Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations

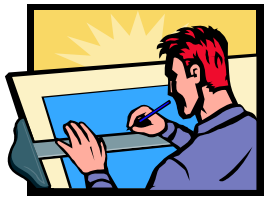
Xu Guo, Sinan Huang
Leyla Nazhandali, Patrick Schaumont
ECE Department, Virginia Tech

Acknowledgement: NIST

Second SHA-3 Conference
Santa Barbara , August 2010

ASIC Designs for SHA-3

- Most SHA-3 candidates < 100KGate
- SHA-3 for ASIC is likely an *Intellectual Property Module*

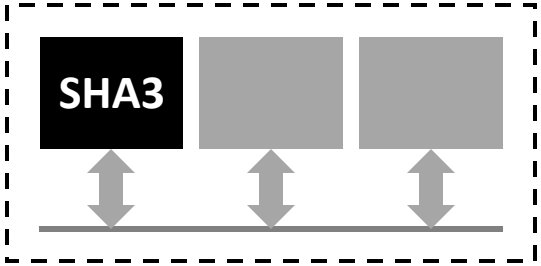


IP Designer

System Integrator

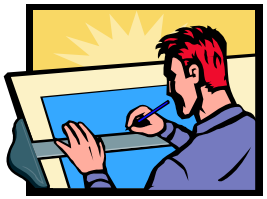
Foundry

SHA3



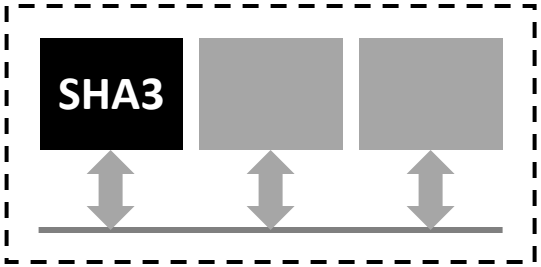
Comparison of SHA-3 ASIC Designs

How do I benchmark a SHA-3 candidate?



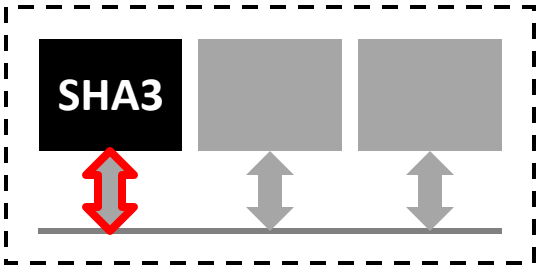
IP Designer

System Integrator



Benchmarking for ASIC Hardware

- System Interface

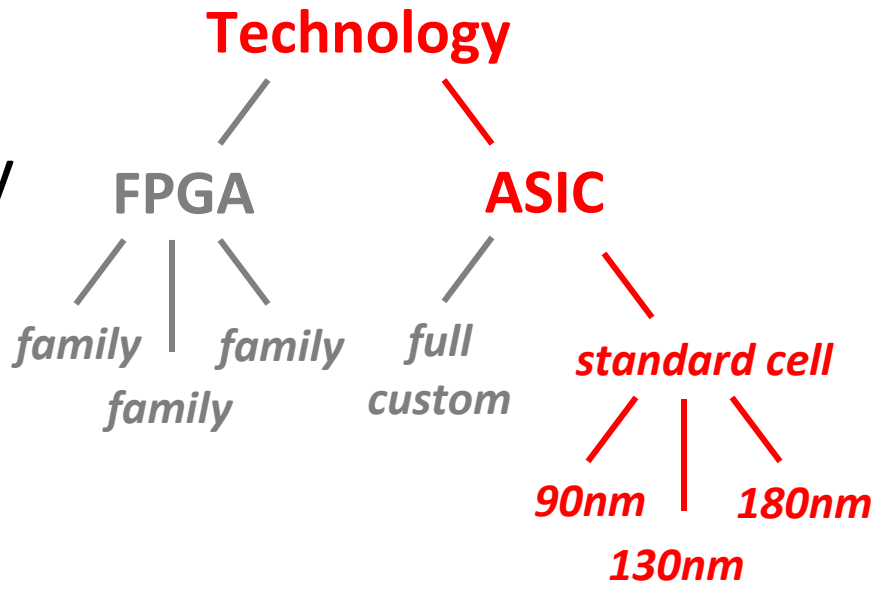


Interface (API)

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

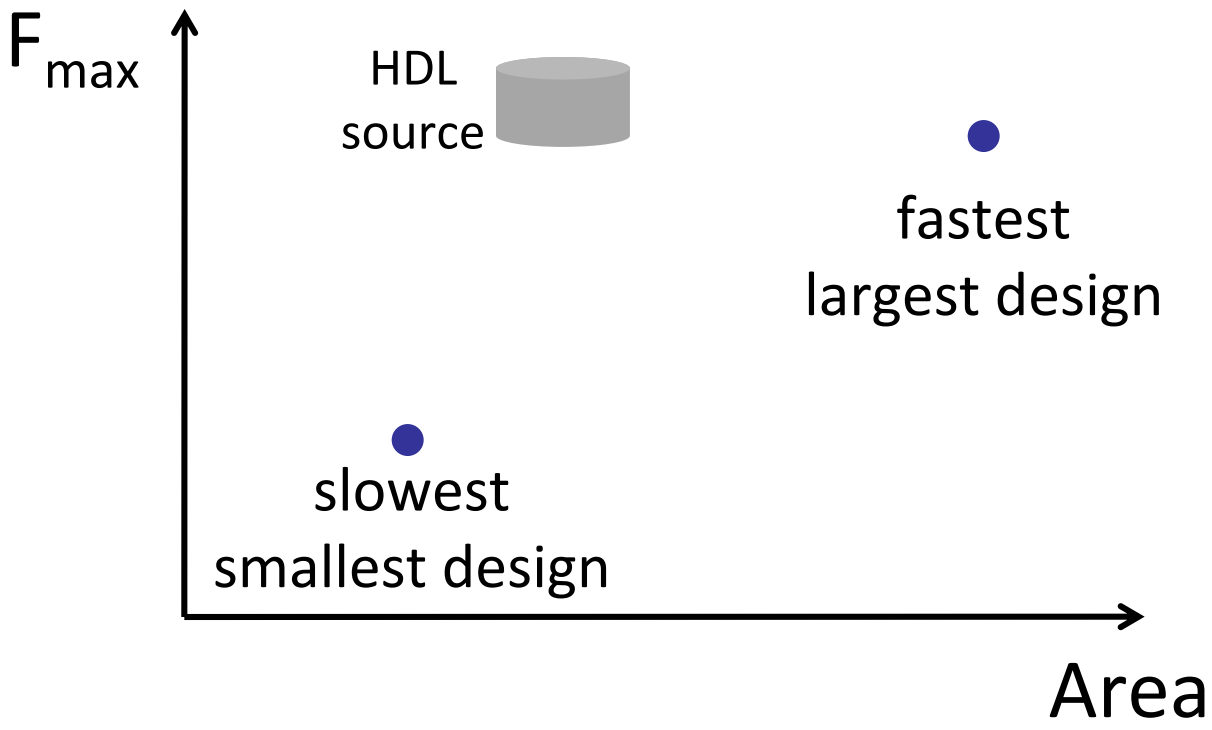
Benchmarking for ASIC Hardware

- System Interface
- Cost Factors
  - Area, F_{max}, Power
  - Throughput, Energy
- **Technology**



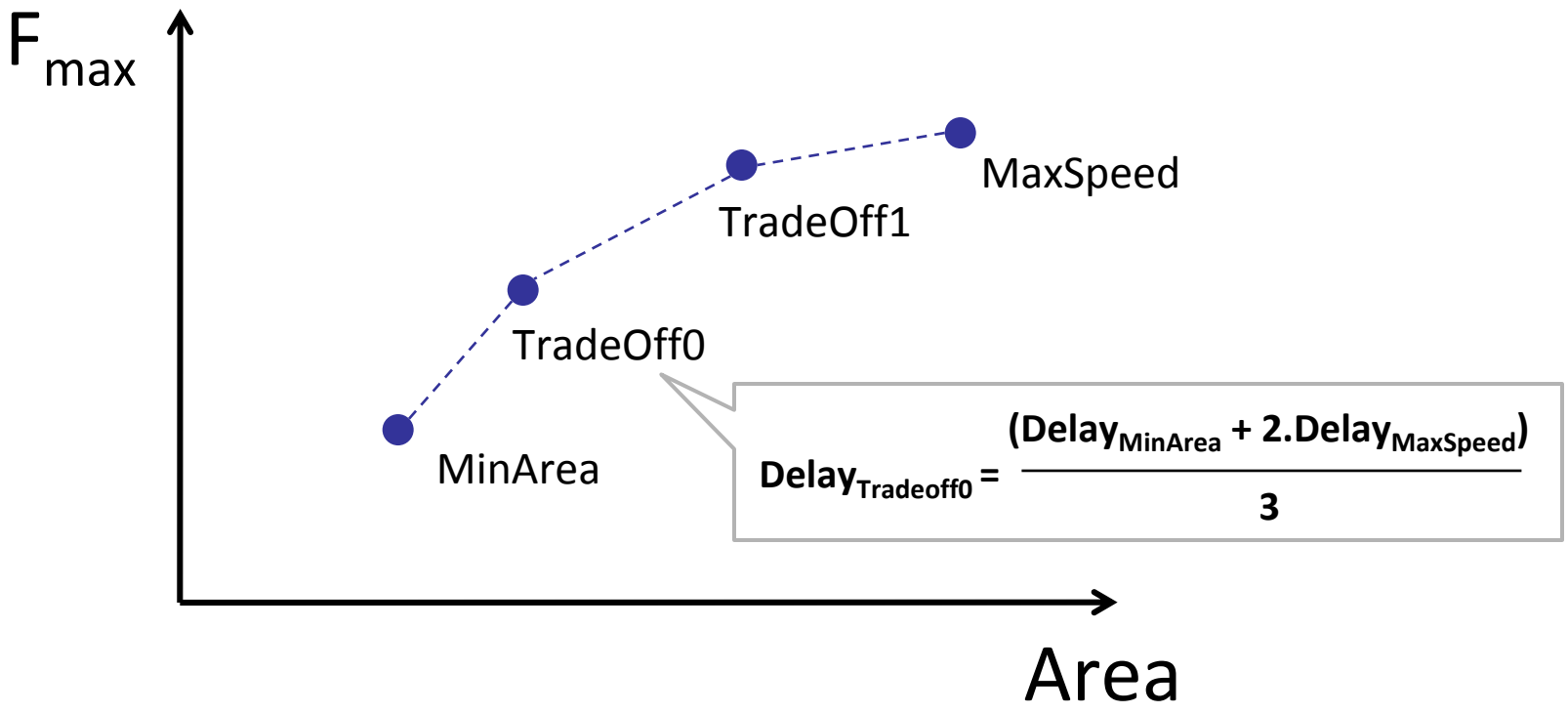
ASIC Design Space

Each hardware SHA-3 module results in **multiple solutions**

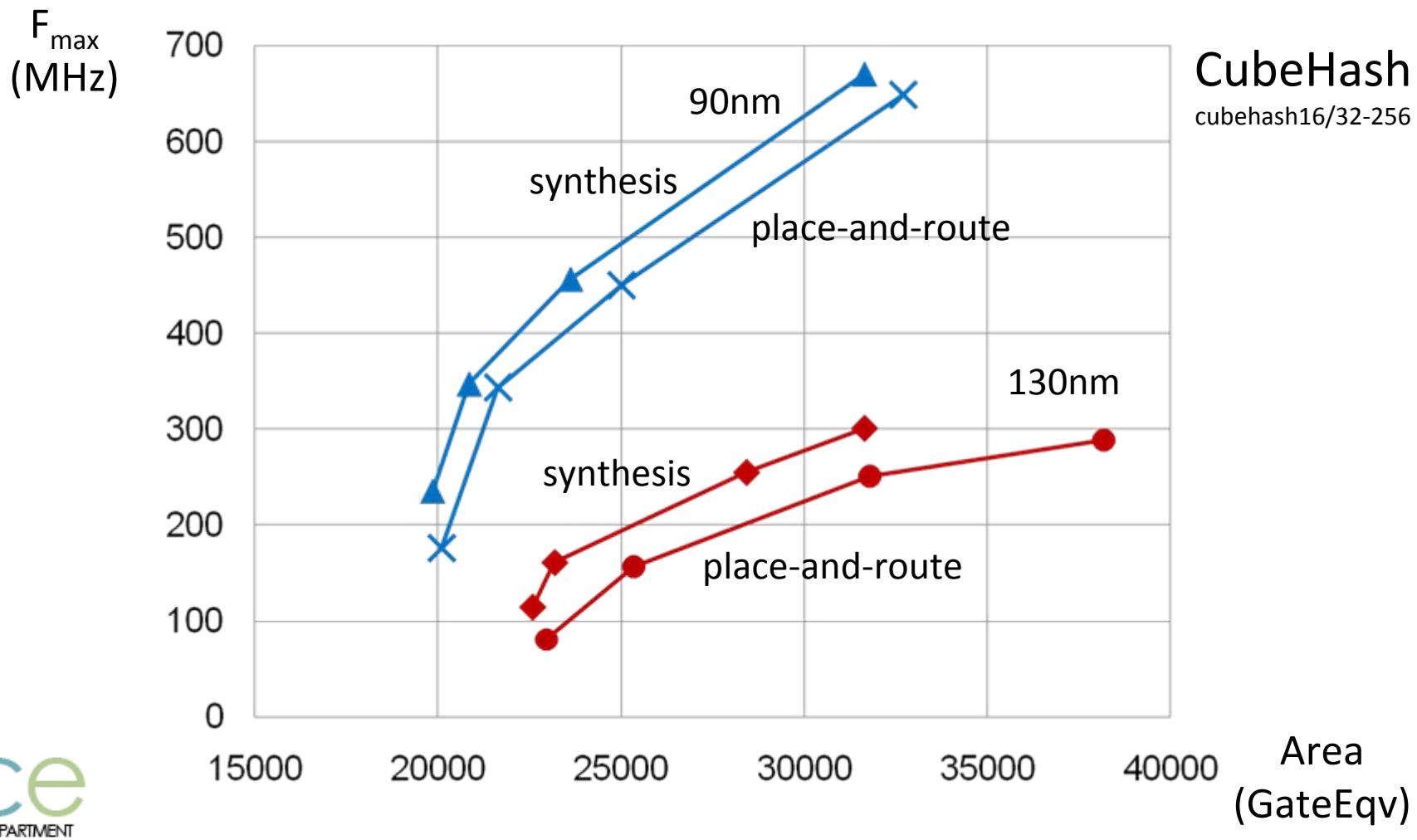


ASIC Design Space

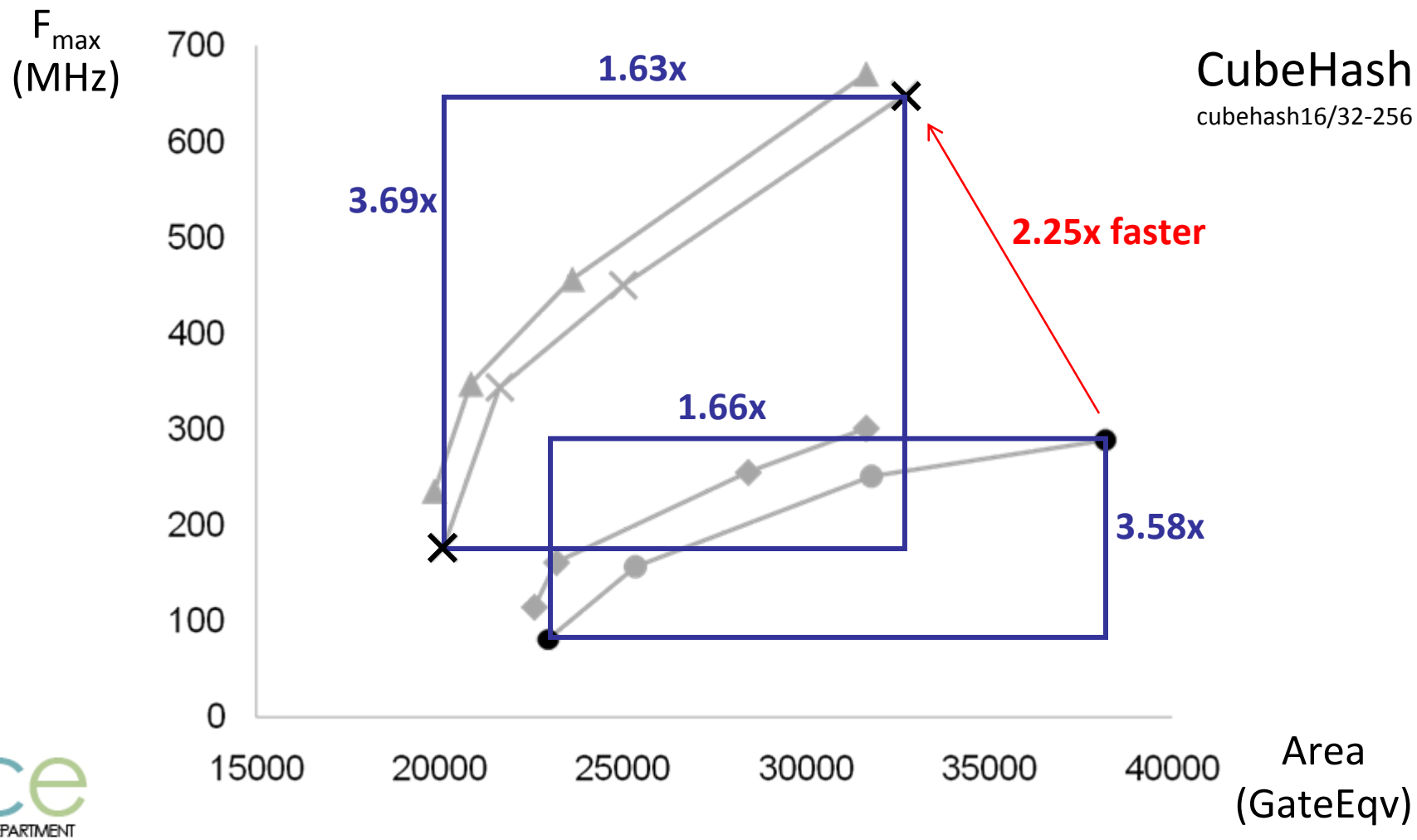
Each hardware SHA-3 module results in **multiple solutions**



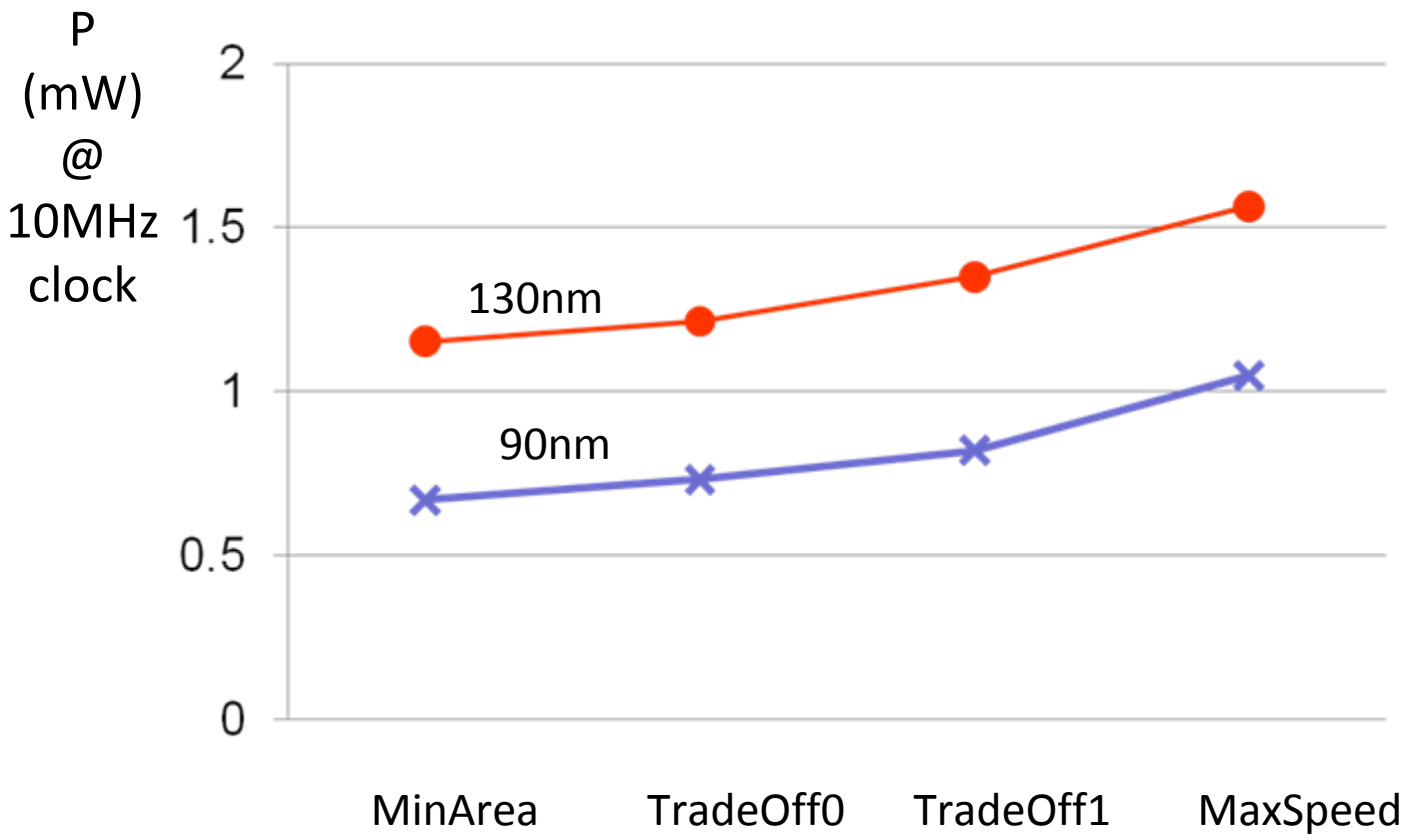
Influence of Technology



Influence of Technology



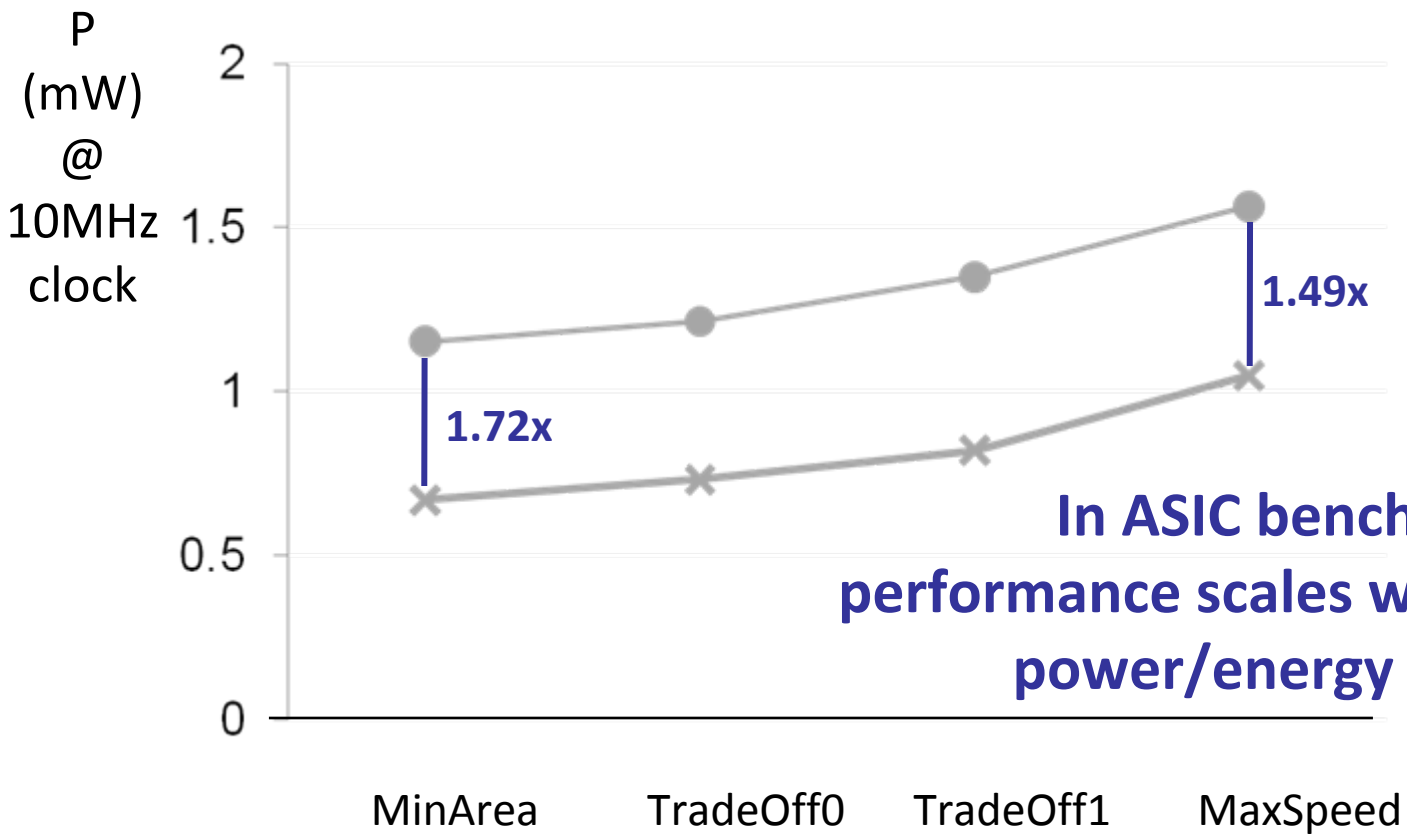
Influence of Technology



CubeHash

cubehash16/32-256

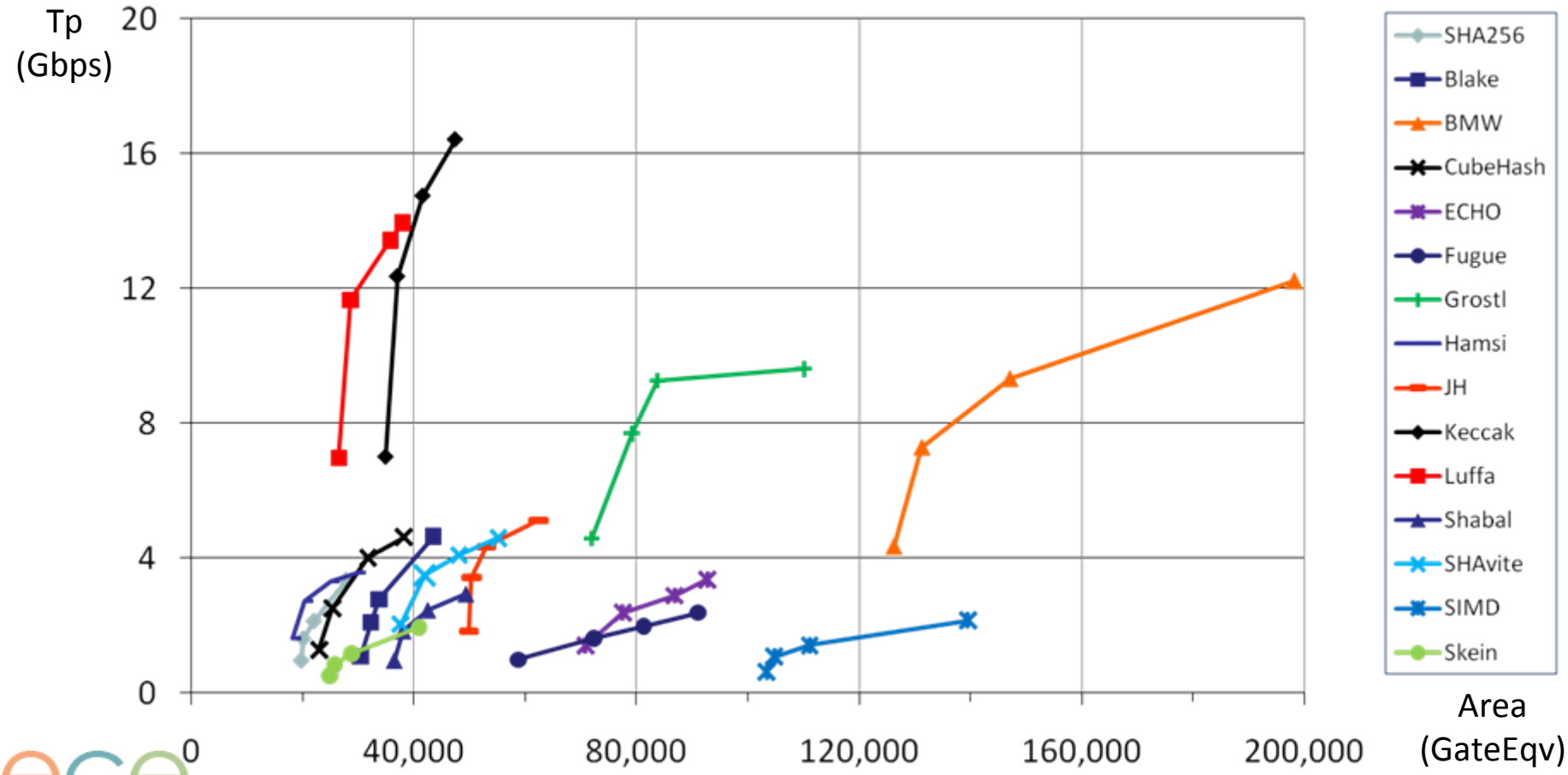
Influence of Technology



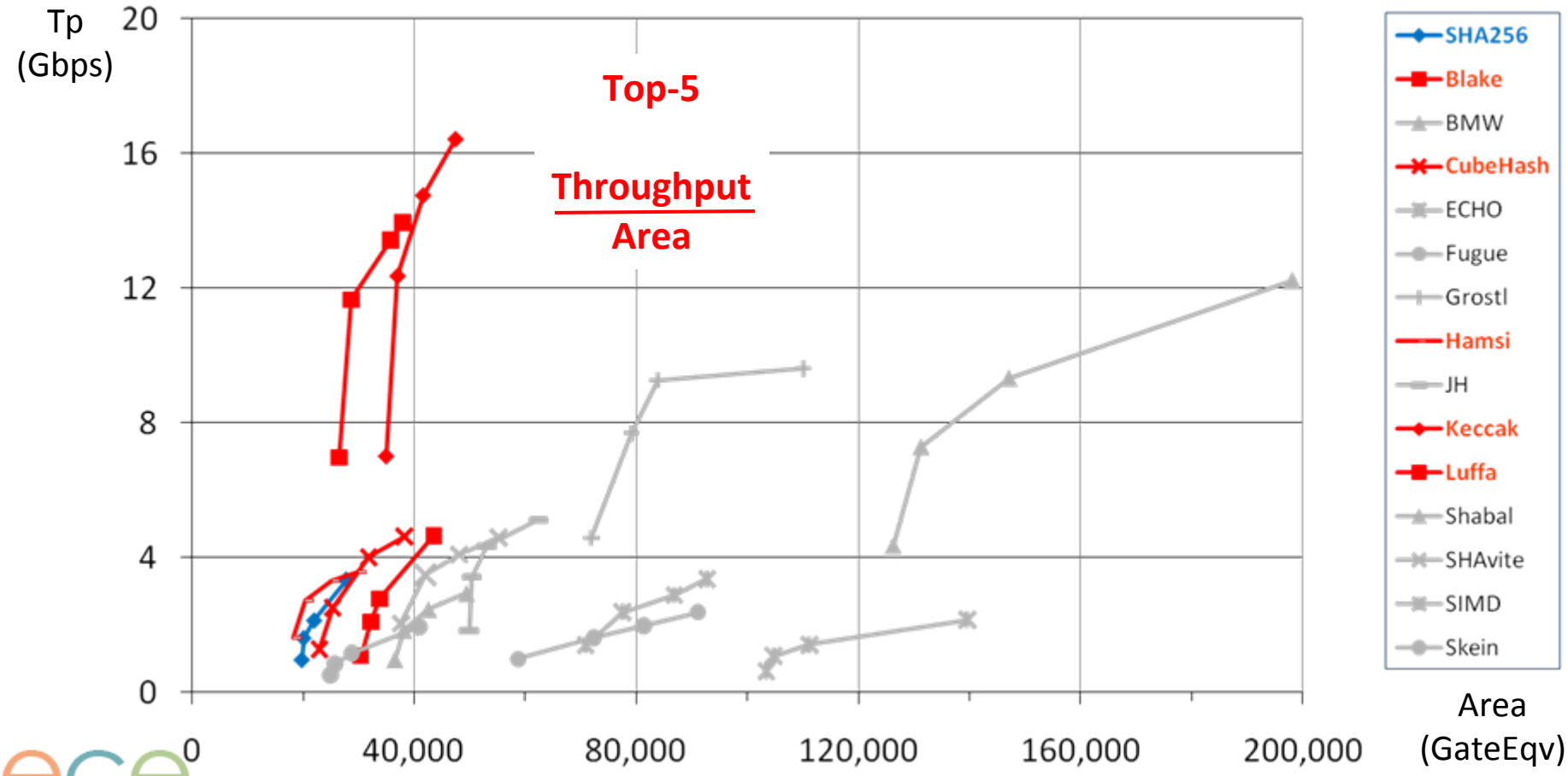
CubeHash
cubehash16/32-256

In ASIC benchmarks, performance scales with technology; power/energy does not

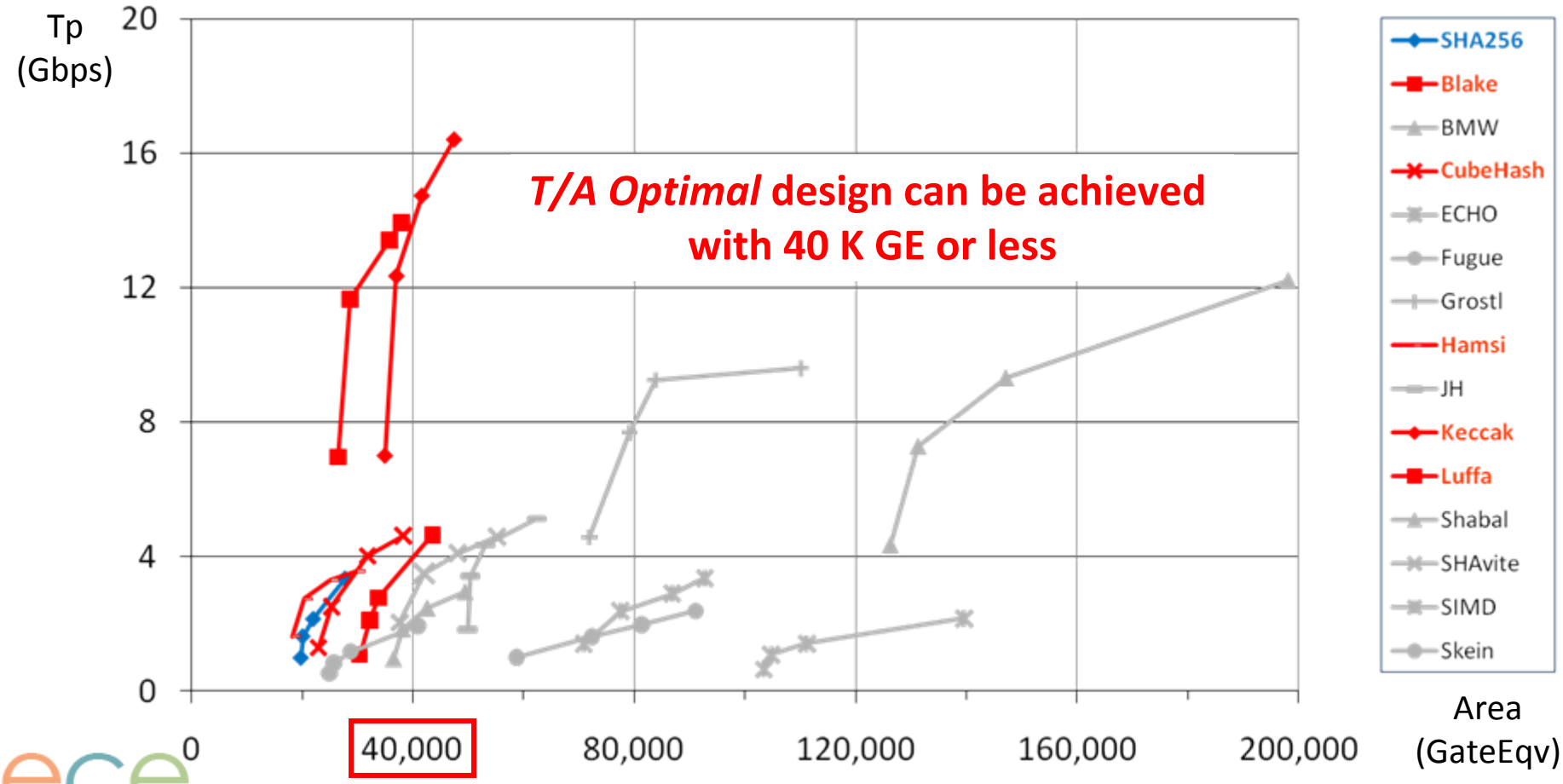
Post-P&R Results for ASIC 130nm



Post-P&R Results for ASIC 130nm

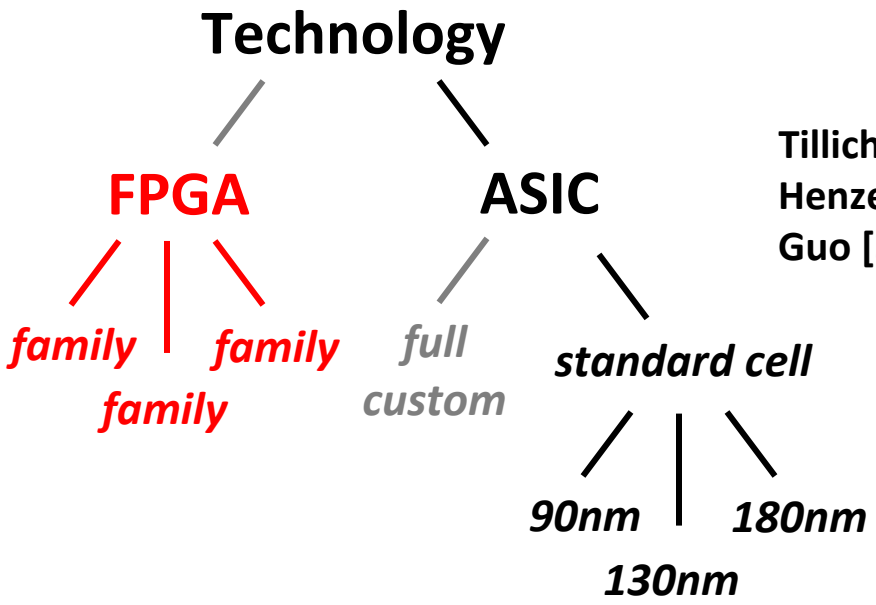


Post-P&R Results for ASIC 130nm



What about other Technologies?

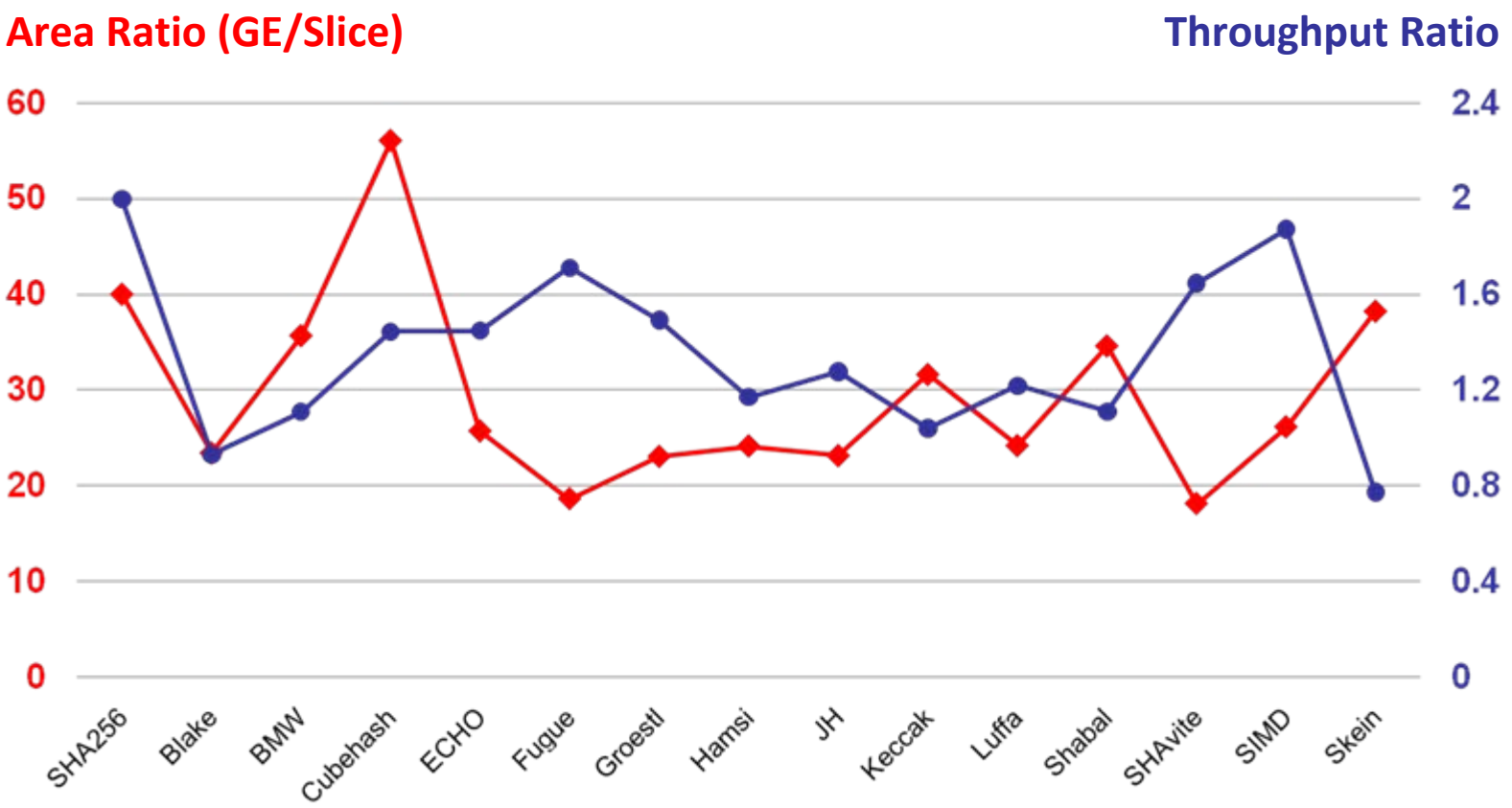
Gaj [CHES]
Kobayashi [HOST]



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

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

FPGA compared to ASIC



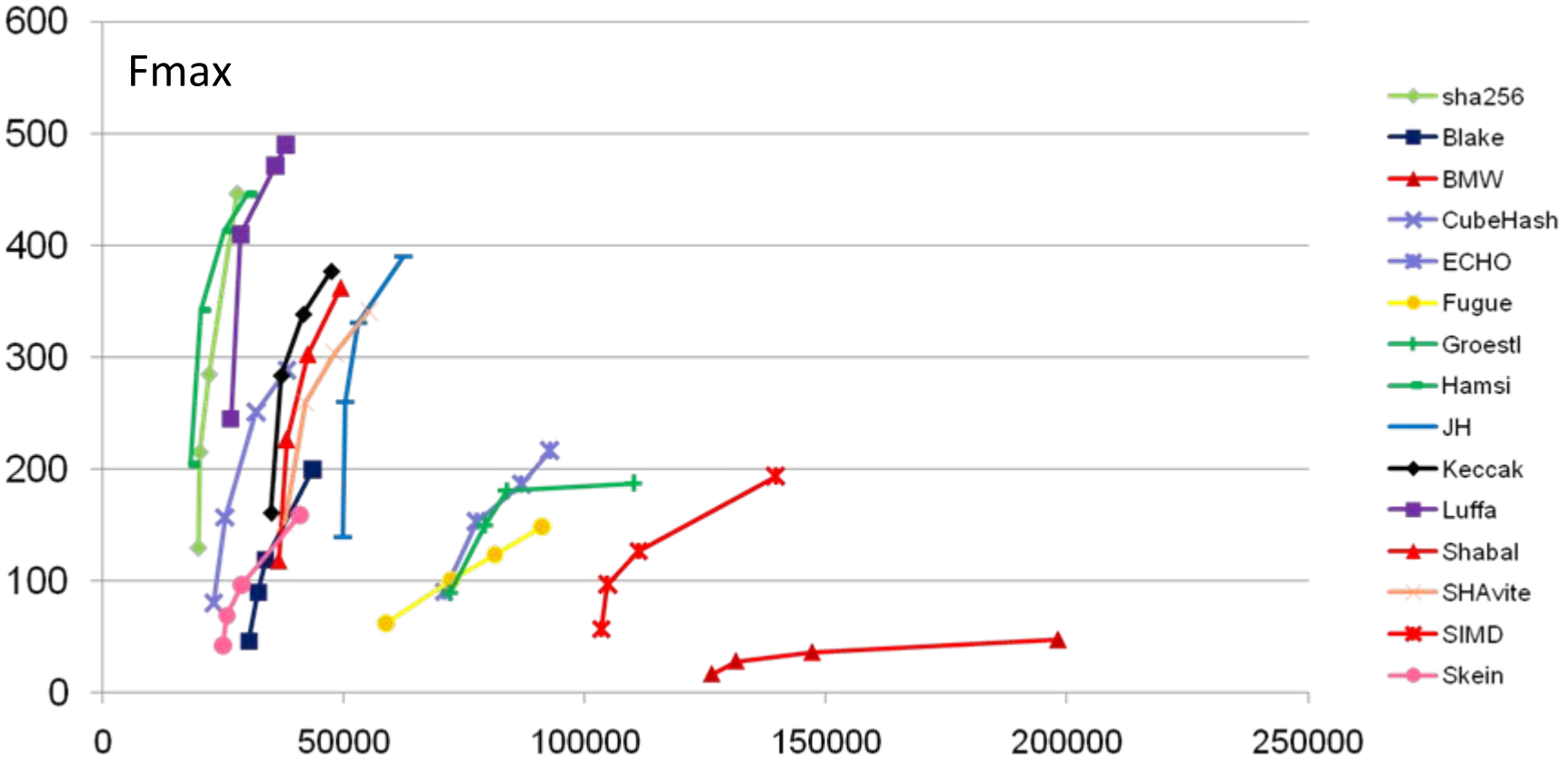
FPGA - Virtex5 65nm ASIC - UMC 130nm

Conclusions

- Top performers in ASIC include
  Blake, CubeHash, Hamsi, Keccak, Luffa

- Impact of Technologies on SHA3 surveys
  - ASIC surveys agree on performance, not on power/energy
  - ASIC surveys will probably not agree with FPGA surveys

Post P&R Results for 130nm ASIC



Area (GateEqv)

Overall Design Flow

Research Groups:
VT + KUL + UEC/NICT/AIST
GMU
IAIK
ETHZ