

A Skein-512 Hardware Implementation

Jesse Walker, Farhana Sheikh, Sanu Mathew,
Ram Krishnamurthy

Intel Labs: Circuits and Systems Research
Intel Corporation

Outline

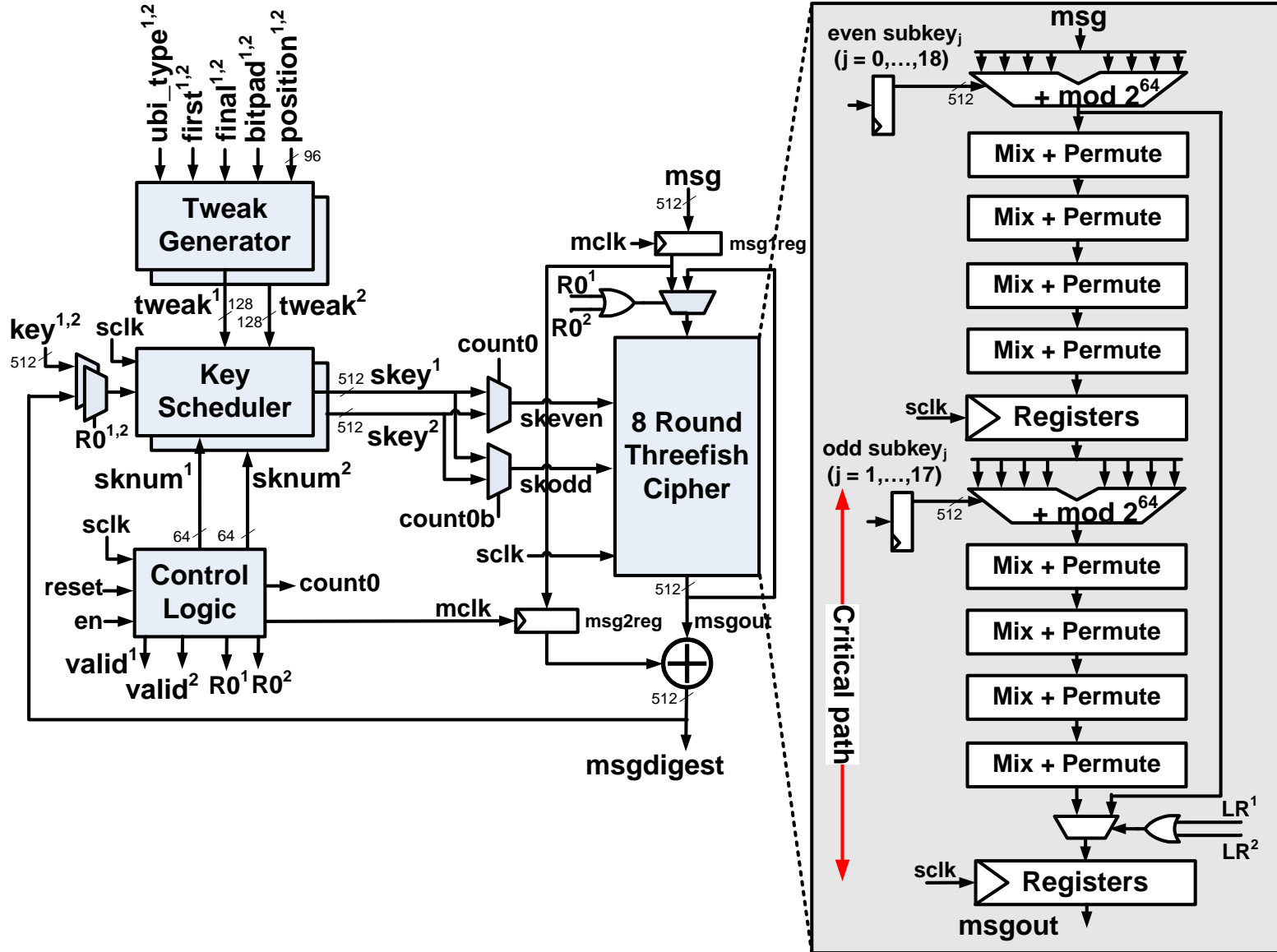
- Introduction
- Skein-512 hardware implementation
- Performance tradeoffs
- Area tradeoffs
- Summary

Introduction

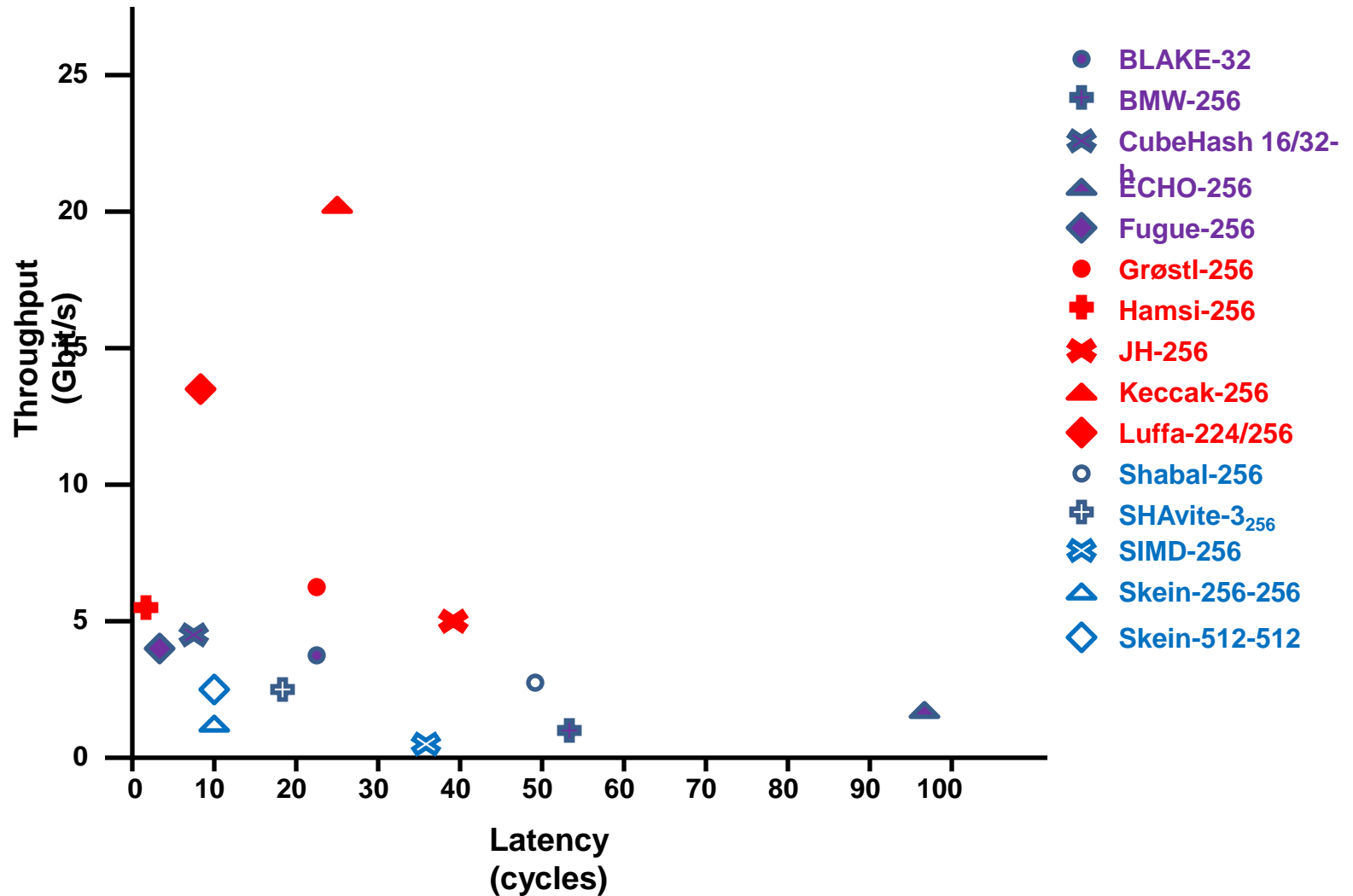
- Motivated by Graz University paper
- Designed using Intel's CMOS 32nm process
 - Intel's standard cells scale exactly 1.2x/generation
- One architecture with 4 alternative pipeline options

Name	Clock Frequency (MHz)	Latency (cycles)	Area (GE)	Throughput (Gbit/s)
iSkein-512-1R-8M	2380.95	80	70701	121.90
iSkein-512-2R-4M	1736.11	40	62954	88.89
iSkein-512-4R-2M	1126.13	20	60395	57.66
iSkein-512-8R-1M	631.31	10	57931	32.32

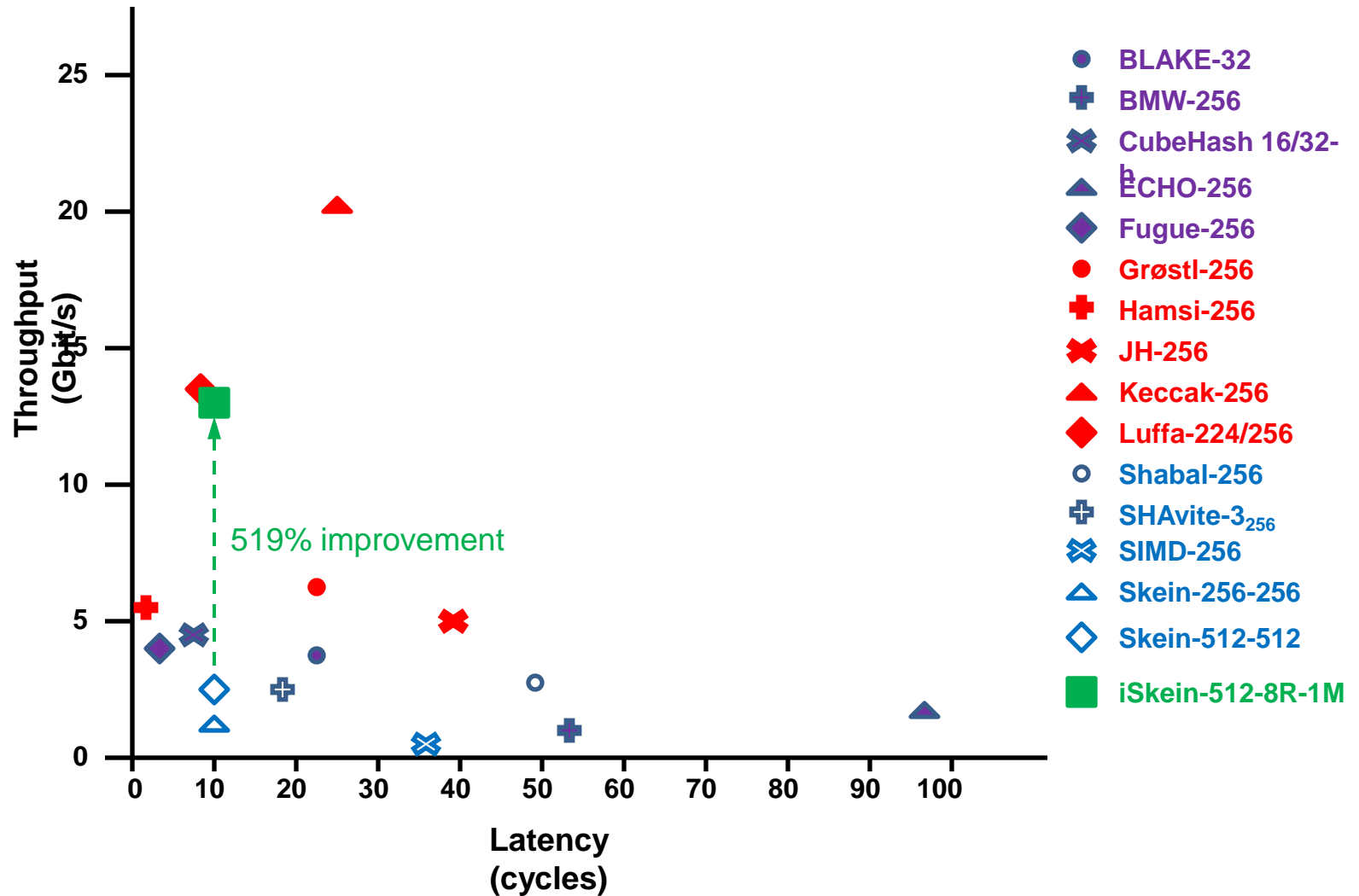
Example Block Diagram



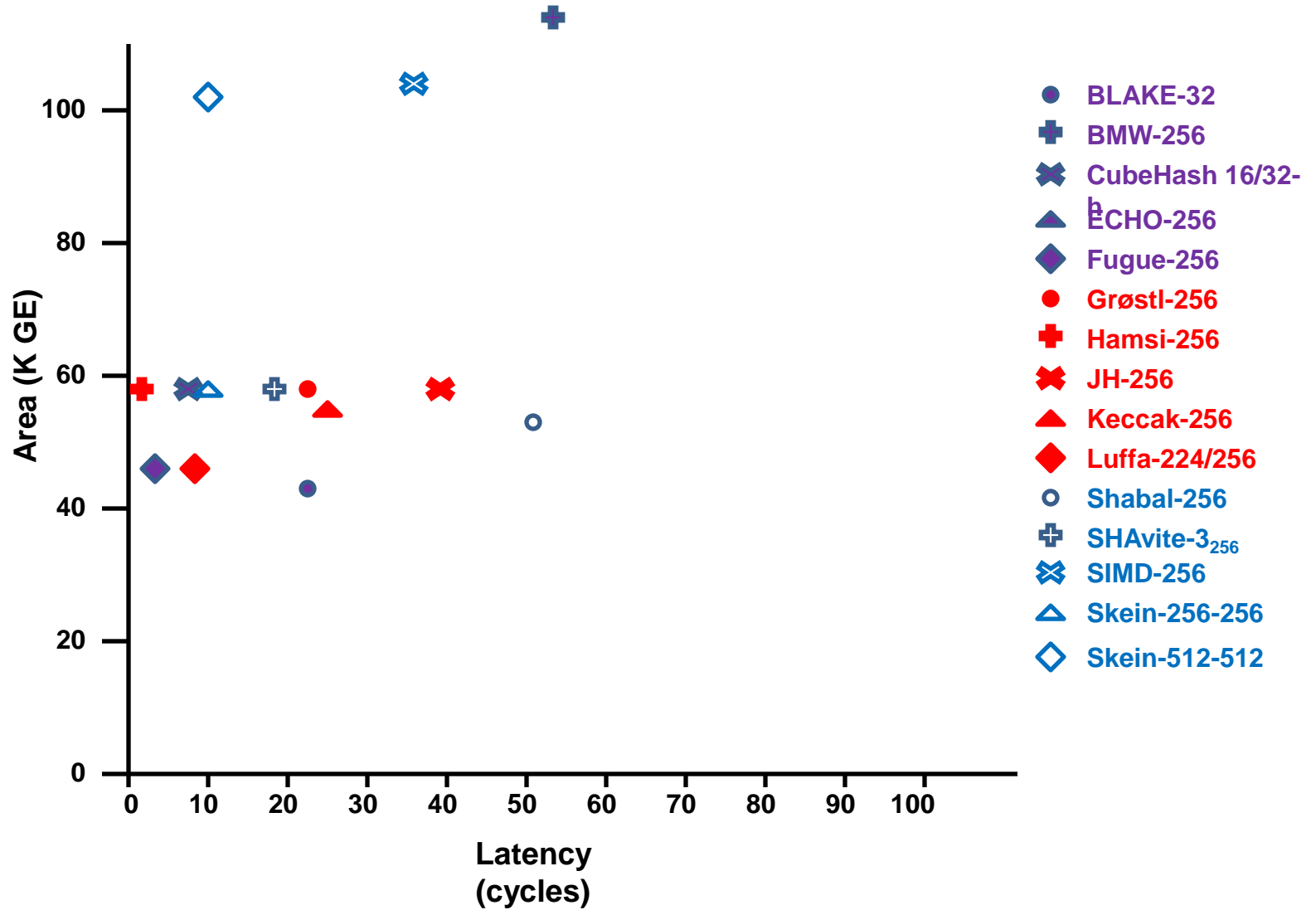
Performance Tradeoffs (180 nm)



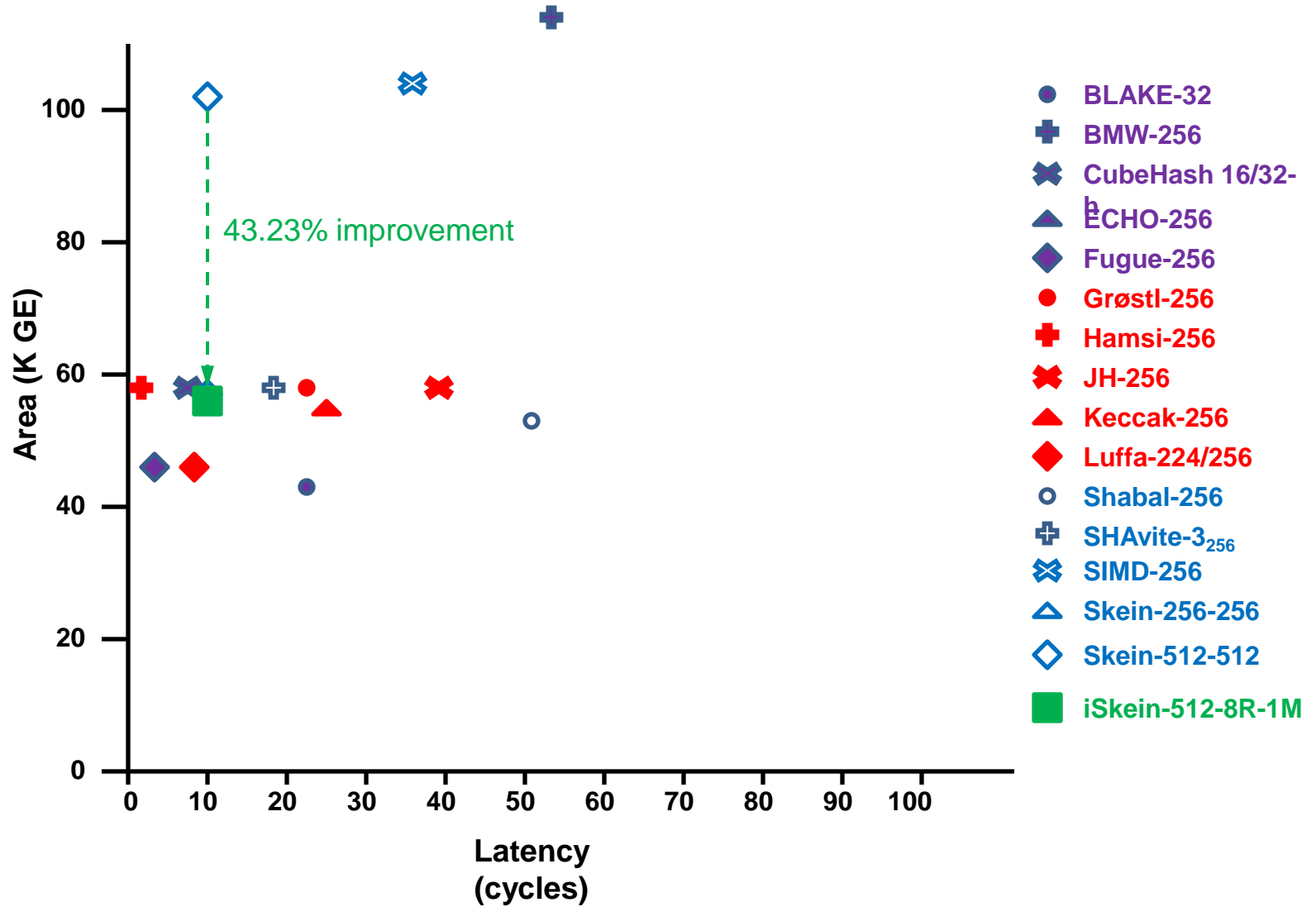
Performance Tradeoffs (180 nm)



Area Tradeoffs



Area Tradeoffs



Summary

- Skein-512 hardware implementation
 - 57.9K GE, 10 cycles latency
 - 32nm: 32Gbit/s
 - 180nm: 12.99 Gbit/s
- Competitive Skein-512 hardware appears feasible
- Needs to understand why different performance between Intel's and other implementations
 - Intel uses carry look-ahead adders

Backup

180 nm Comparison

Implementation	Block size (bits)	Latency (cycles)	Area (GE)	Clock freq (MHz)	TP (Gbit/s)
BLAKE-32	512	22	45640	170.64	3.971
BMW-256	512	53	122092	164.20	1.586
Cubehash 16/32-h	256	8	58872	145.77	4.665
ECHO-256	1536	97	141489	141.84	2.246
Fuege-256	32	2	46257	255.75	4.092
Groestl-256	512	22	58402	270.27	6.290
Hamsi-256	32	1	58661	173.91	5.565
JH-256	512	39	58832	380.22	4.991
Keccak-256	1088	25	56316	487.80	21.229
Luffa-224/256	256	9	44972	483.09	13.741
Shabal-256	512	50	54186	320.51	3.282
SHAvite-3 ₂₅₆	512	19	58828	88.57	2.387
SIMD-256	512	36	104166	64.93	0.924
Skein-256-256	256	10	58611	73.52	1.882
Skein-512-512	512	10	102039	48.87	2.502
iSkein-512-8R-1M	512	10	57931	253.71	12.989
iSkein-512-4R-2M	512	20	60395	452.57	23.172
iSkein-512-2R-4M	512	40	62954	697.70	35.723
iSkein-512-1R-8M	512	80	70071	956.85	48.989