Environment for Fair and Comprehensive Performance Evaluation of Cryptographic Hardware and Software

ASIC Status Update

ECE Department, Virginia Tech

Faculty - Patrick Schaumont, Leyla Nazhandali

Students - Xu Guo, Sinan Huang, Meeta Srivastav

9 November 2010

VirginiaTech
Invent the Future

Outline

- Evaluation of SHA3 Candidates in ASIC
  - Evaluation in 130m
  - Impact of technology and RTL
- Hardware Metrics for Ranking
  - Survey of commonly used technologies
  - Impact of technology (FPGA/ASIC) on ranking
- ASIC Chip Planning
  - Architecture Design
  - Test Plan
  - Tape-out Timeline
  - ASIC Cost Estimate

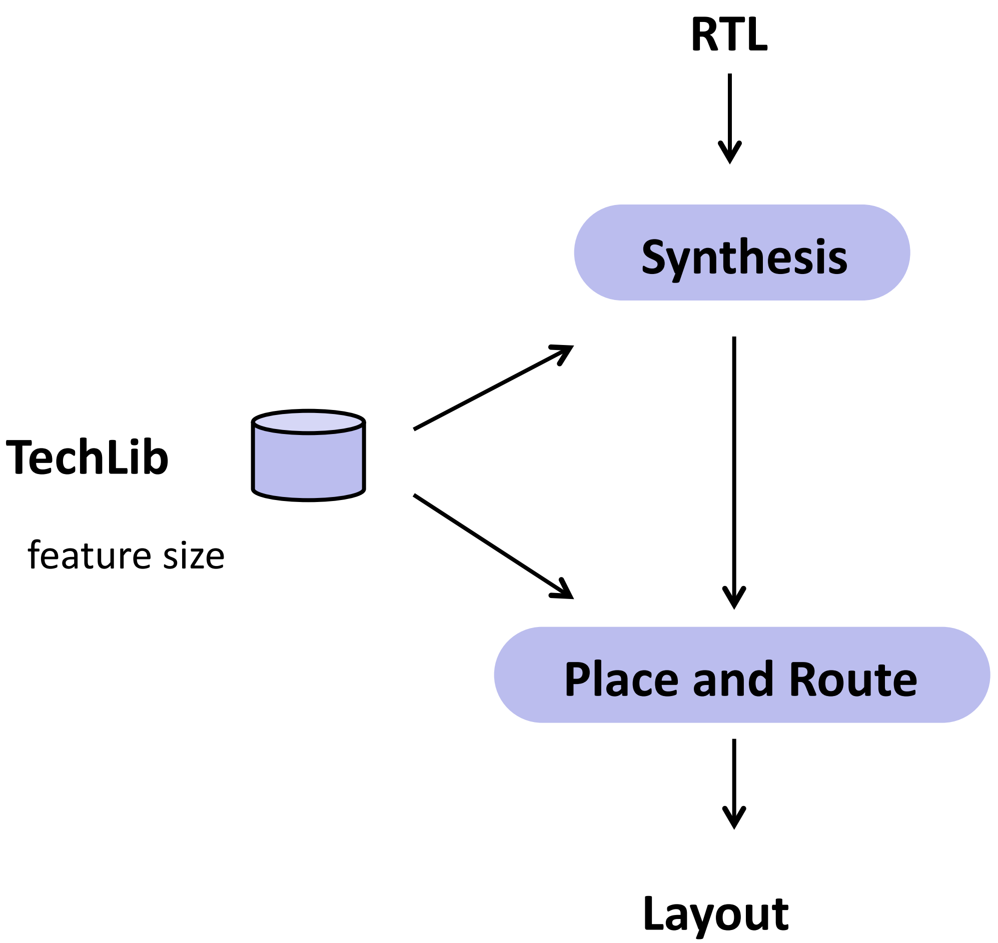
Main References

[1] K. Kobayashi, J. Ikegami, M. Knezevic, 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 International Symposium on Hardware-Oriented Security and Trust (HOST2010) , Jun. 2010. http://filebox.vt.edu/users/xuguo/homepage/publications/HOST10sha3.pdf

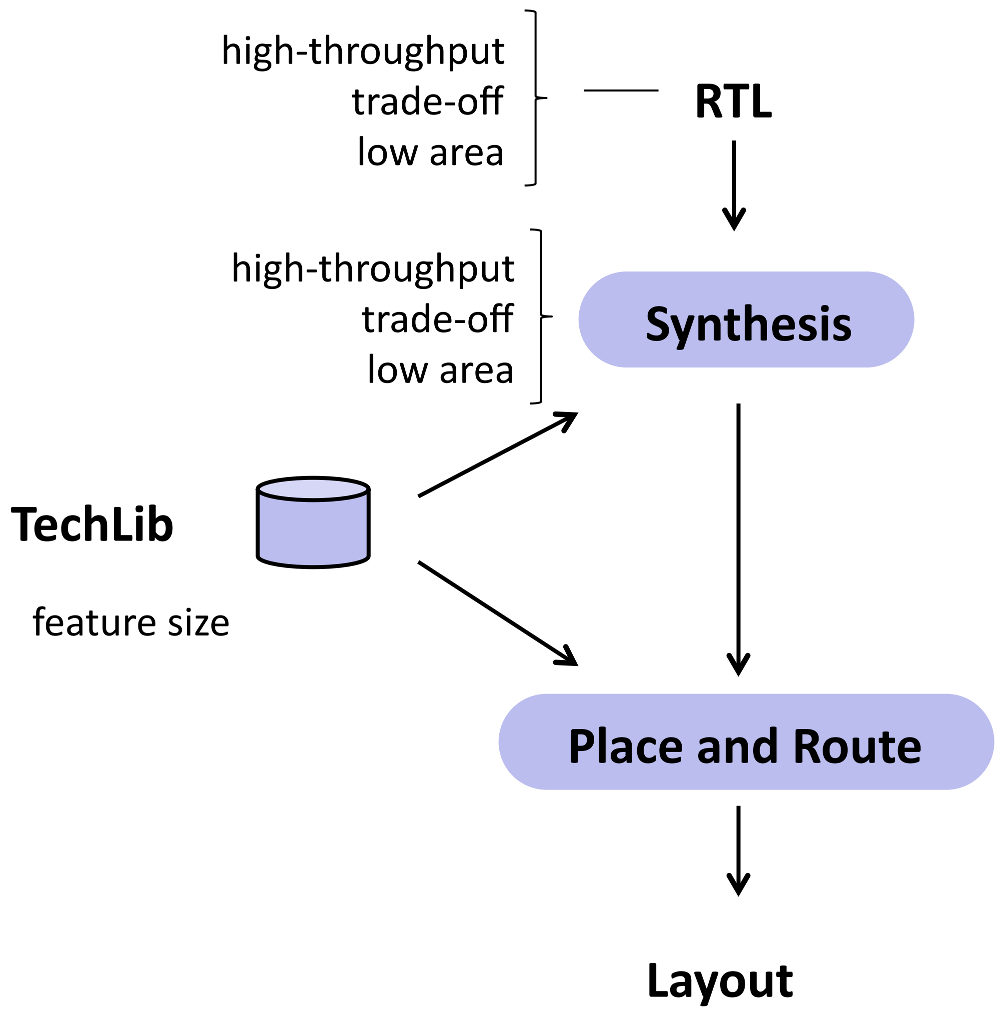
[2] X. Guo, S. Huang, L. Nazhandali, P. Schaumont, "Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations", NIST 2nd SHA-3 Candidate Conference, Santa Barbara, CA, August 2010. http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/SCHAUMONT_SHA3.pdf

[3] X. Guo, S. Huang, L. Nazhandali, P. Schaumont, "On The Impact of Target Technology in SHA-3 Hardware Benchmark Rankings," IACR ePrint 2010/536, October 2010. http://eprint.iacr.org/2010/536.pdf

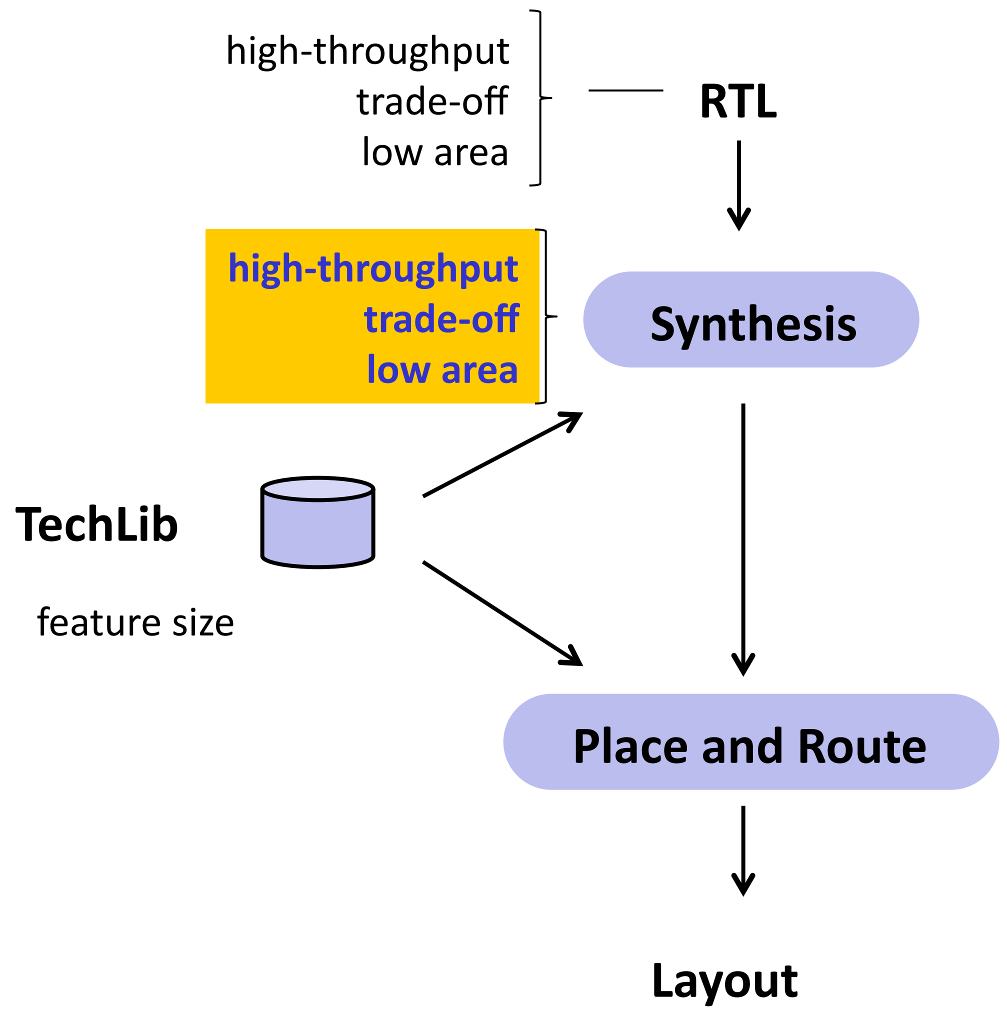
ASIC Evaluation



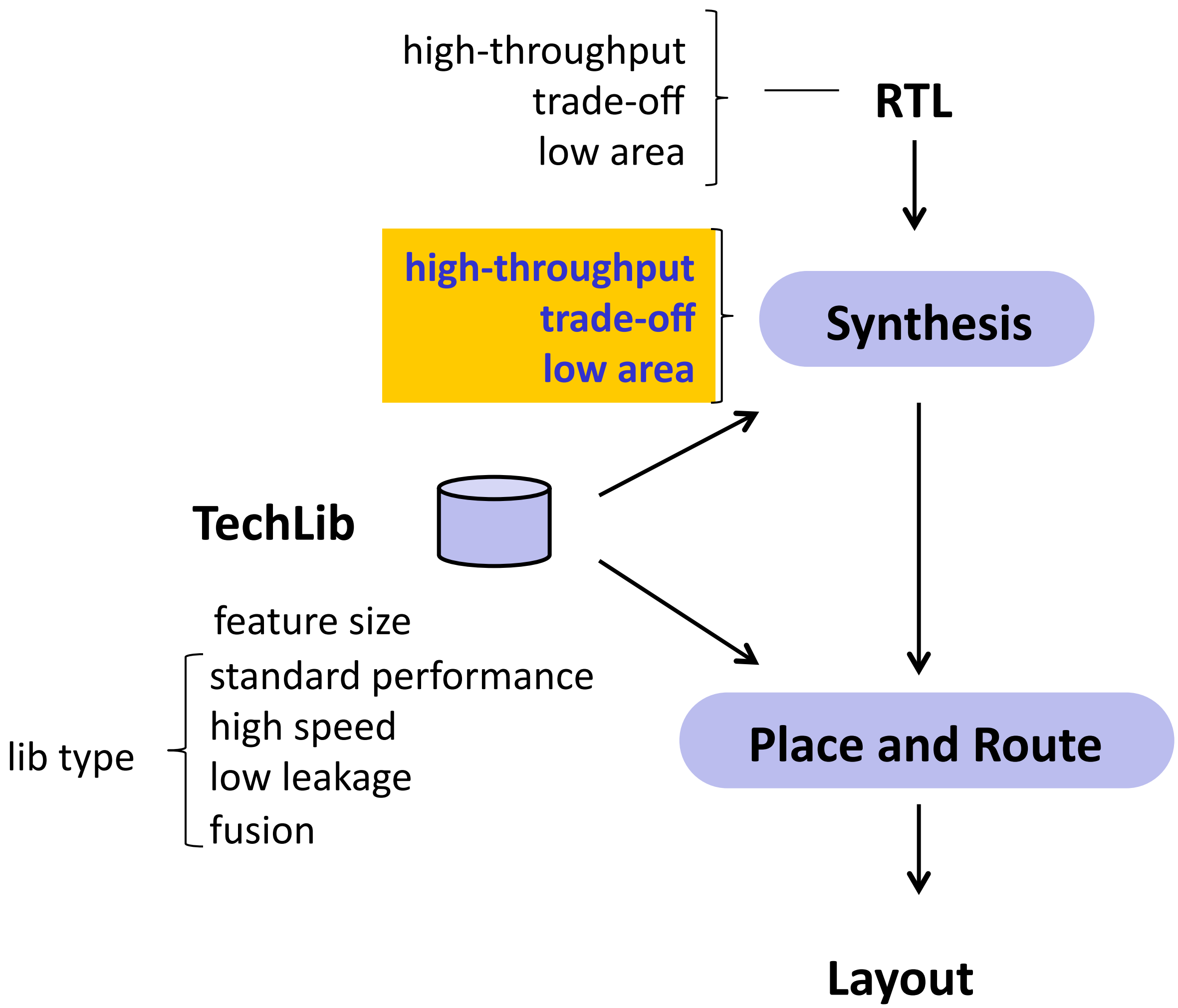
ASIC Evaluation



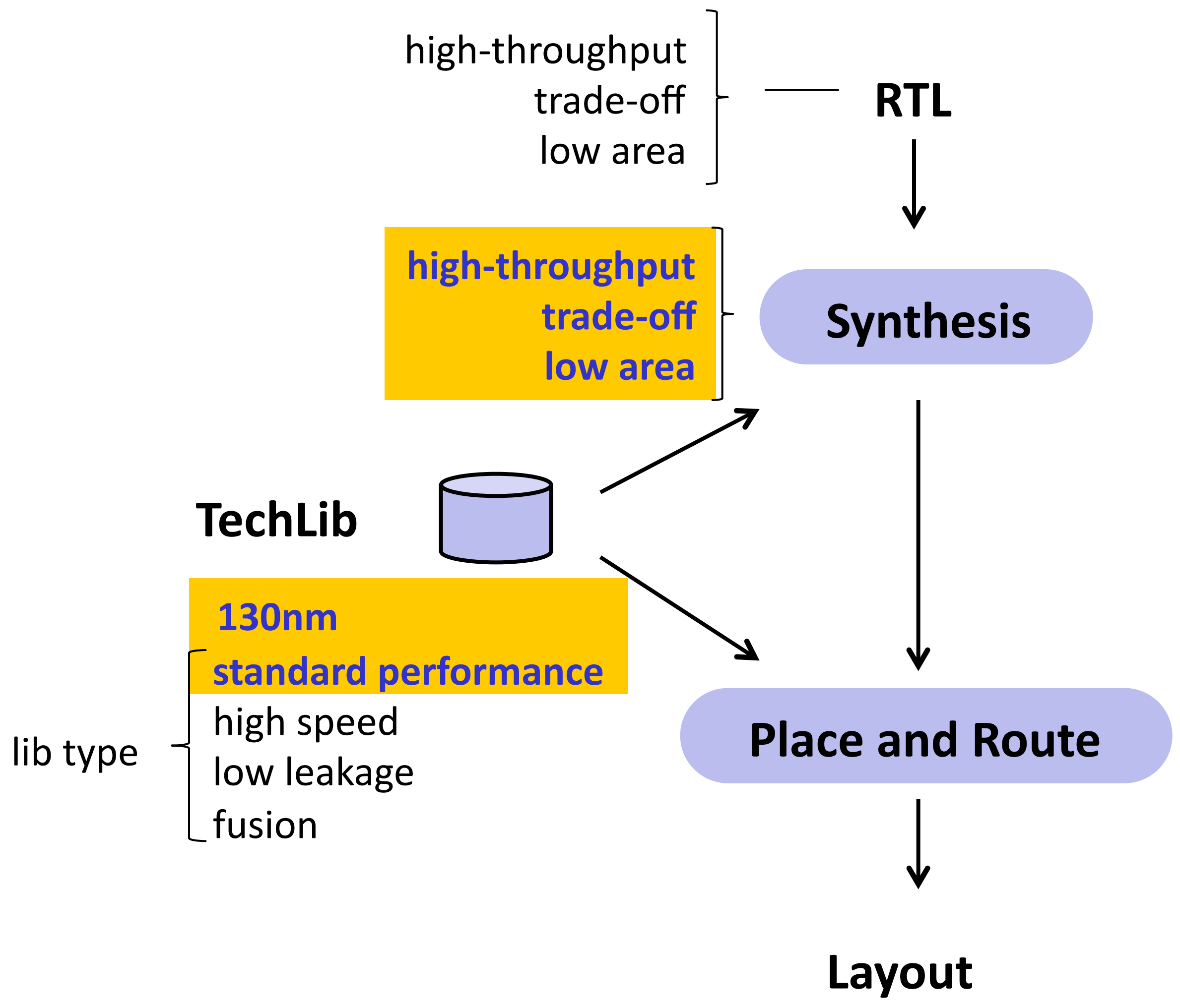
ASIC Evaluation



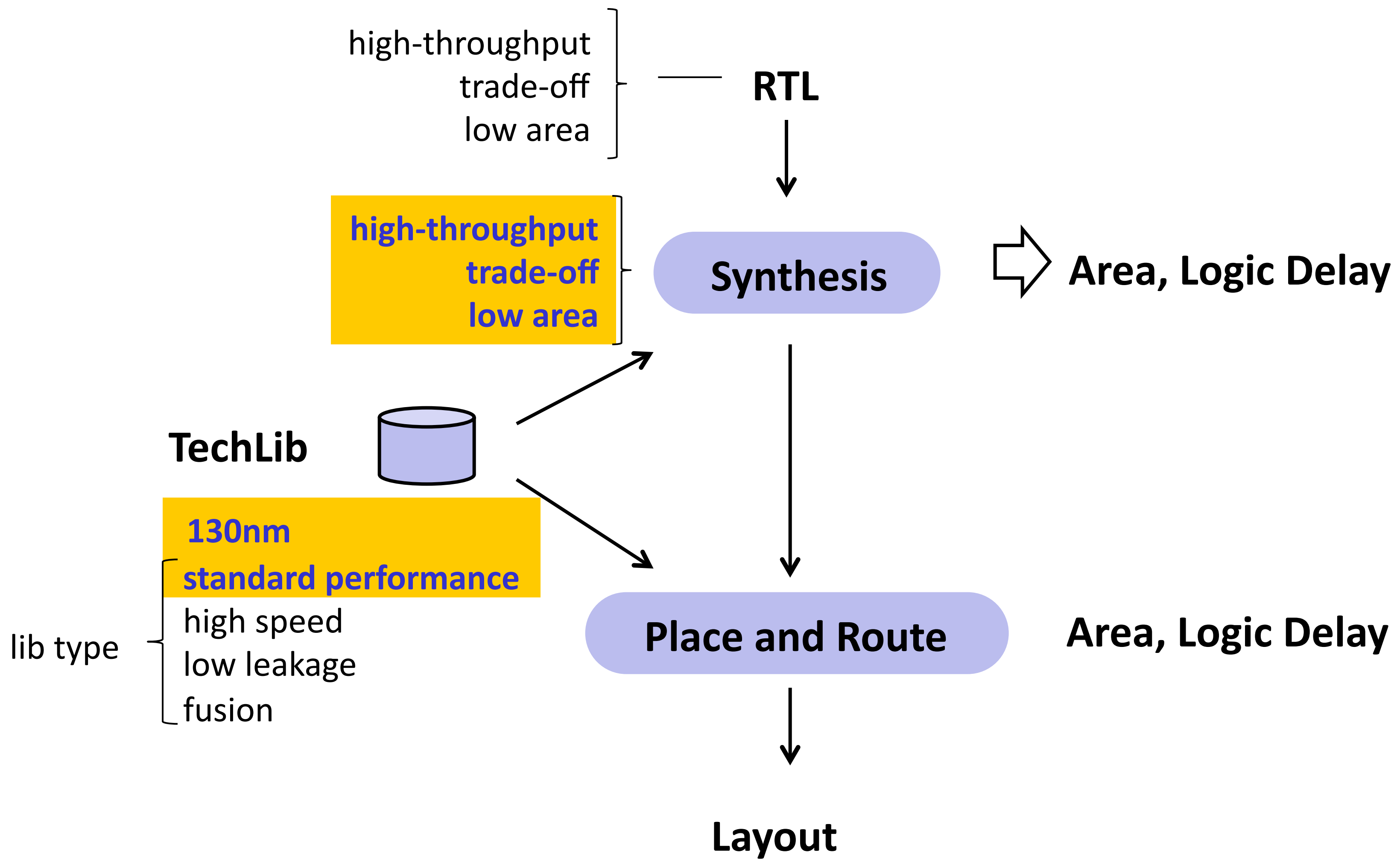
ASIC Evaluation



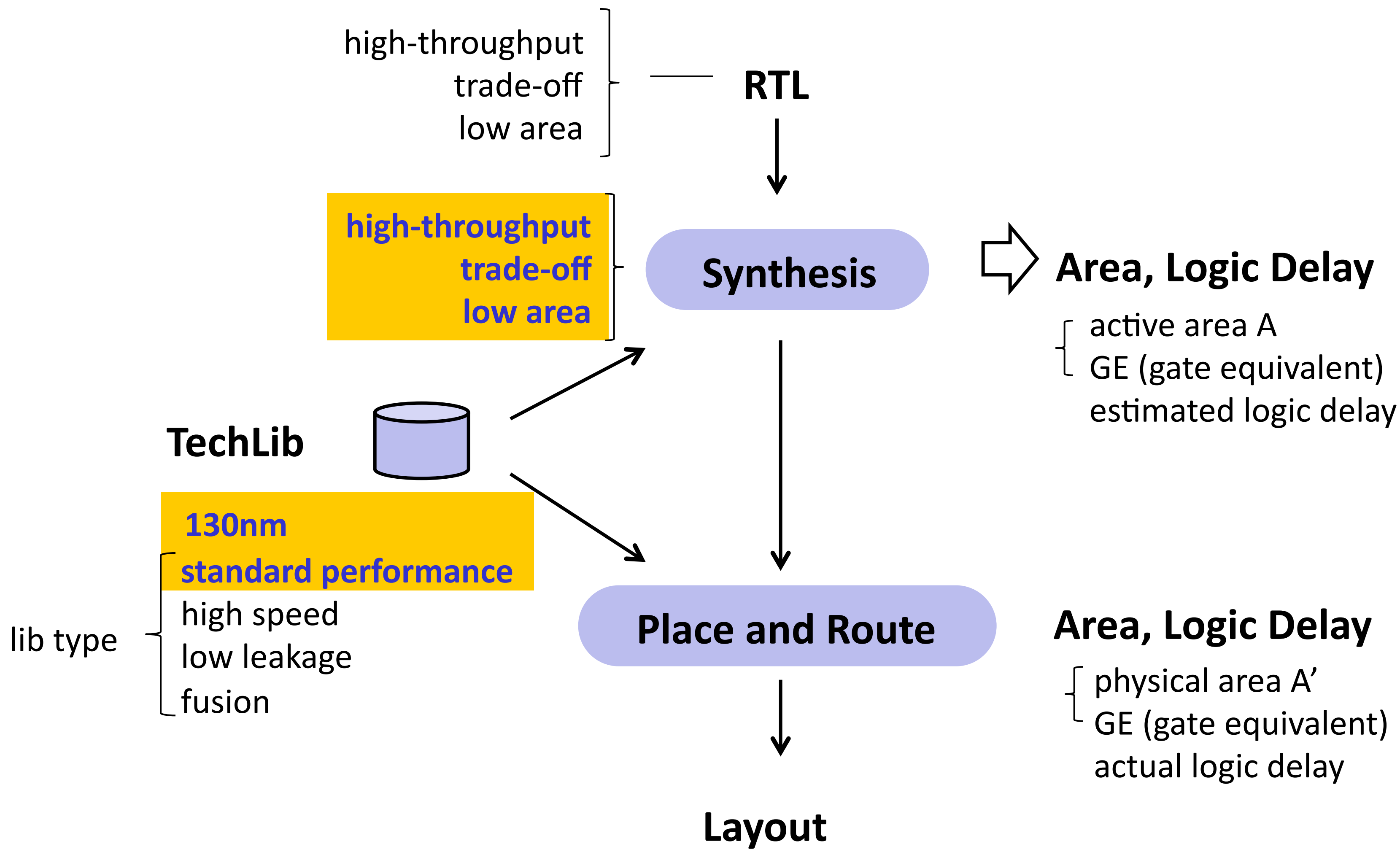
ASIC Evaluation



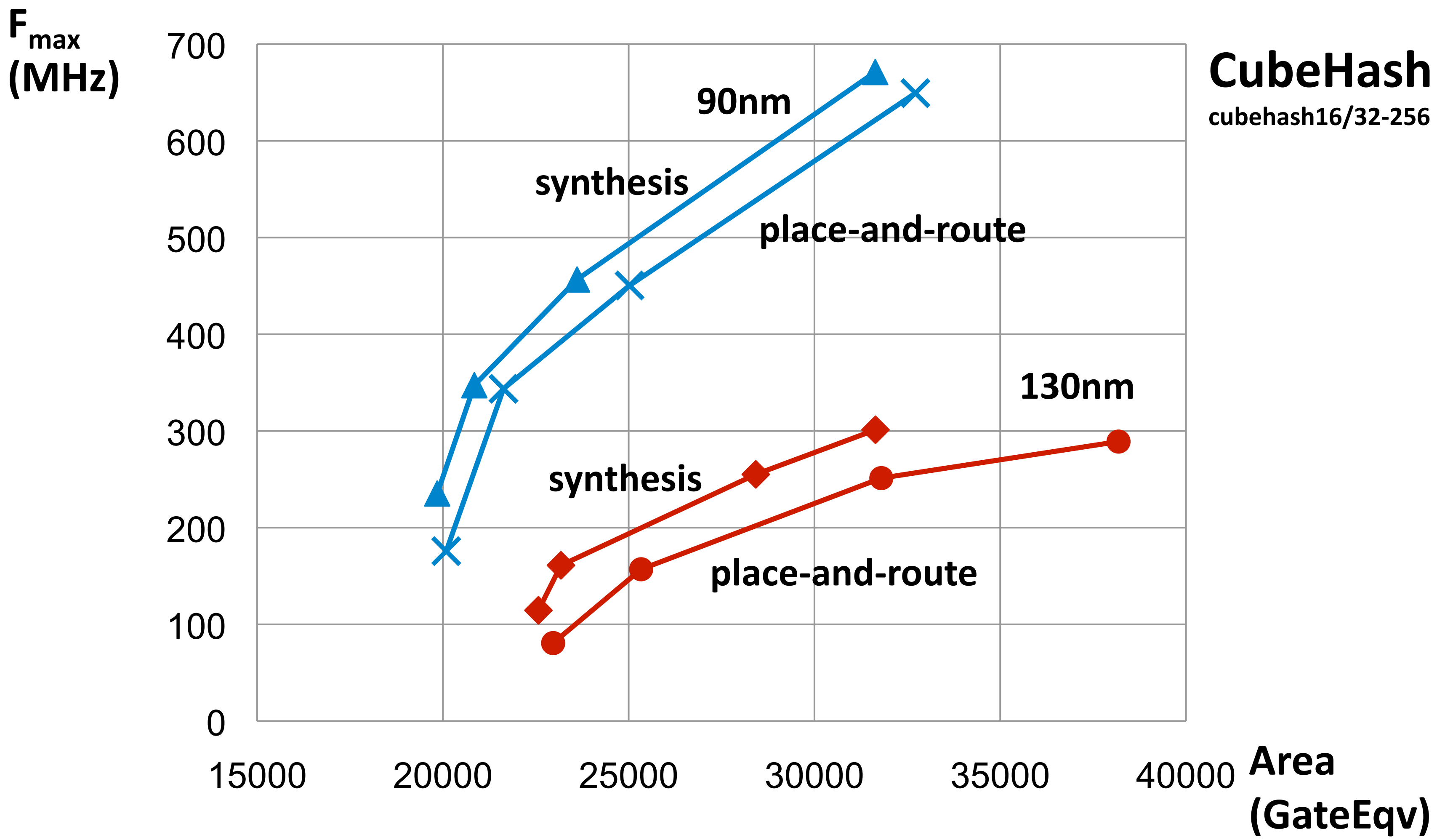
ASIC Evaluation



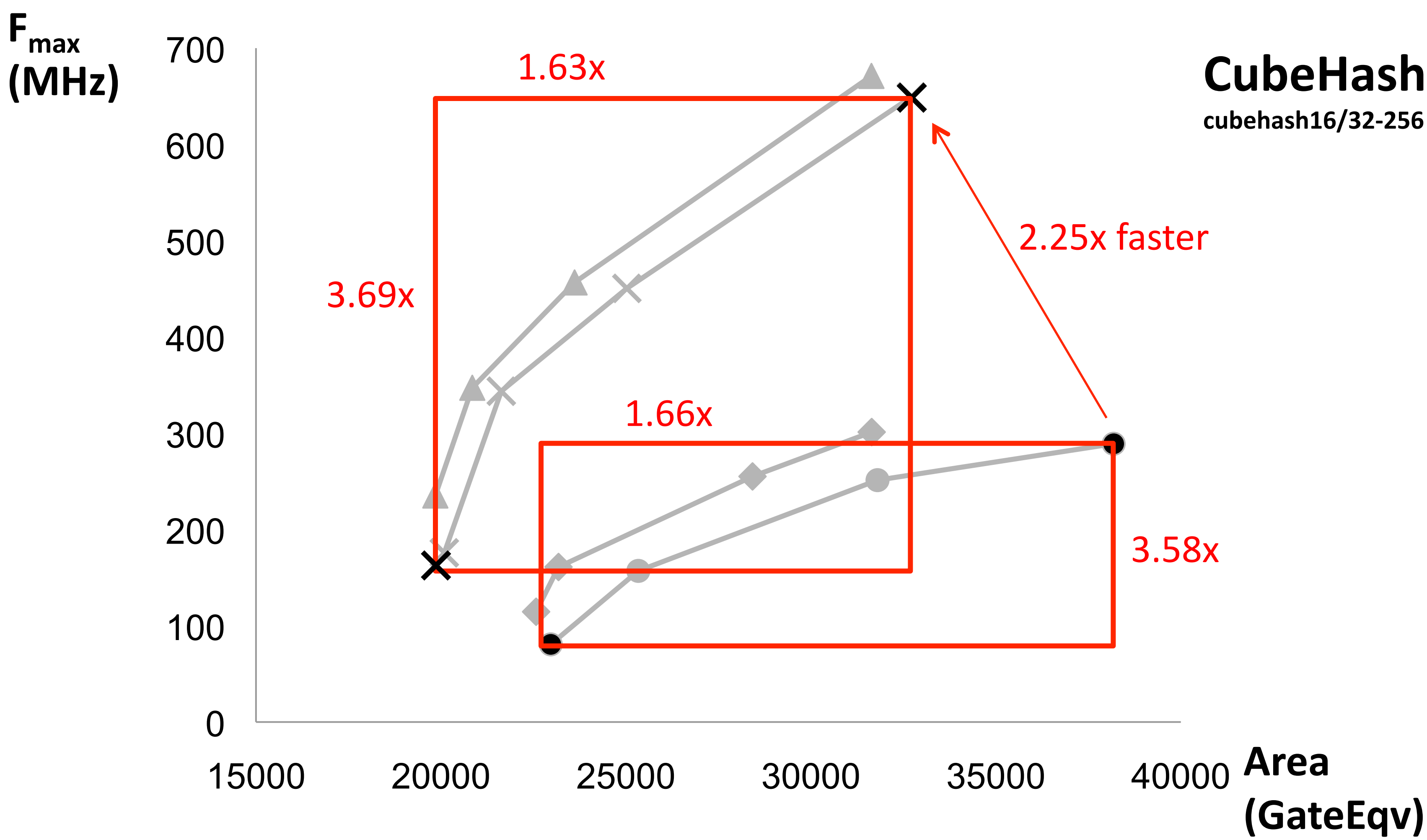
ASIC Evaluation



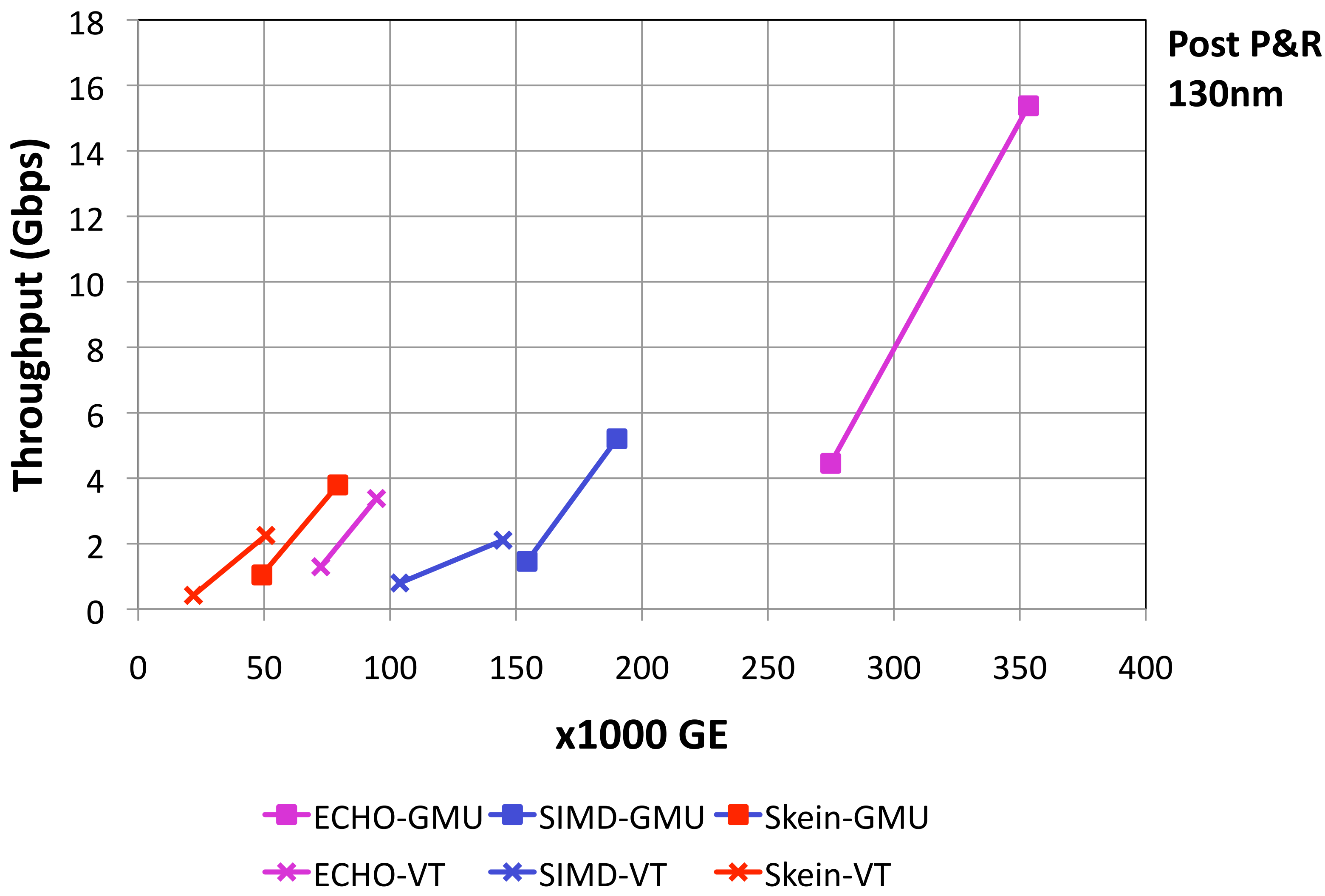
Influence of Technology



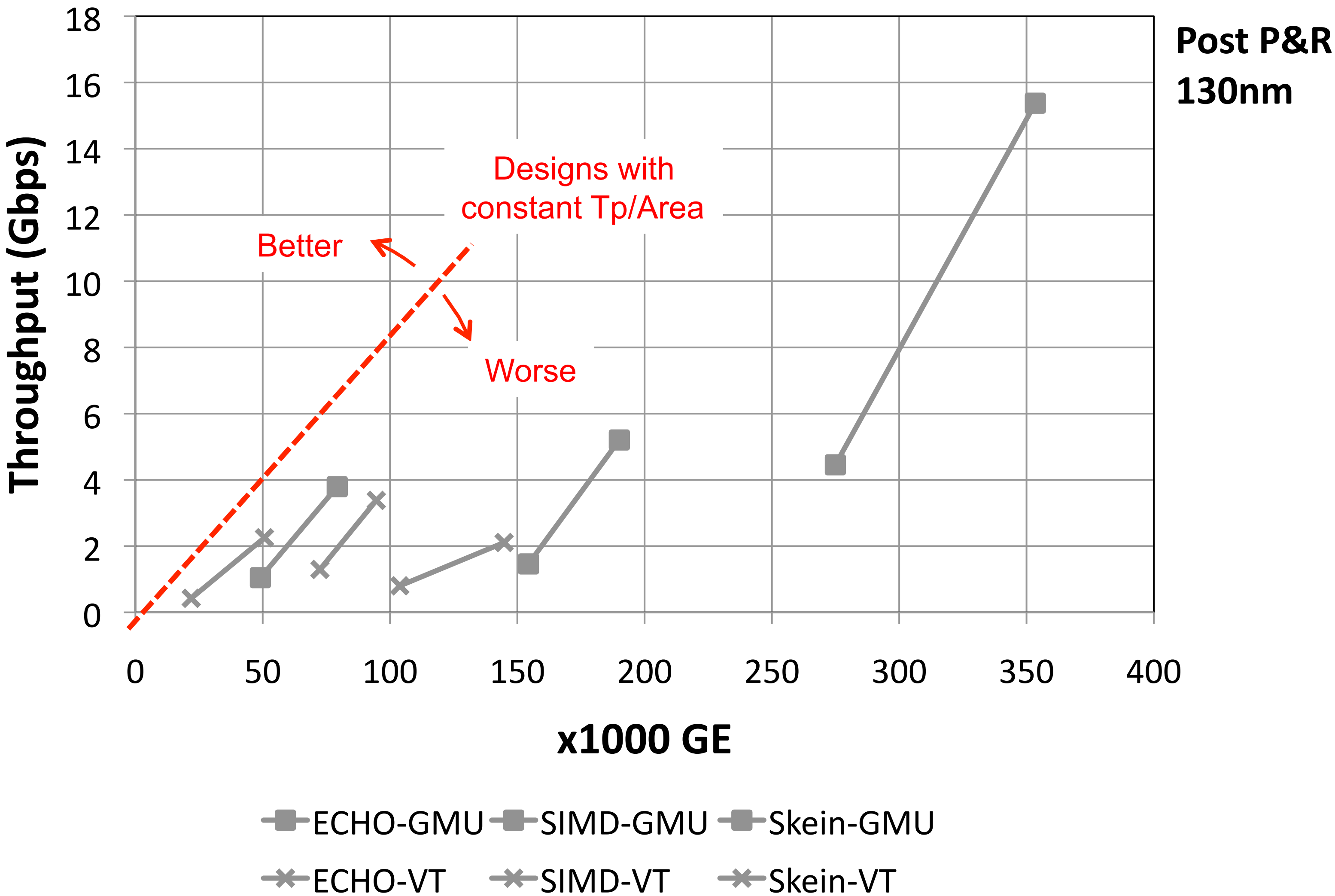
Influence of Technology



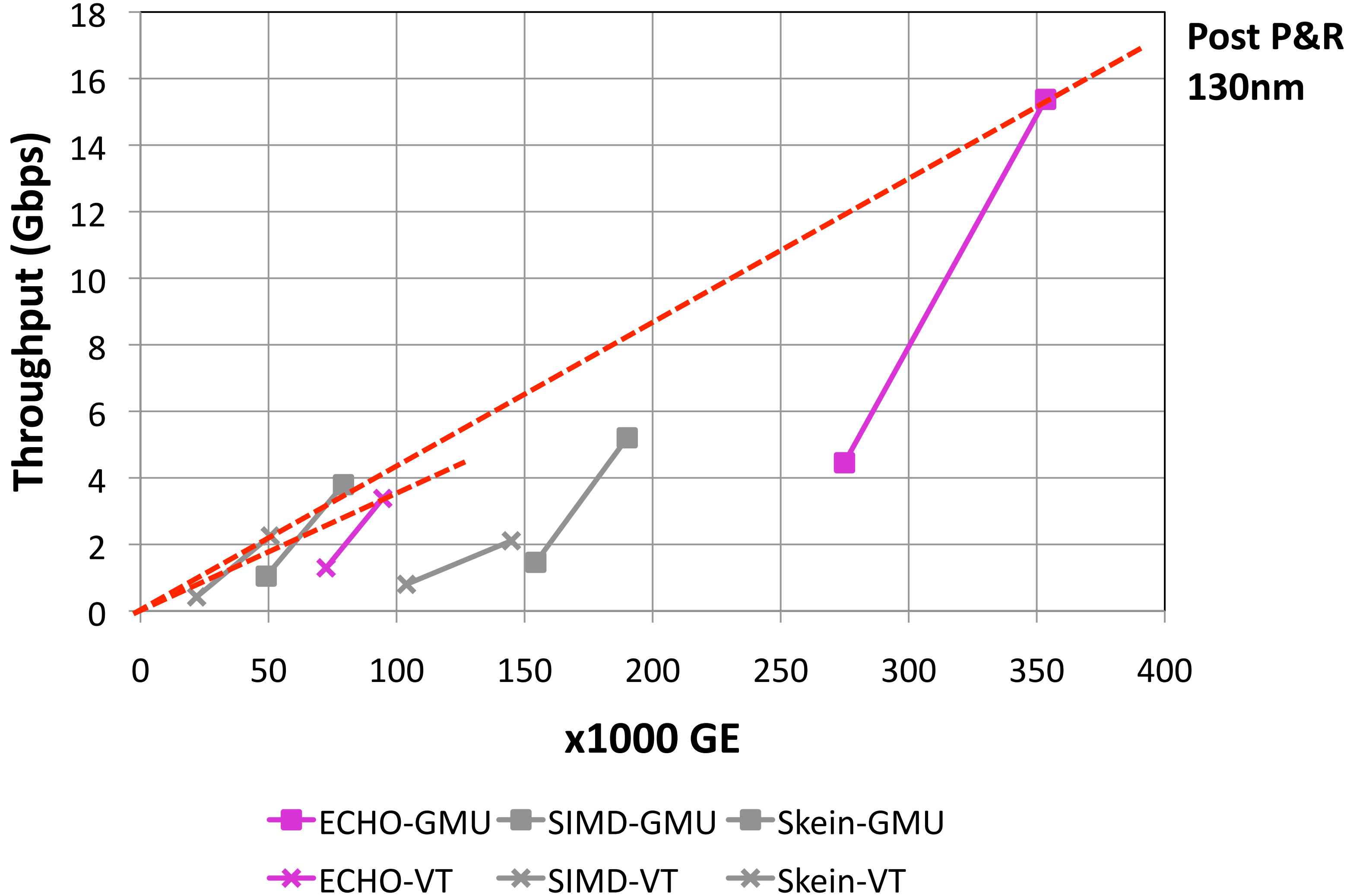
Influence of RTL



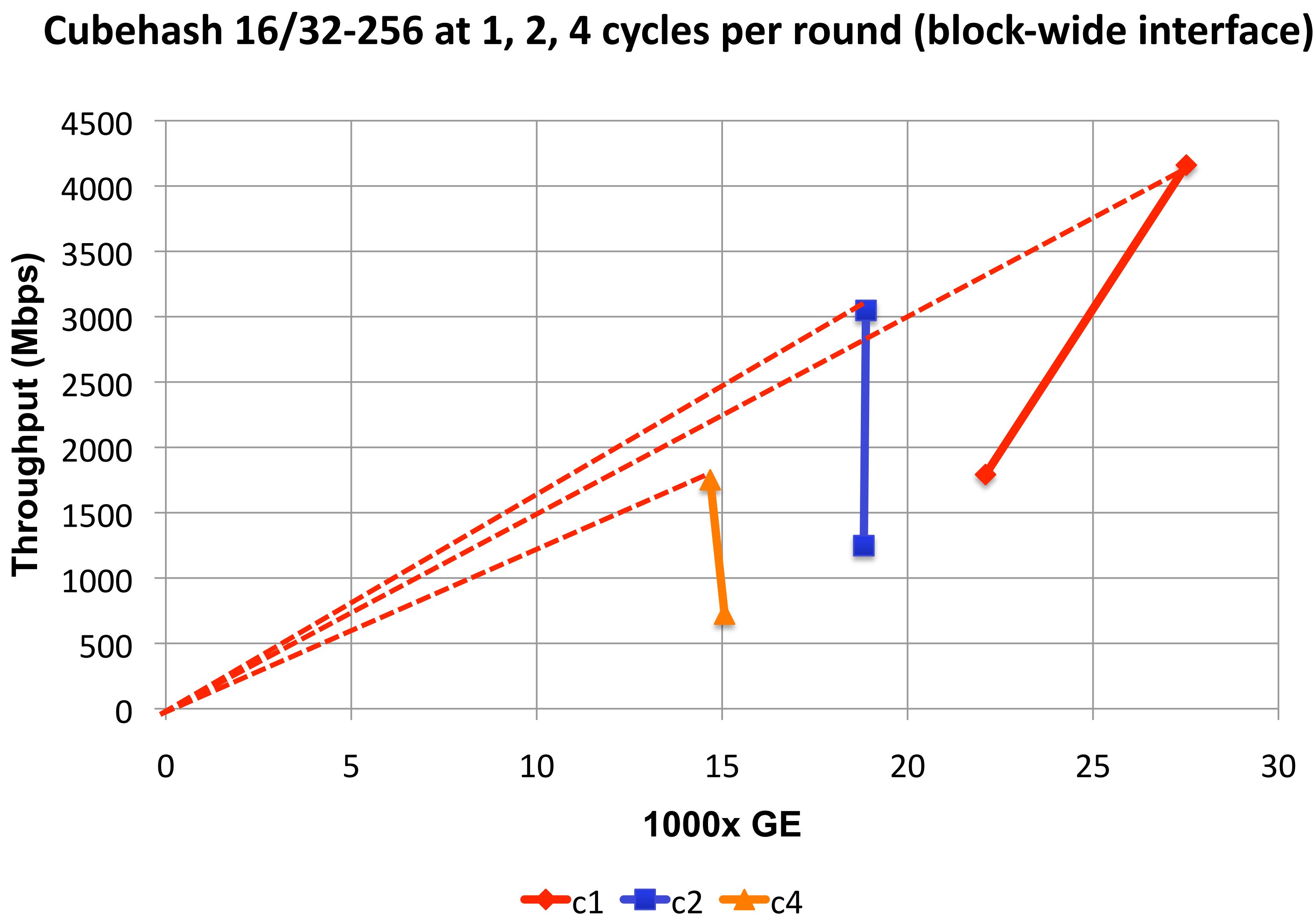
Influence of RTL



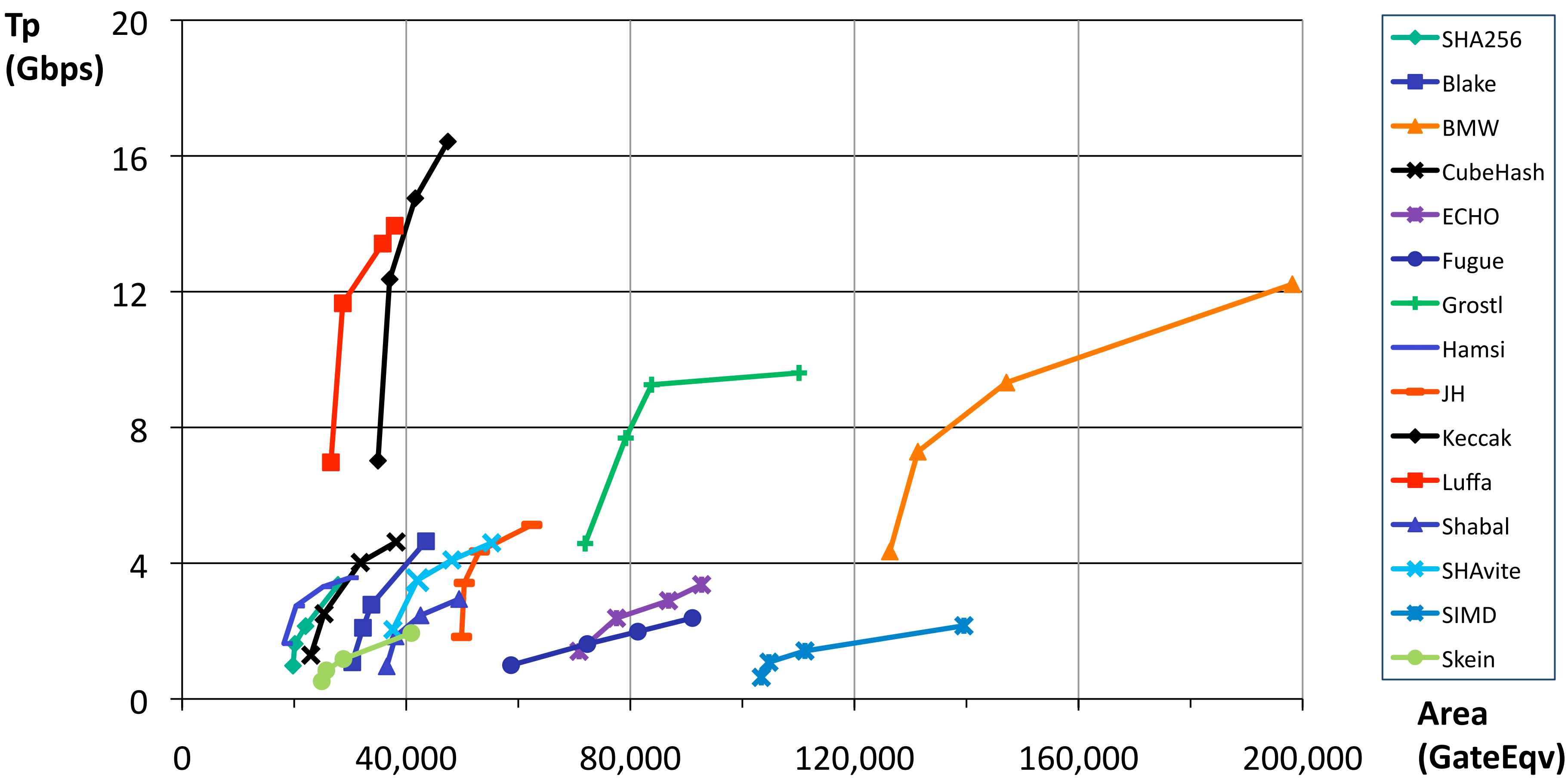
Influence of RTL



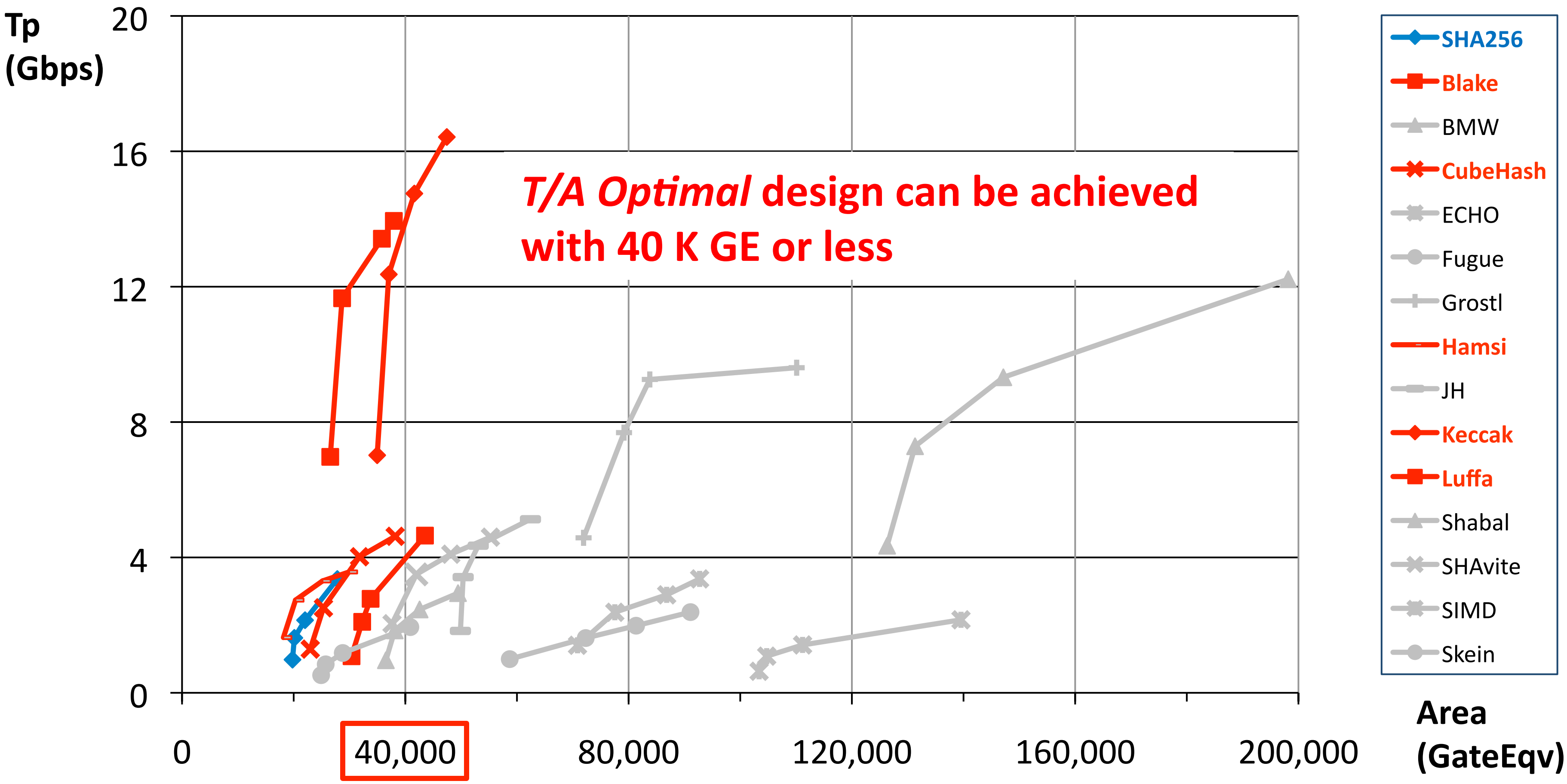
Influence of RTL



Post-P&R Results for ASIC 130nm



Post-P&R Results for ASIC 130nm



Influence of RTL

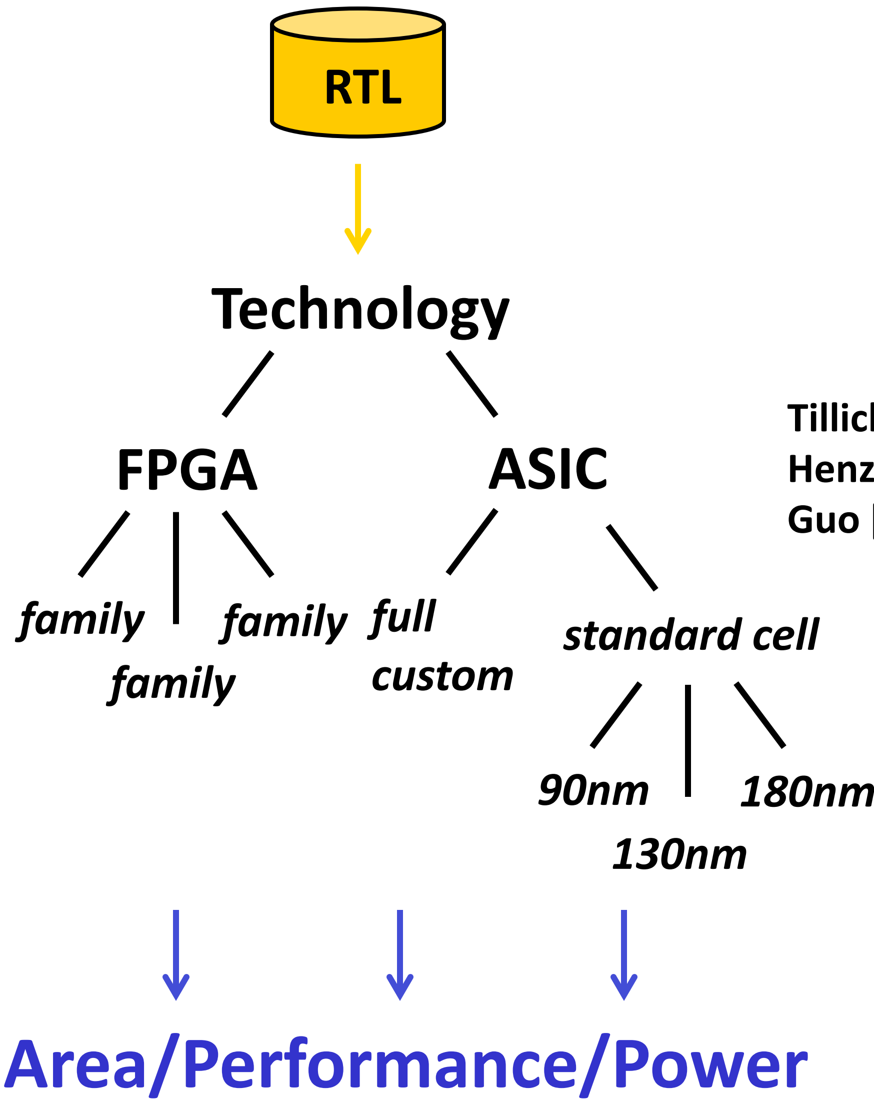
- Impact of RTL optimizations will be as high as the impact of logic synthesis optimization
- For our ASIC, we will give preference to implementations with a higher throughput/area ratio

Outline

- **Evaluation of SHA3 Candidates in ASIC**
  - **Evaluation in 130m**
  - **Impact of technology and RTL**
- **Hardware Metrics for Ranking**
  - **Survey of commonly used technologies**
  - **Impact of technology (FPGA/ASIC) on ranking**
- **ASIC Chip Planning**
  - **Architecture Design**
  - **Test Plan**
  - **Tape-out Timeline**
  - **ASIC Cost Estimate**

How does technology influence a ranking?

Gaj [CHES]
Kobayashi [HOST]
Baldwin [SHA3]



Tillich [ePrint] - 180nm
Henzen [CHES] - 90nm
Guo [SHA3] - 130nm

Common Crypto HW Technologies

Published SHA designs (2005 – present) in SHA3-Zoo, CHES, IACR ePrint

	65nm	90nm	130nm	180nm	350nm
FPGA	50	31	9	0	0
ASIC	0	8	20	29	4

ASIC standard-cell technology nodes lag FPGA technology nodes

We compared 65nm FPGA (Xilinx Virtex-5) with 130nm ASIC (UMC)

What is known about the FPGA/ASIC gap? [Kuon & Rose 2007]

90nm FPGA vs *90nm* ASIC: 18X..35X Area

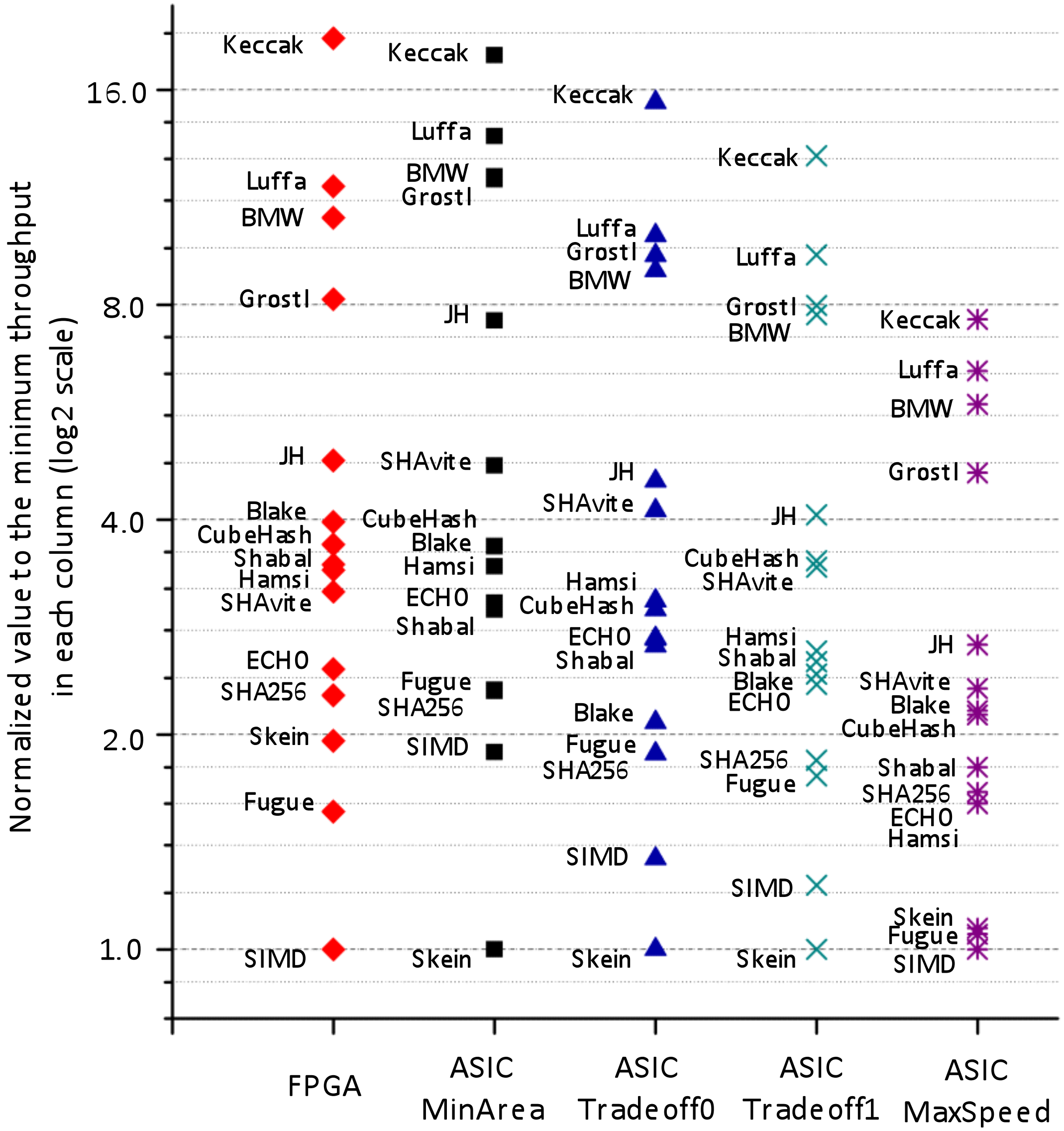
3X..4X Performance

14X Dynamic Power

Metrics

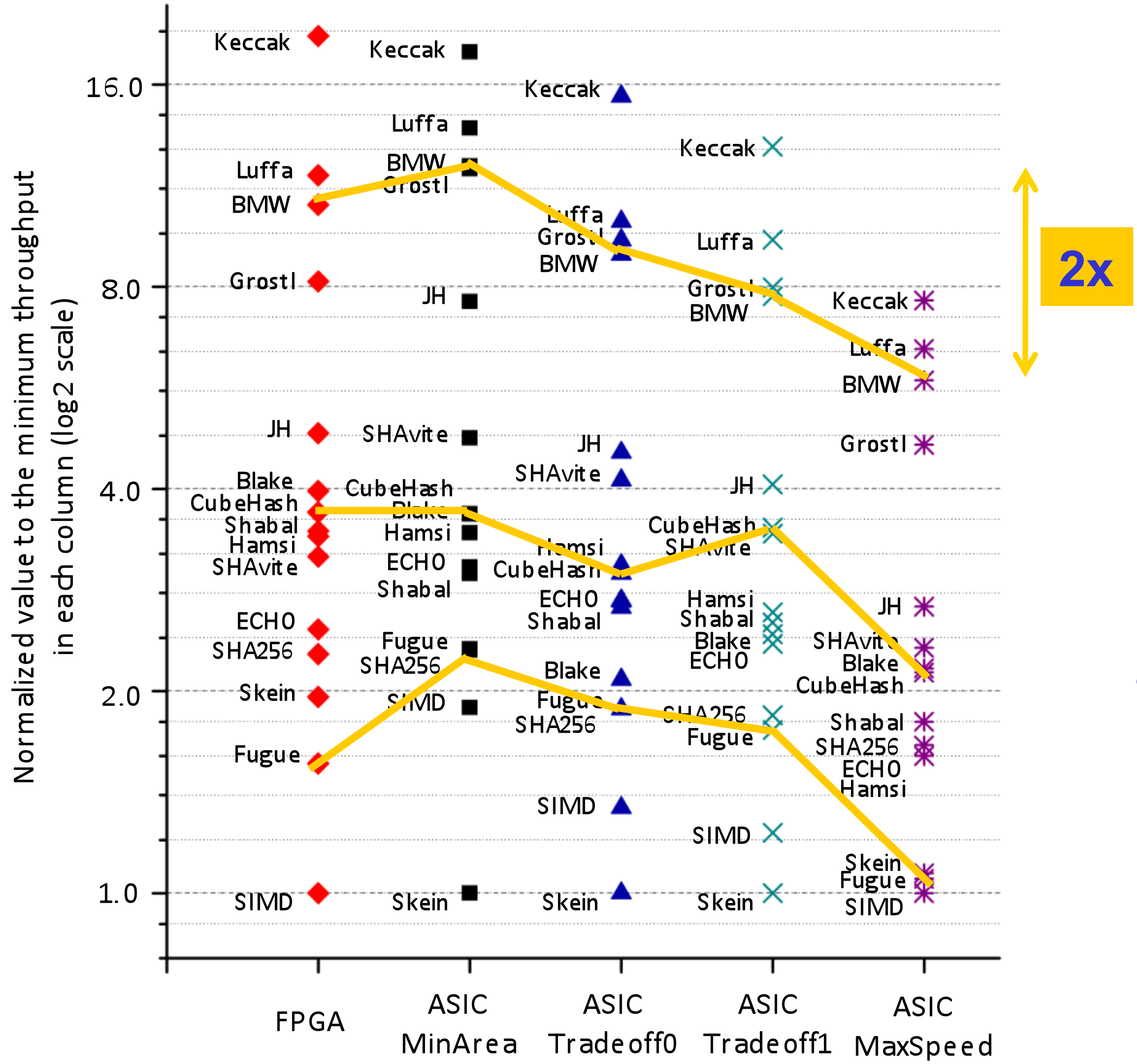
- For a given RTL implementation
  - Implement the design in Virtex-5 VLX30-3 (LUT-only synthesis)
  - Implement the design in ASIC 130nm (standard-logic library)
- Determine, for each design
  - **Throughput**
  - Throughput/Area
  - Area and **Power** Dissipation at a fixed throughput (0.2 Gbps)
- Scripts and source code online at `http://rijndael.ece.vt.edu/sha3`

Throughput



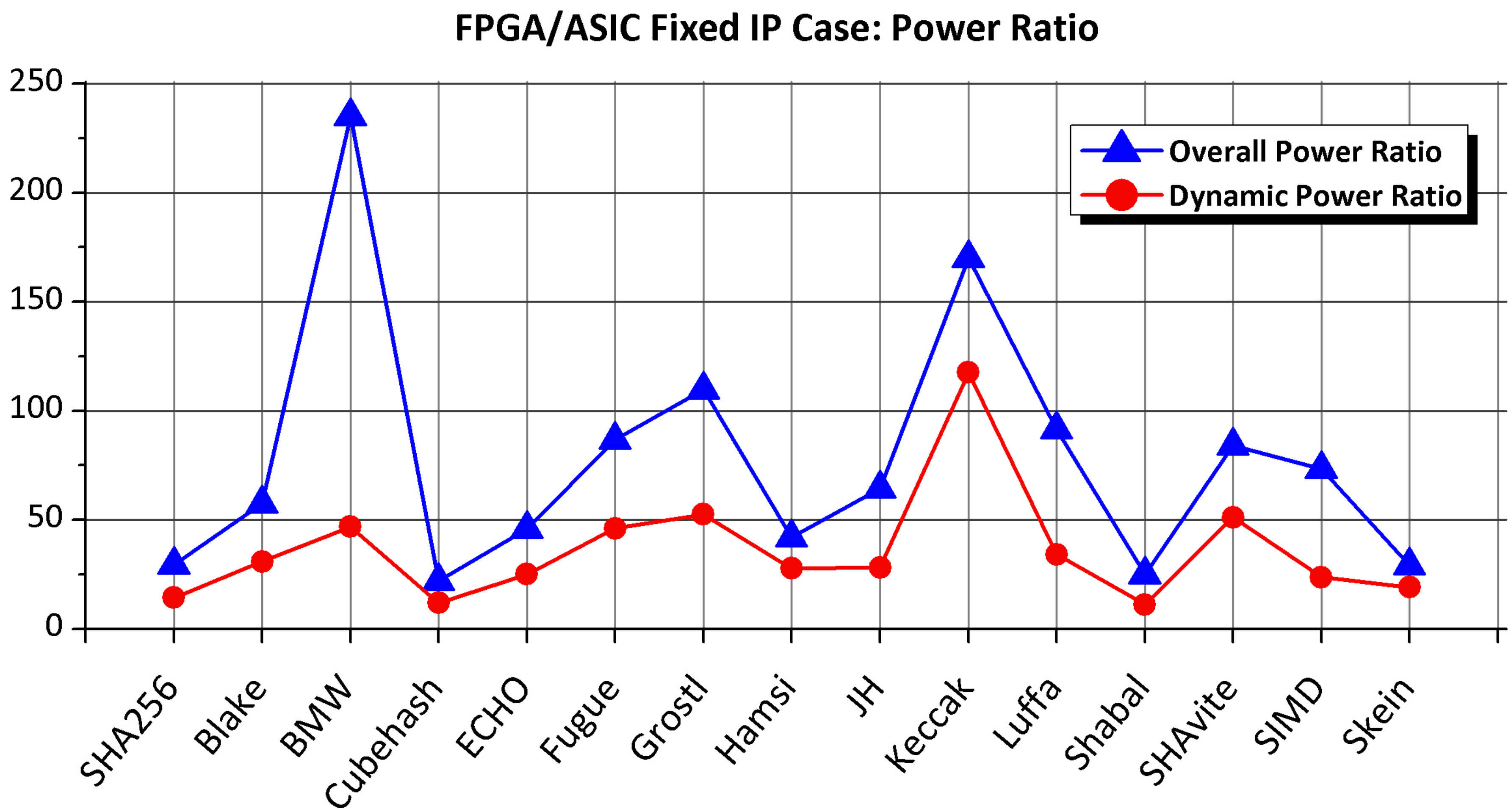
Normalized value to the minimum throughput in each column (log2 scale)
16.0
8.0
4.0
2.0
1.0
FPGA
ASIC MinArea
ASIC Tradeoff0
ASIC Tradeoff1
ASIC MaxSpeed
Keccak
Luffa
BMW
Grostl
JH
Blake
CubeHash
Shabal
Hamsi
SHAvite
ECHO
SHA256
Skein
Fugue
SIMD

Throughput



generally, variations remain less than a factor 2X

ASIC to FPGA: Power



Variations are significantly higher than a factor 2X

Outline

- Evaluation of SHA3 Candidates in ASIC
  - Evaluation in 130m
  - Impact of technology and RTL
- Hardware Metrics for Ranking
  - Survey of commonly used technologies
  - Impact of technology (FPGA/ASIC) on ranking
- ASIC Chip Planning
  - Test Plan
  - Architecture Design
  - Tape-out Timeline
  - ASIC Cost Estimate

ASIC Prototype - Est. Gate Complexity

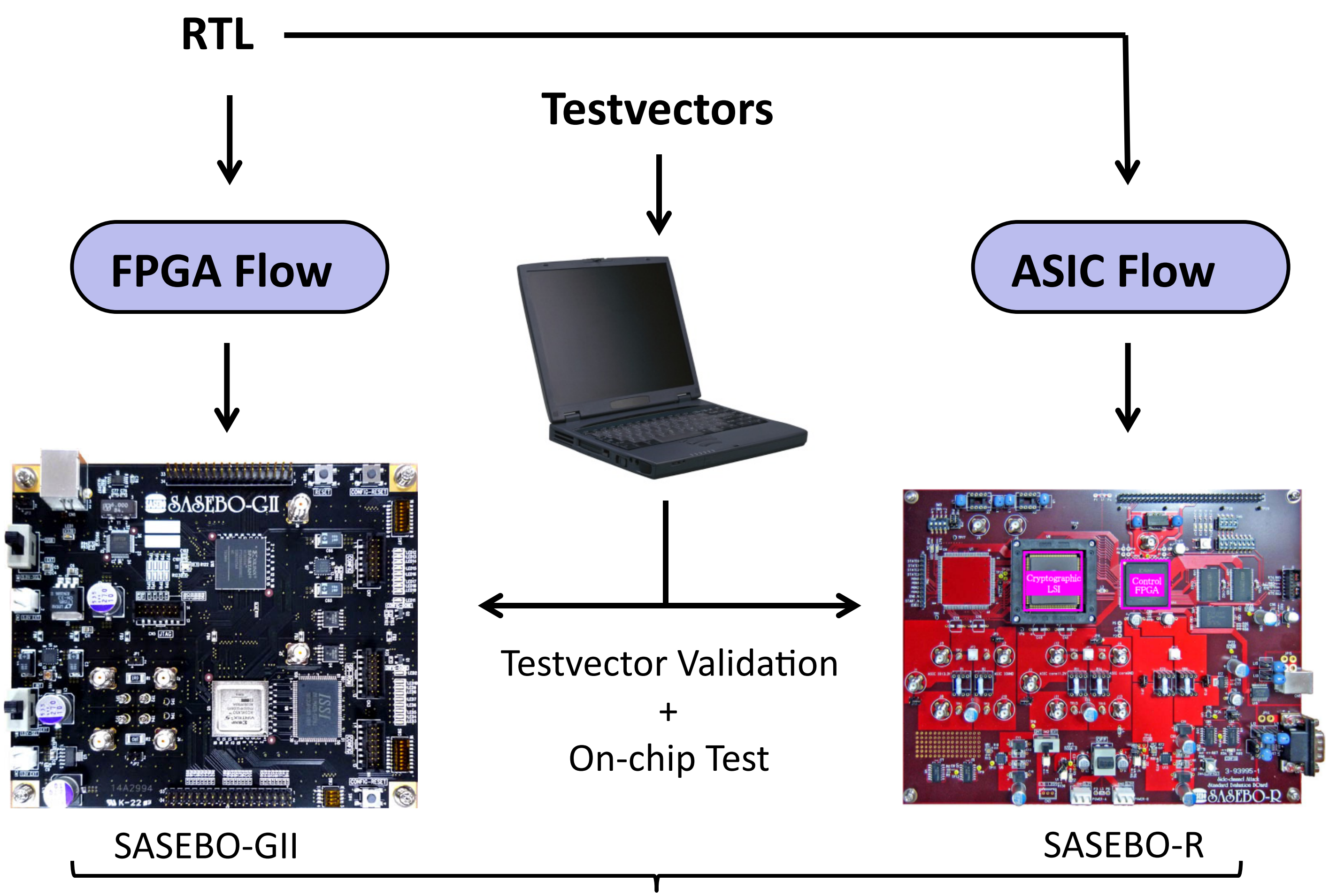
Name	Area (GEs)
Hamsi	19278
Cubehash	25374
Skein	27932
Blake	33136
Keccak	36946
Luffa	37168
SHAvite	41405
Shabal	42221
JH	50362
Fugue	72316
ECHO	74979
Groestl	79041
SIMD	105177
BMW	135550

Smallest 7
221,239 GE

Middle 7
313,553 GE

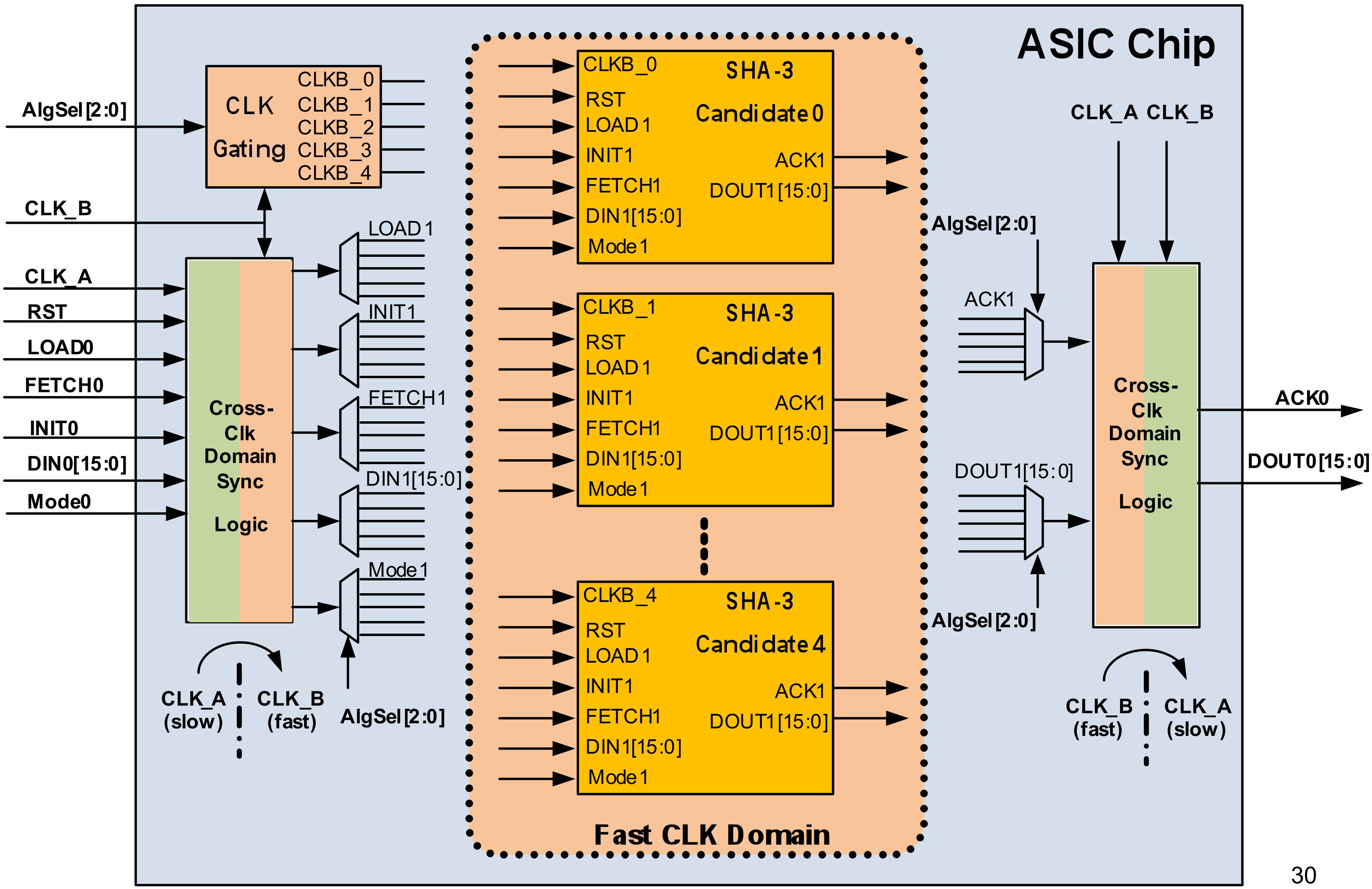
Largest 7
559,646 GE

Overall Test Plan



- Integrated FPGA/ASIC Prototyping
- Power/Performance Measurement
- SASEBO widely used in cryptographic community

ASIC Architecture Design

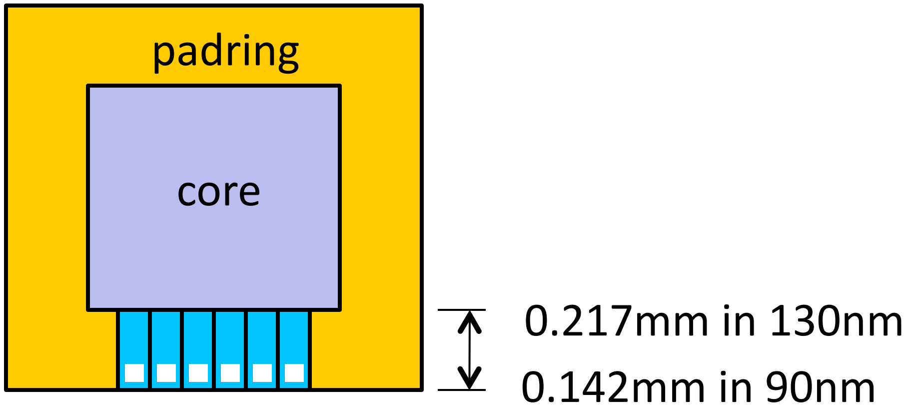


Design Features

- Modular, candidate-agnostic design with standard test harnes
- Variable clock for on-chip performance test
- Clock-gated design for per-candidate dynamic power measurement
  - Static power measurement is proportional to chip area
- Chip Test Control through
  - on-chip test (peak performance, power)
  - on-board FPGA
  - USB-connected test software

ASIC Area Estimation

		Core	*Chip*	*Core*	*Chip*
Design	**GE**	**TSMC 90nm (mm2)**	**TMSC 90nm (mm2)**	**TSMC 130nm (mm2)**	**TSMC 130nm (mm2)**
Smallest 7	221,239	0.624	1.153	1.126	2.236
Middle 7	313,553	0.884	1.499	1.596	2.881
Largest 7	559,646	1.579	2.373	2.849	4.502



Tape-out Schedules and Cost

IMEC	Min Size mm^2	Min Price $	Price per mm^2	Run Dates (only 2010 available)
UMC 130nm	2.32	7344	3166	Jan 11, April 26th, July 26th, October 25th
UMC 90nm	3.515	25775	7333	Jan 11, March 22, May 31, July 12, Oct 25
TSMC 90nm	3.515	25775	7333	Feb 3, April 2, July 1, Oct 15
TSMC 65nm	3.515	38109	10842	April 14, Oct 15
MOSIS				**2011 Run Dates**
IBM 180nm	4	10000	2500	Jan 18, Mar 14, May 2, Jul 11, Sep 6, Nov 7
IBM 130nm	4	10000	2500	Feb 7, May 9, Aug 8, Nov 7
IBM 90nm	4	**25000**	6250	**Feb 28**, May 31, Aug 29, Nov 28
IBM 65nm	4	48000	12000	Jan 19, Mar 15, Aug 9

Packaging adds $1,000 to $2,500 for 40 packaged chips

Timeline

• 30 November	Mock prototype on FPGA (SASEBO-GII)
• 31 December	RTL Selection
• 20 January	Design Review
• **28 February 2011**	Chip Tape-out
• 30 May 2011	Chip Packaging (assuming 3 month turn around)
• 15 June	Chip Test
• 15 July	Performance/Power Measurement Results