

Fair and Comprehensive Performance Evaluation **of SHA3 Hardware Implementations**

PhD Student: Eric Xu Guo

Advisor: Prof. Patrick Schaumont

Sep. 24, 2010



Digital VLSI Design Class

Homework:

Compare the ASIC results of 2 versions of HDL designs of the same algorithm. Which one has better performance?

Discussion Board



Student: Since I already have FPGA EDA tools installed on my laptop, may I just use the FPGA results to conclude the comparison in ASIC?



TA: The answer is

NO! 

*Note: ASIC – Application Specific Integrated Circuit
FPGA – Field Programmable Gate Array*

❑ Introduction

- *Hash Definition and Applications*
- *SHA3 Competition*

❑ Hardware Benchmarking Methodology

- *Application Scenario*
- *Interface*
- *Metrics*
- *Design Space*
- *Results*

❑ Conclusions

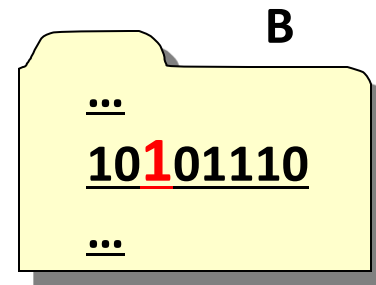
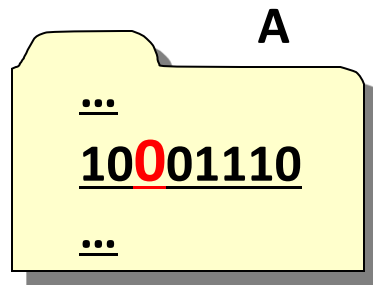
Cryptographic Hash Function

❖ **Hash functions** take a variable-length message x and reduce it to a shorter fixed-length message digest $\text{hash}(x)$.

❖ **Applications:** “Swiss army knives” of crypto:

- Digital signatures (with public key algorithms)
- Random number generation
- Key update and derivation
- Message authentication codes & user authentication

Example:
File Integrity
Check



Hash Digest: 9e107d9d372bb6826bd81d3542a419d6

e4d909c290d0fb1ca068ffaddf22cbd0

NIST SHA3 Competition

❖ **Our Task:** Tell NIST which are the top candidates most suitable for hardware.



***Hardware
Benchmarking
of 14 SHA3
candidates***

□ Introduction

- *Hash Definition and Applications*
- *SHA3 Competition*

□ **Hardware Benchmarking Methodology**

- *Application Scenario*
- *Interface*
- *Metrics*
- *Design Space*
- *Results*

□ Conclusions

Current Hardware Benchmarks

	FPGA		ASIC	
Develop own source codes?	Kobayashi Yes	Gaj Yes	Tillich Yes	Henzen Yes



Different design optimizations and quality

Current Hardware Benchmarks

	FPGA		ASIC	
Technology Choices	Kobayashi Xilinx 65nm	Gaj Xilinx & Altera Multiple	Tillich 180nm Standard Cell	Henzen 90nm Standard Cell



Different platforms and technology nodes

Current Hardware Benchmarks

	FPGA		ASIC	
Hardware Interface	Kobayashi Handshake IF	Gaj FIFO IF	Tillich Infinite Bandwidth IF	Henzen Infinite Bandwidth IF

 Different hardware interface and application scenarios

Current Hardware Benchmarks

	FPGA		ASIC	
Chosen Metrics	Kobayashi	Gaj	Tillich	Henzen
	Area	Area	Area	Area
	Throughput	Throughput	Throughput	Throughput
	Power	Tp/Area		Energy
	Energy			



Different metrics for comparison

Current Hardware Benchmarks

	FPGA		ASIC	
Design Flow	Kobayashi FPGA Prototype w/ Measurements	Gaj Post-P&R Simulation	Tillich Post- Synthesis Simulation	Henzen Post- Layout Simulation

 Different design flow or stages for results extraction

❖ **Current Status: N people have N ways to do HW benchmarks**



Different design optimizations and quality



Different platforms and technology nodes



Different hardware interface and application scenarios



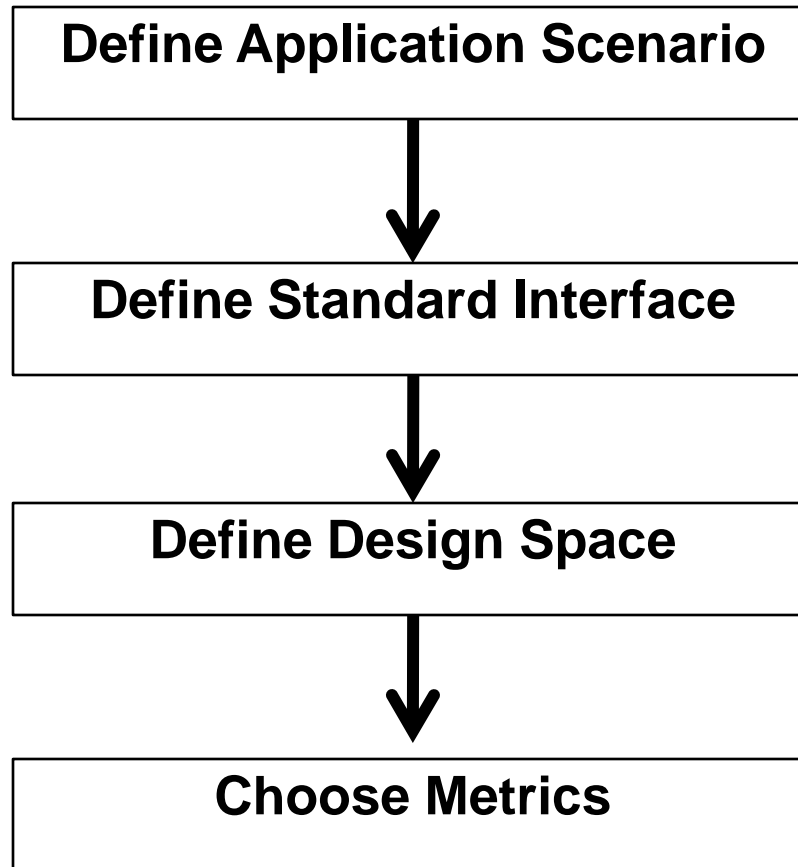
Different metrics for comparison



Different design flow or stages for results extraction

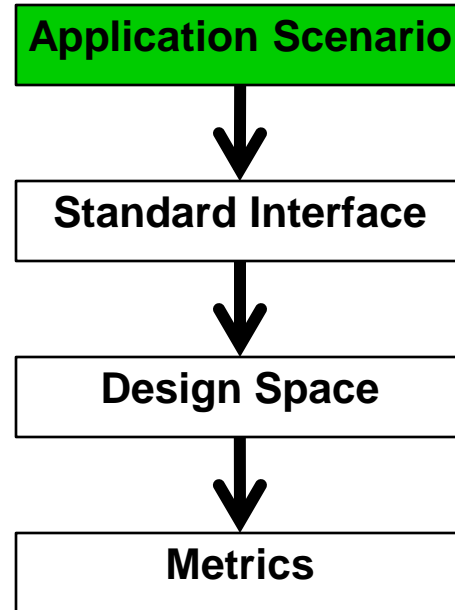
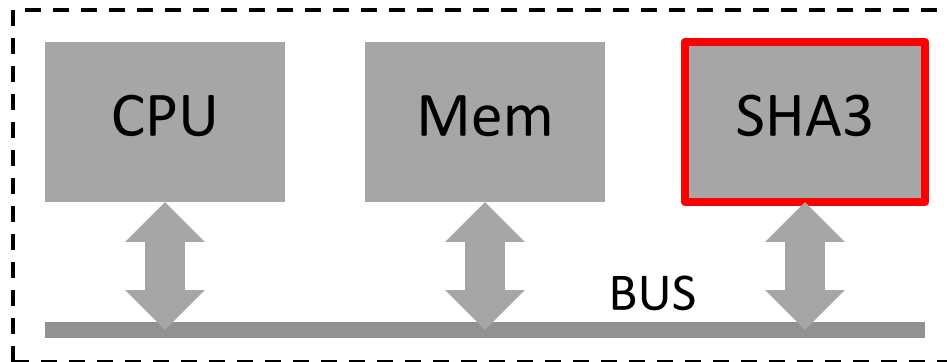
Consistent cross-platform comparisons between current results are impossible!

Proposed Methodology



❖ SHA3 HW as Intellectual Property Module

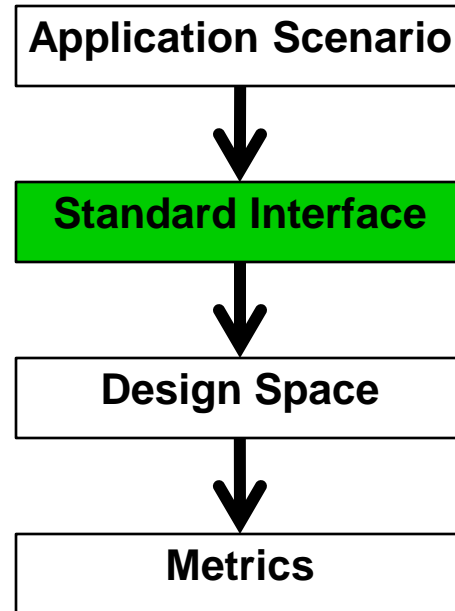
- System-on-Chip (SoC) Integration



❖ Define Standard Interface

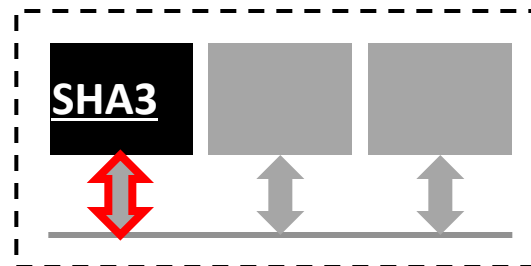
Hardware IF(API)

- [Gaj, CHES2010]
- [Kobayashi, HOST2010]
- [Chen, ePrint2008]
- [Baldwin, ePrint2010]



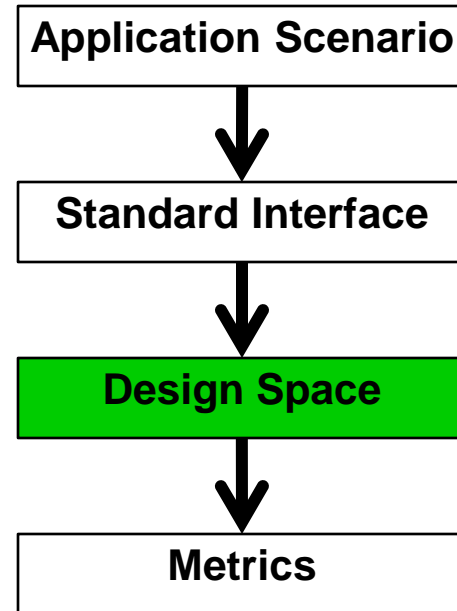
System Integrator

same interface?



❖ Define Design Space

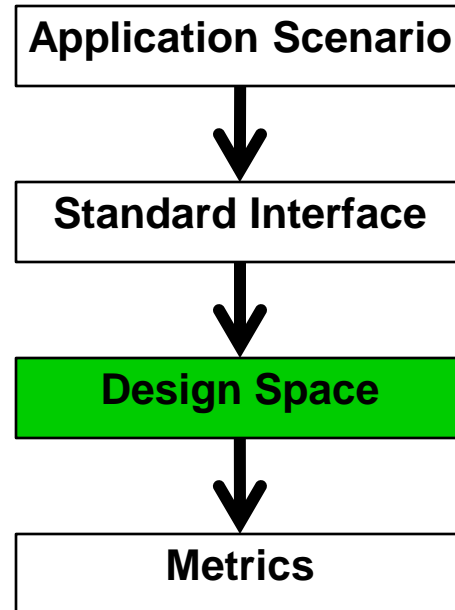
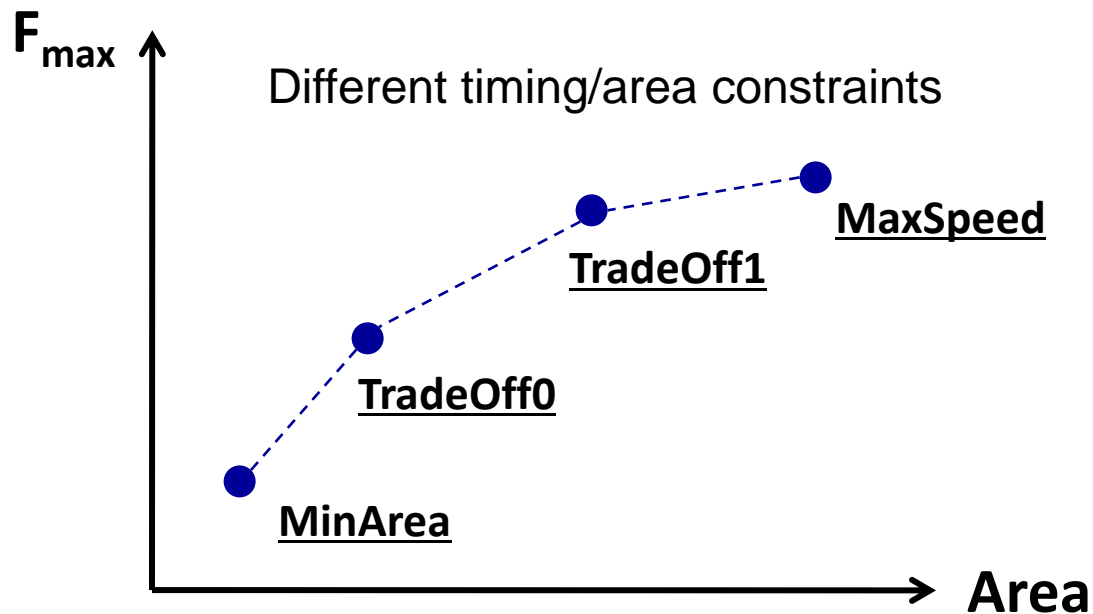
- **Design Abstraction Level**
 - RTL Level
- **Physical Implementation**
 - Different constraints for 4 trade-off points
- **Technology**
 - ASIC: UMC 130nm Standard Cell Library
 - FPGA: Xilinx 65nm Virtex-5 FPGA



❖ Define Design Space

▪ Physical Implementation

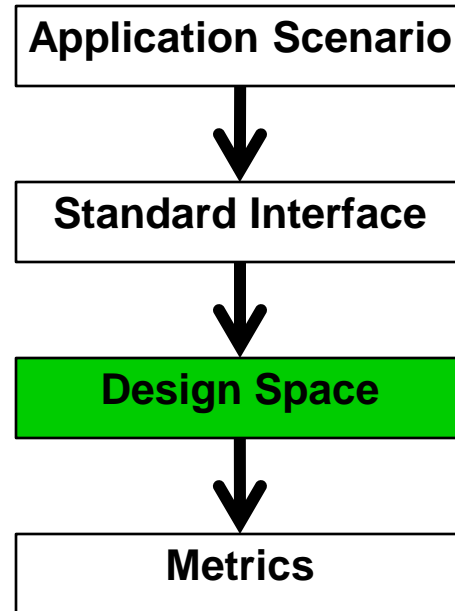
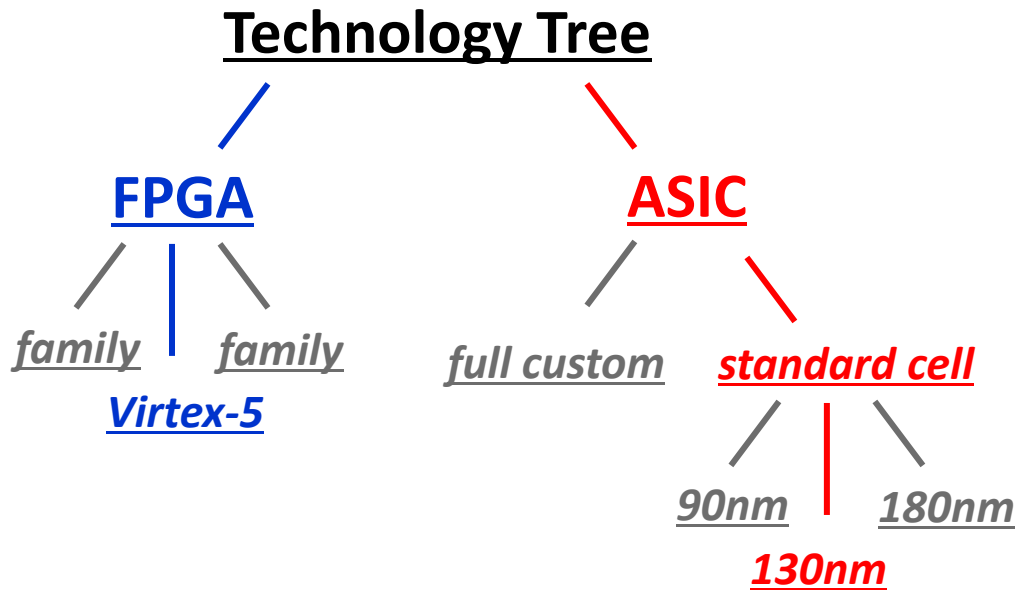
- Different constraints for 4 trade-off points



❖ Define Design Space

▪ Technology

- ASIC: UMC 130nm Standard Cell Library
- FPGA: Xilinx 65nm Virtex-5 FPGA



❖ Choose Metrics

▪ Basic Metrics

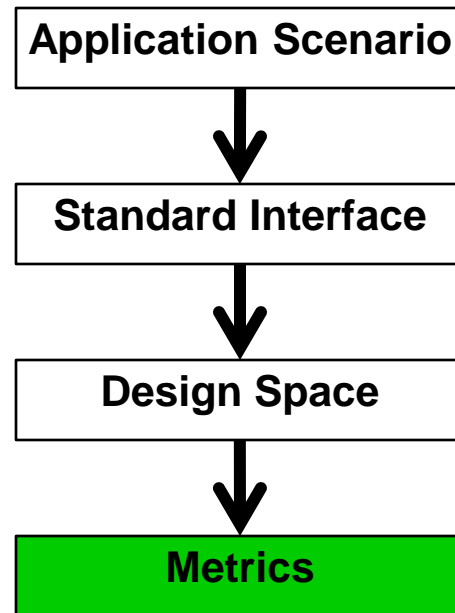
- Area, Throughput, Power

▪ Advanced Metrics

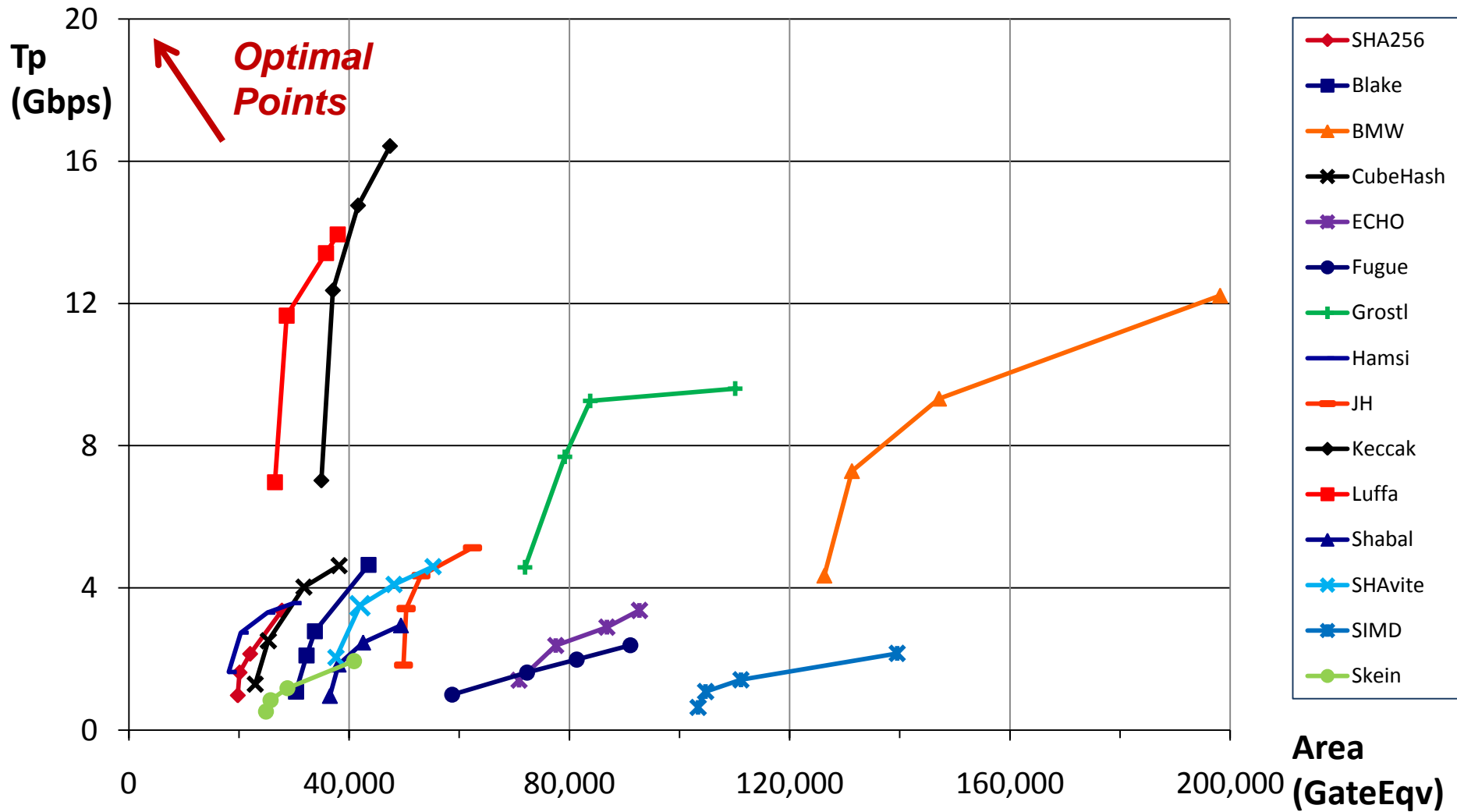
- Achievable Throughput per Area
- Power and Area under Fixed Throughput

❖ Issues

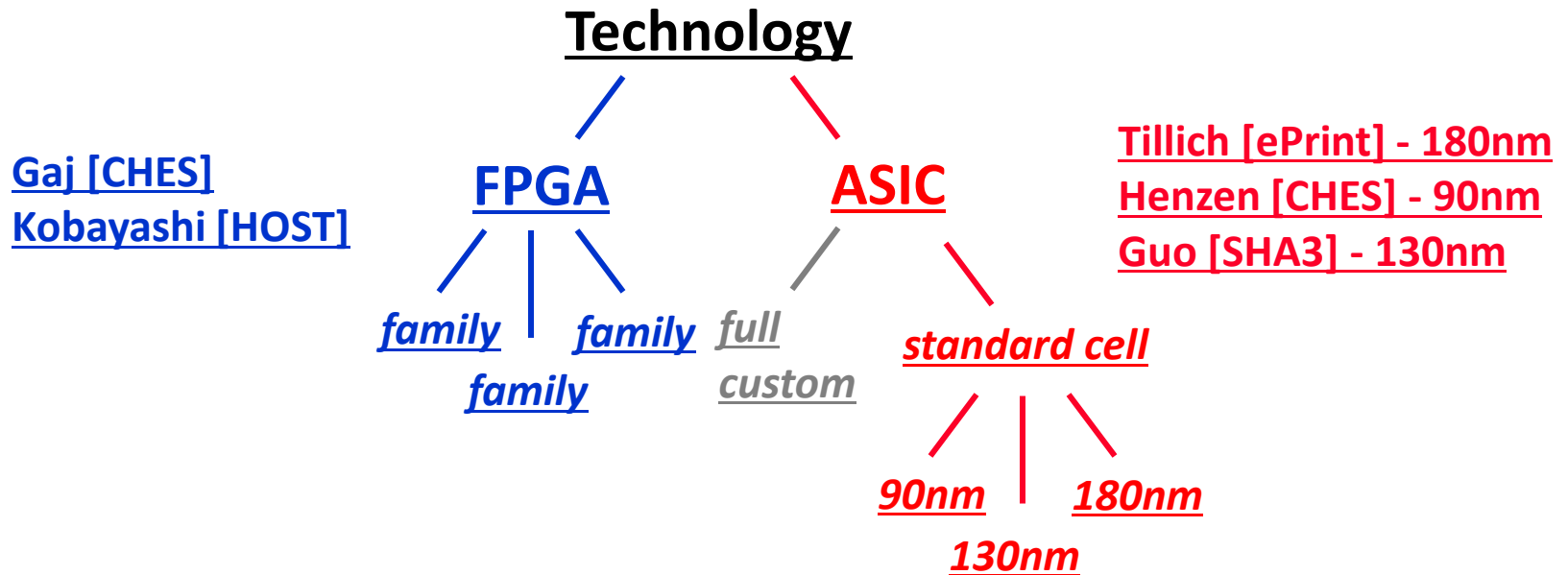
- Strong technology correlated metrics
- Strong algorithm correlated metrics



UMC 130nm Standard Cell Lib

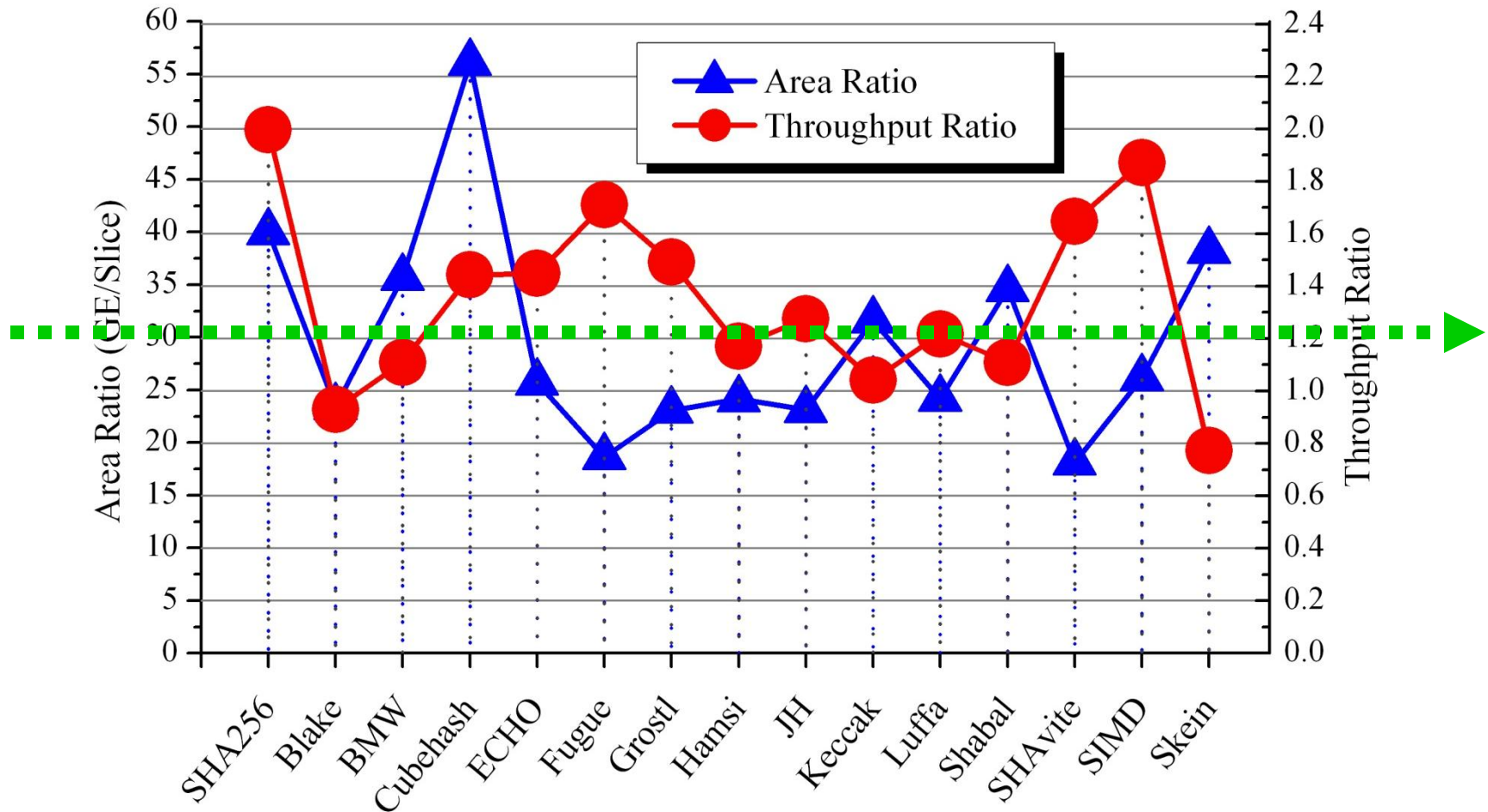


Comparison between FPGAs and ASICs



Is a ranking for FPGA compatible with a ranking in ASIC?

ASIC/FPGA Area and Achievable Throughput Ratio

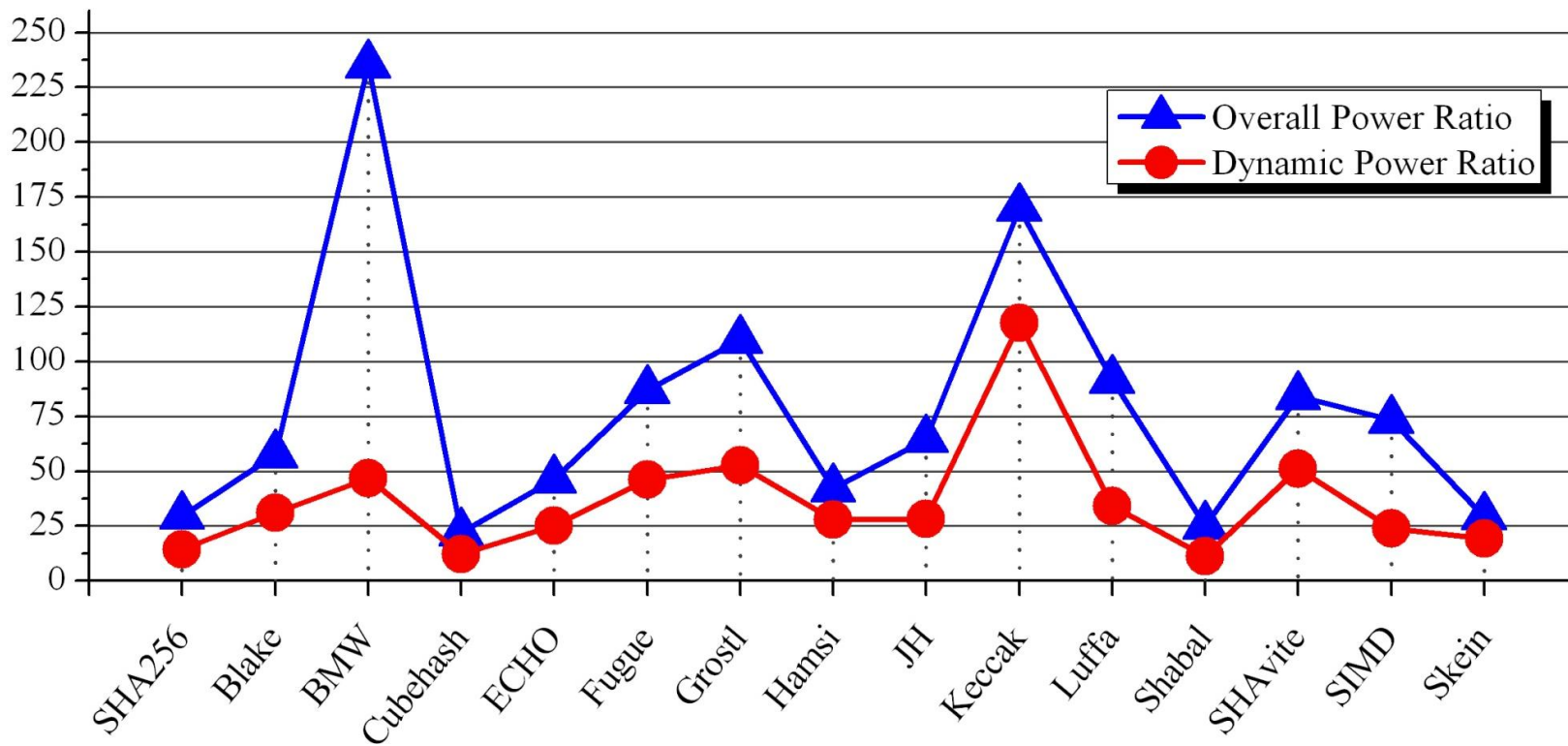


FPGA - Virtex5 65nm vs. ASIC - UMC 130nm

Area ratio range: 18.11 ~ 56.10 with *avg. 29.51*

Throughput ratio range: 0.77 ~ 2.0 with *avg. 1.35*

FPGA/ASIC Power Ratio



FPGA - Virtex5 65nm vs. ASIC - UMC 130nm

Overall Power ratio range: 21.92 ~ 235.20 with **avg. 77.75**

Dynamic Power ratio range: 11.23 ~ 117.53 with **avg. 36.05**

Percentage of Static power: FPGAs is 31% ~ 90%; ASICs is < 1%.

Dynamic power: the FPGAs still consume 36 times of ASIC power in average.

□ Introduction

- *Hash Definition and Applications*
- *SHA3 Competition*

□ Hardware Benchmarking Methodology

- *Related Work*
- *Application Scenario*
- *Interface*
- *Metrics*
- *Design Space*
- *Results*

□ Conclusions

- ❖ **Propose a methodology to perform SHA3 HW benchmarking**
- ❖ **Need more standardized procedures for HW benchmarking**
 - Avoid 'unrealistic' application scenario
 - Avoid 'uncommon' interface
 - Avoid 'unlimited' design space comparison
 - Avoid 'stretching technology too far'
- ❖ **Report 'meaningful' results and make 'precise' comparisons for hardware implementations**

❖ Future Work

- Detailed analysis of the inconsistent FPGA-to-ASIC gaps for different SHA3 candidates.
- Evaluation of the real system integration cost (Nallatech Server)
- SHA3-ASIC chip tape-out (1Q11).

NIST SHA3 Timeline

3Q10 Second Candidate Conference

4Q10 Announce finalist candidates

1Q11 Final tweaks of candidates

1Q12 Last Candidate Conference

2Q12 announce winner

4Q 12 FIPS package to Secretary of Commerce

Our Related Publications

1. X. Guo, S. Huang, L. Nazhandali, P. Schaumont, "Comparing SHA-3 Hardware Benchmarks on FPGA and ASIC", *submitted*.
2. Z. Chen, X. Guo, A. Sinha, P. Schaumont, "Data-Oriented Performance Analysis of SHA-3 Candidates on FPGA Accelerated Computers", *submitted*.
3. X. Guo, S. Huang, L. Nazhandali, P. Schaumont, "Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations", NIST 2nd SHA-3 Candidate Conference, Santa Barbara, CA, August 2010.
4. M. Shiichiro, K. Miroslav, P. Schaumont, I. Verbauwhede, A. Satoh, K. Sakiyama, K. Ota, "How Can We Conduct 'Fair and Consistent' Hardware Evaluation for SHA-3 Candidate?" NIST 2nd SHA-3 Candidate Conference, Santa Barbara, CA, August 2010.
5. K. Kobayashi, J. Ikegami, M. Knezevid, X. Guo, S. Matsuo, S. Huang, L. Nazhandali, U. Kocabas, J. Fan, A. Satoh, I. Verbauwhede, K. Sakiyama, K. Ota, "A Prototyping Platform for Performance Evaluation of SHA-3 Candidates", IEEE Intl. Symposium on Hardware-Oriented Security and Trust (HOST2010) , Jun. 2010.
6. X. Guo, "Benchmarking of Hardware Implementations of SHA-3 Candidates Using High Level Synthesis", Secure Embedded Systems Lab Technical Report, Mar. 2010.
7. Z. Chen, S. Morozov, P. Schaumont, "A Hardware Interface for Hashing Algorithms", ePrint IACR Archive, 2008/529, December 2008.