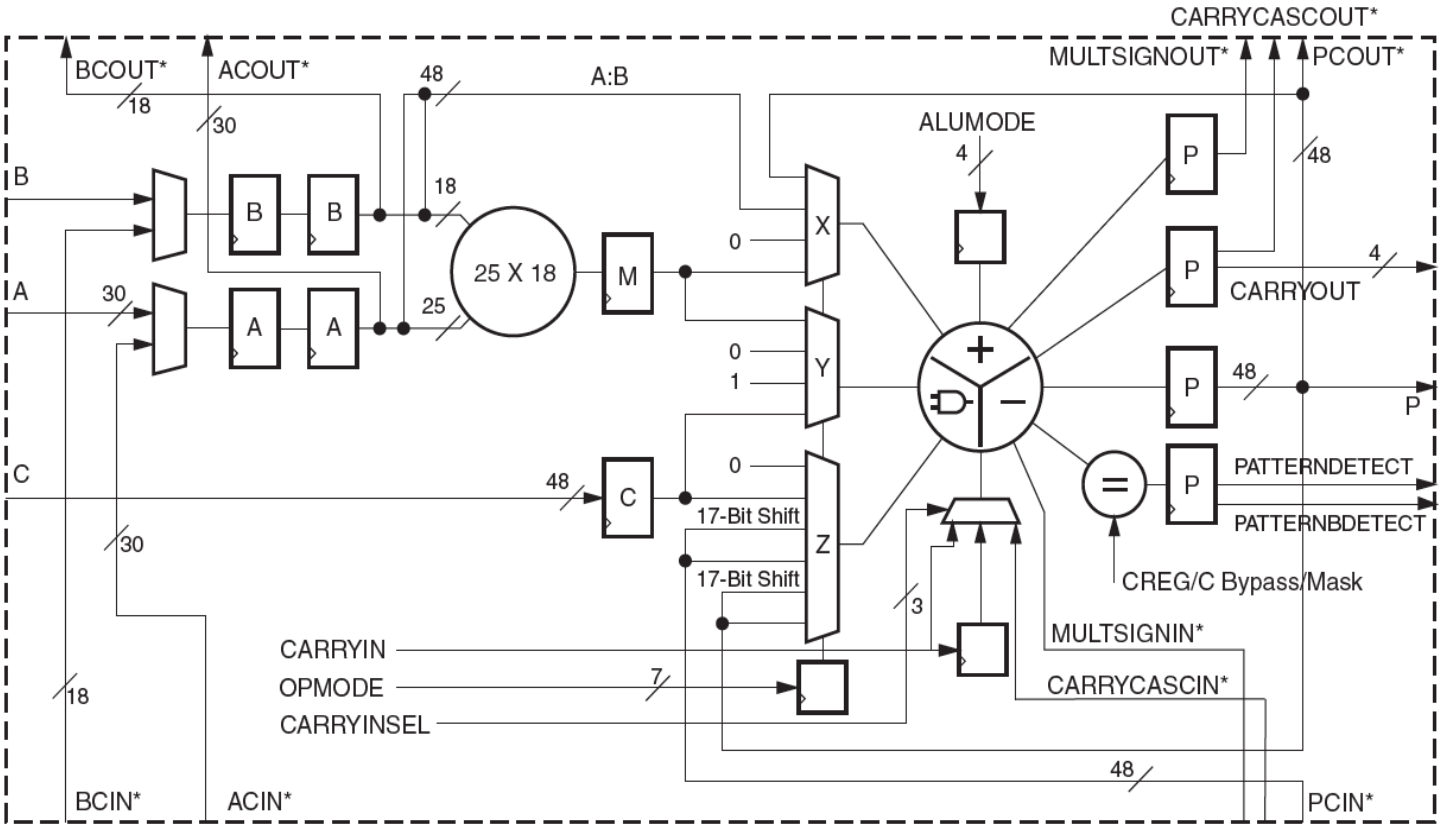
Block Memories

- Cyclone II (M4k), Stratix III (M9k),
- Spartan 3 (RAM18k), Virtex 5 (RAM36k)
- Aspect ratio (up to 32 bits 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



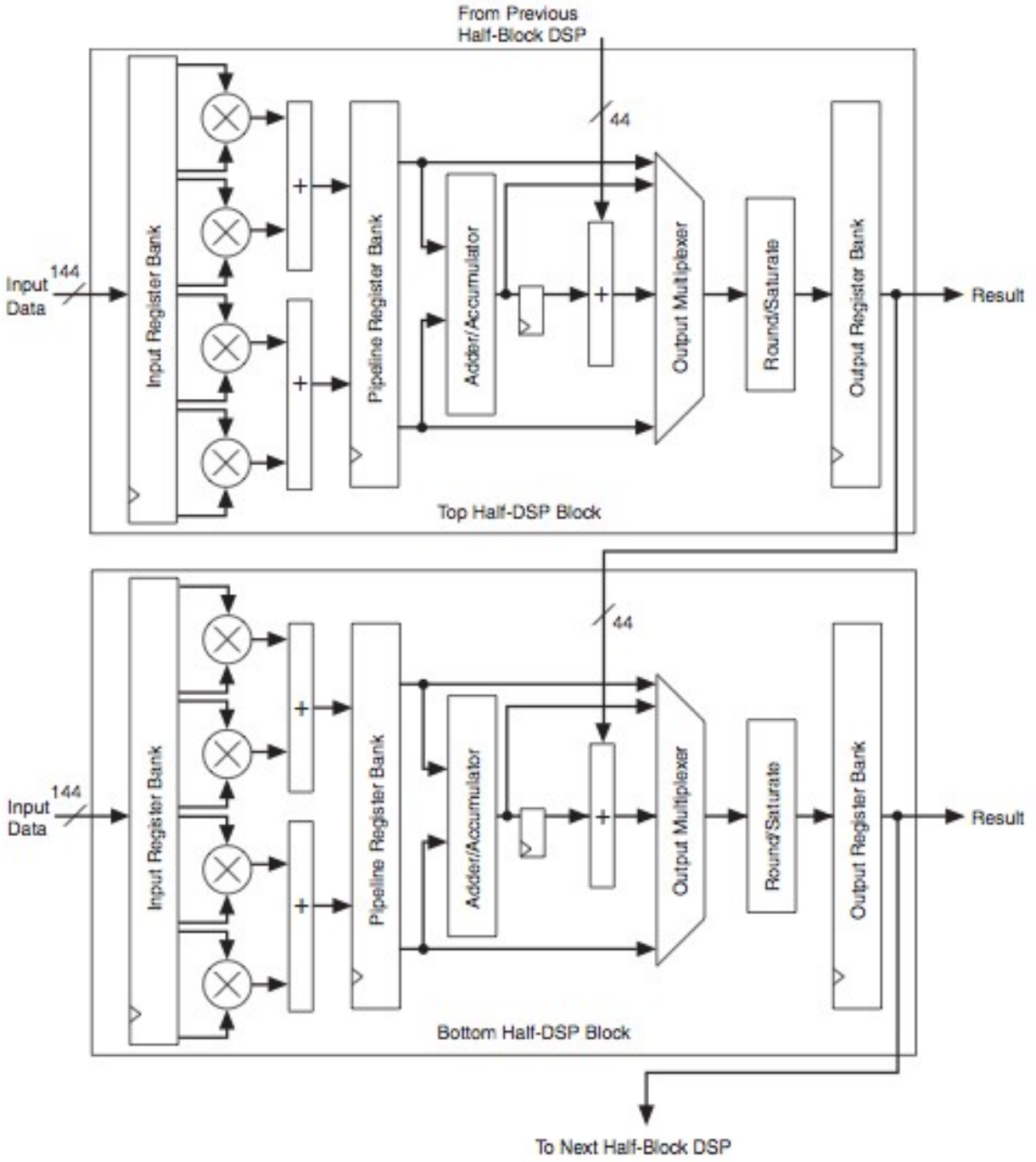
DSP48E Slice : Xilinx Virtex5



*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



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
SHA-2	Basic	1504	418,0,0	3.6
	Embedded	1591	381,1,0	4.17

Altera Stratix III results

Algorithm	Architecture	Throughput	Resource utilization	Tp/#ALUT
		Mb/s	#ALUT, #Mem_bits, #DSPs	(Mb/s)/#ALUT
DSP Units				
Skein	Basic	2426	4381,0,0	0.55
	Embedded	1472	5705,0,128	0.26
DSP Units and Block RAMs				
Blake	Basic	2086	4752,0,0	0.43
	Embedded	1073	1773,12k,32	0.6
SHA-2	Basic	1654	988,0,0	1.67
	Embedded	1621	795,2k,16	2.03
Block RAMs				
Blake	Basic	2086	4752,0,0	0.43
	Embedded	1808	1900,12k,0	0.94
Groestl	Basic	5649	7242,0,0	0.78
	Embedded	6082	4438,655k,0	2.18
JH	Basic	4654	3331,0,0	1.39
	Embedded	4651	2743,9k,0	1.7
Keccak	Basic	13746	4221,0,0	3.25
	Embedded	14103	4277,2k,0	3.3
SHA-2	Basic	1654	988,0,0	1.67
	Embedded	1661	956,2k,0	1.73

Throughput/area ranking 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	1.7	22
Keccak	3.25	3.3	2
Skein	0.55	0.26	-52

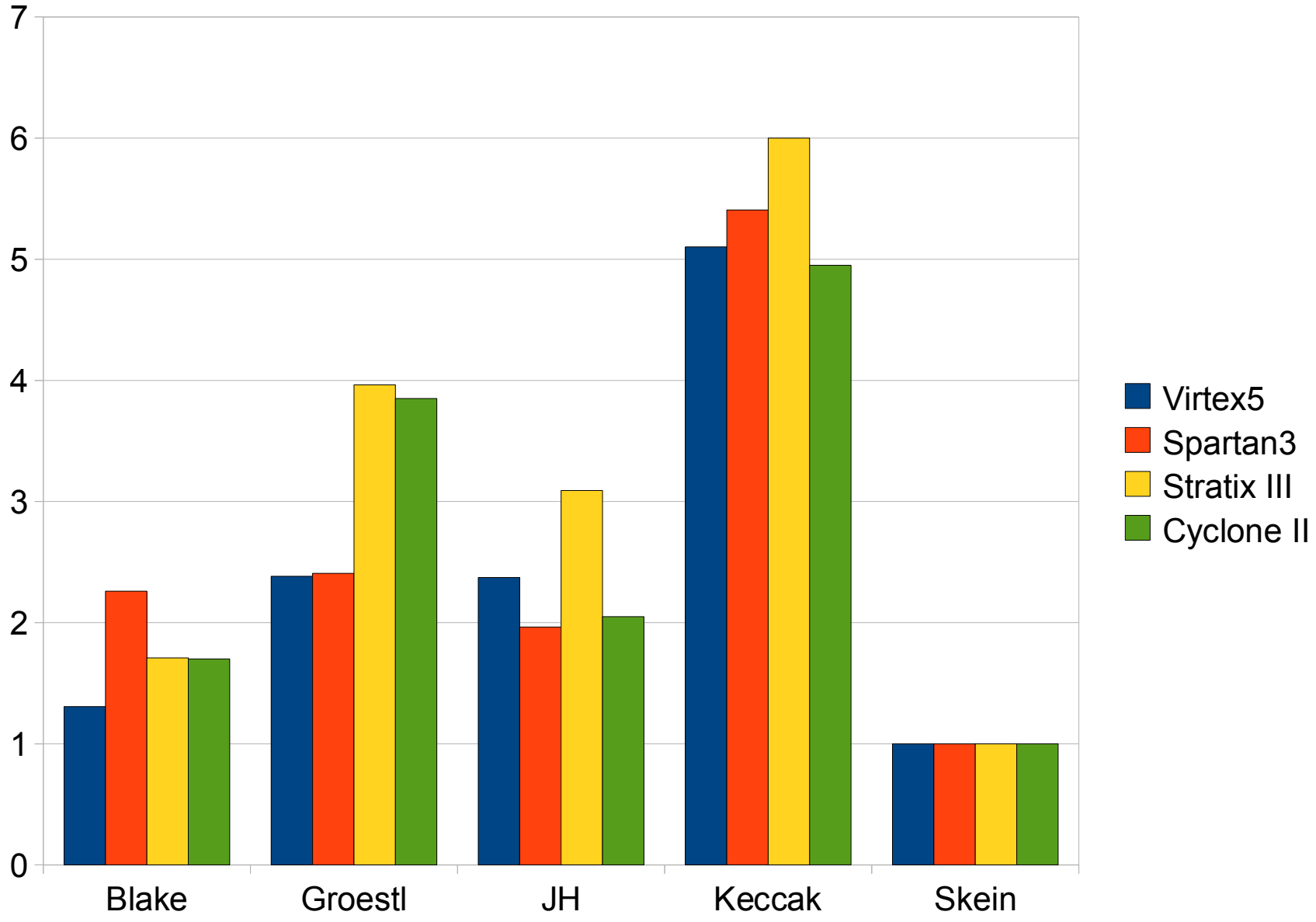
Spartan 3

	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	0.2	N/A	N/A

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



Conclusions

- Basic Architectures of SHA-3 candidates were enhanced by embedded resources – results were collected for both Altera and Xilinx low cost and high performance devices.
- The drop in frequency 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.
- The biggest improvement noted for Blake and Groestl FPGA architectures with hardwired components.
- SHA-3 Round 3 candidates ranking changes for High Speed implementations on FPGAs: 1. Keccak, 2. Groestl, 3. JH, 4. Blake, 5. Skein.

Questions ?

CERG: https:/cryptography.gmu.edu

ATHENa: https:/cryptography.gmu.edu/athena

ATHENaDB: https://cryptography.gmu.edu/athenadb/