ATHENa – Automated Tool for Hardware EvaluatioN:

Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware using FPGAs

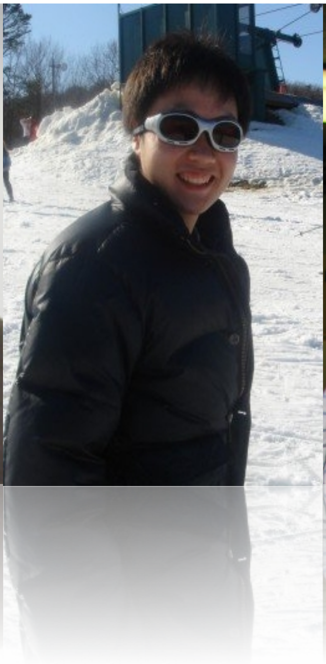
Kris Gaj, Jens-Peter Kaps,
Venkata Amirineni, Marcin Rogawski,
Ekawat Homsirikamol,
Benjamin Y. Brewster

Supported in part by the National Institute of Standards & Technology (NIST)

ATHENa Team

Venkata
“Vinny”
MS CpE
student

Ekawat
“Ice”
PhD CpE
student



Marcin

PhD ECE
student

John

MS CpE
student

Rajesh

PhD ECE
student

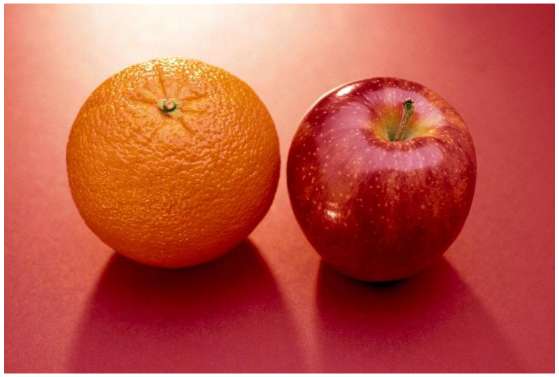
Michal
PhD exchange
student from
Slovakia

Outline

- Motivation & Goals
- Previous Work
- ATHENa
- Two Case Studies
- Future Work & Conclusions

Common Benchmarking Pitfalls

- *taking credit for improvements in technology*
- *choosing a convenient (but not necessarily fair) performance measure*
- *comparing designs with different functionality*
- *comparing designs optimized using different optimization target*
- *comparing clock frequency after synthesis vs. clock frequency after placing and routing*



Objective Benchmarking Difficulties

- *lack of standard interfaces*
- *influence of tools and their options*
- *stand-alone performance vs. performance as a part of a bigger system*
- *time & effort spent on optimization*

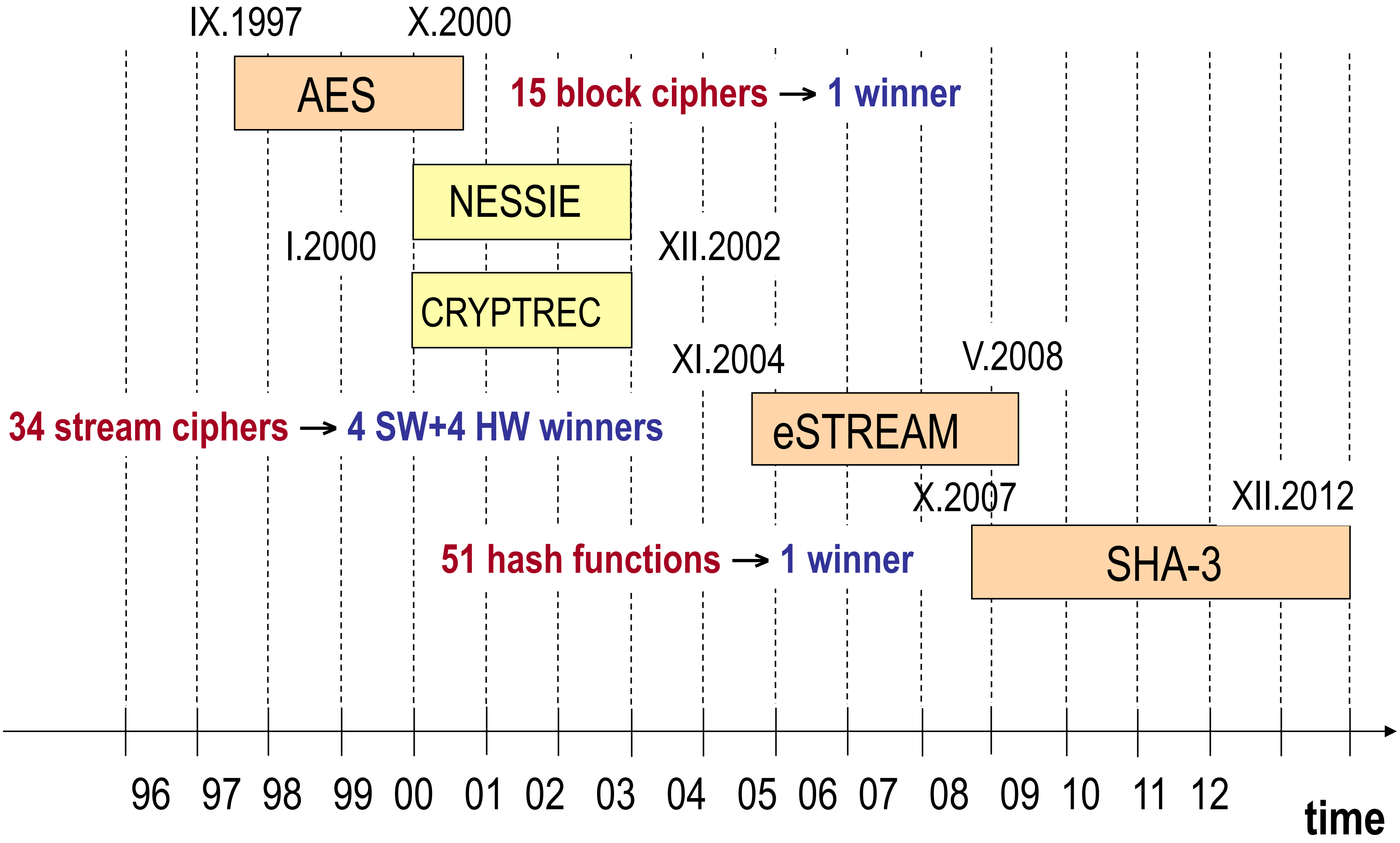
Goal of Our Project

- ***spread knowledge and awareness*** *needed to eliminate benchmarking pitfalls*
- ***develop methodology and tools*** *required to overcome objective difficulties*

Why Cryptographic Algorithms?

- *well documented speed-ups (10x-10,000x)*
- *security gains (e.g., key generation & storage)*
- *constantly evolving standards*
- *cryptographic standard contests*

Cryptographic Standard Contests



Criteria Used to Evaluate Cryptographic Algorithms

Security

Software Efficiency

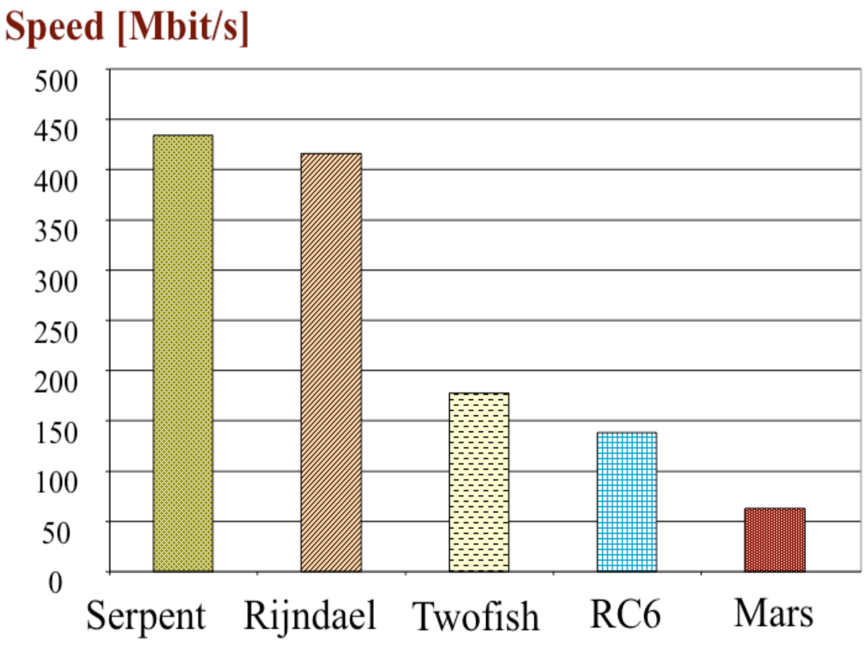
Hardware Efficiency

Flexibility

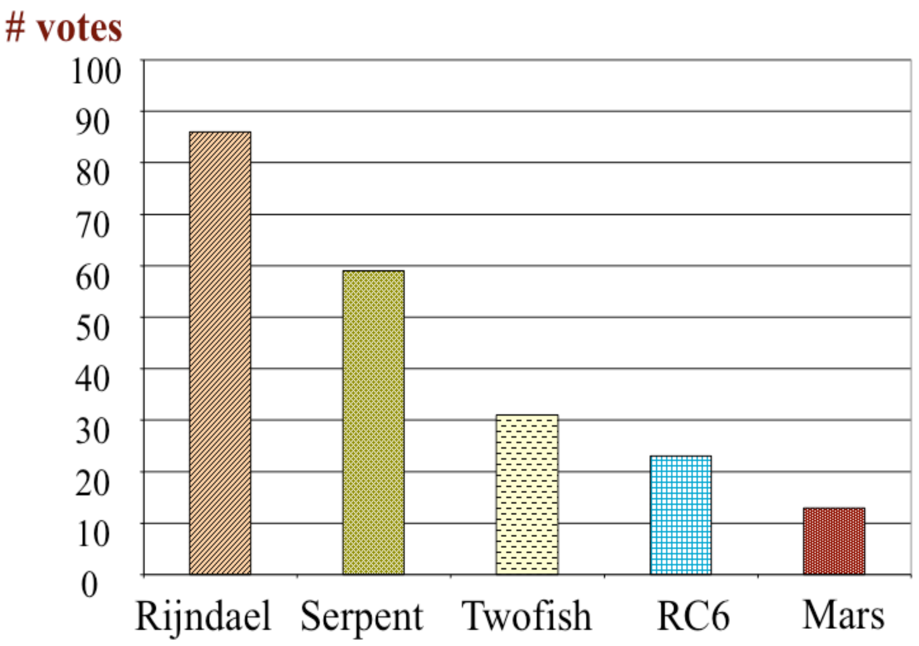
Advanced Encryption Standard Contest

Round 2 of AES Contest, 2000

Speed in FPGAs



Votes at the AES 3 conference

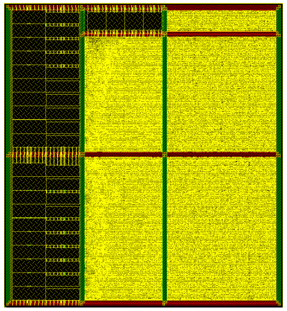


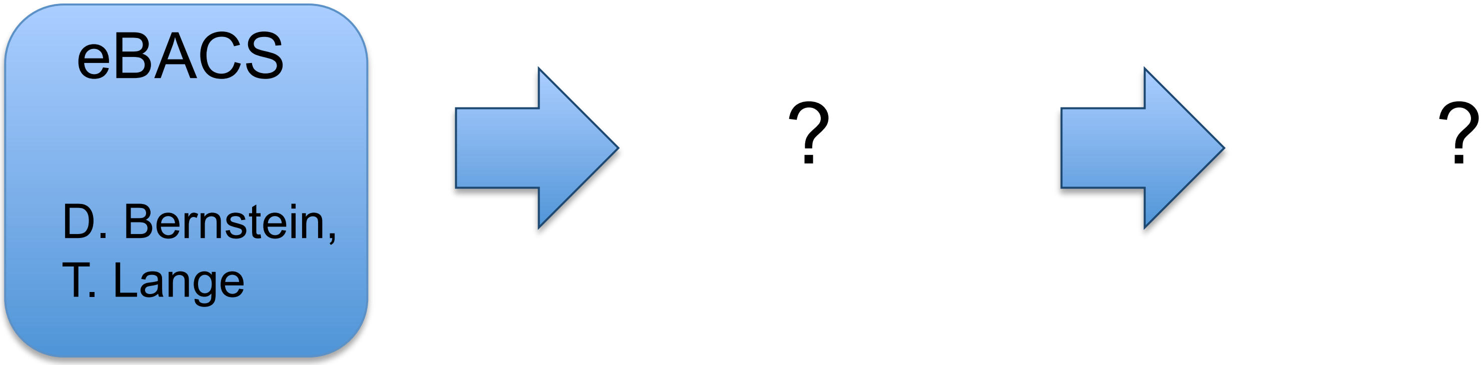
Benchmarking in Cryptography

Software

FPGAs

ASICs





eBACS

D. Bernstein,
T. Lange

?

?

eBACS: ECRYPT Benchmarking of Cryptographic Systems

SUPERCOP - toolkit developed by D. Bernstein and T. Lange for measuring performance of cryptographic software

- measurements on multiple machines (currently over 70)
- each implementation is recompiled multiple times (currently over 1200 times) with various compiler options
- time measured in clock cycles/byte for multiple input/output sizes
- median, lower quartile (25th percentile), and upper quartile (75th percentile) reported
- standardized function arguments (common API)

ATHENa – **A**utomated **T**ool for **H**ardware **E**valuatio**N**

http://cryptography.gmu.edu/athena

Benchmarking open-source tool, written in Perl, aimed at an
AUTOMATED generation of
OPTIMIZED results for
MULTIPLE hardware platforms

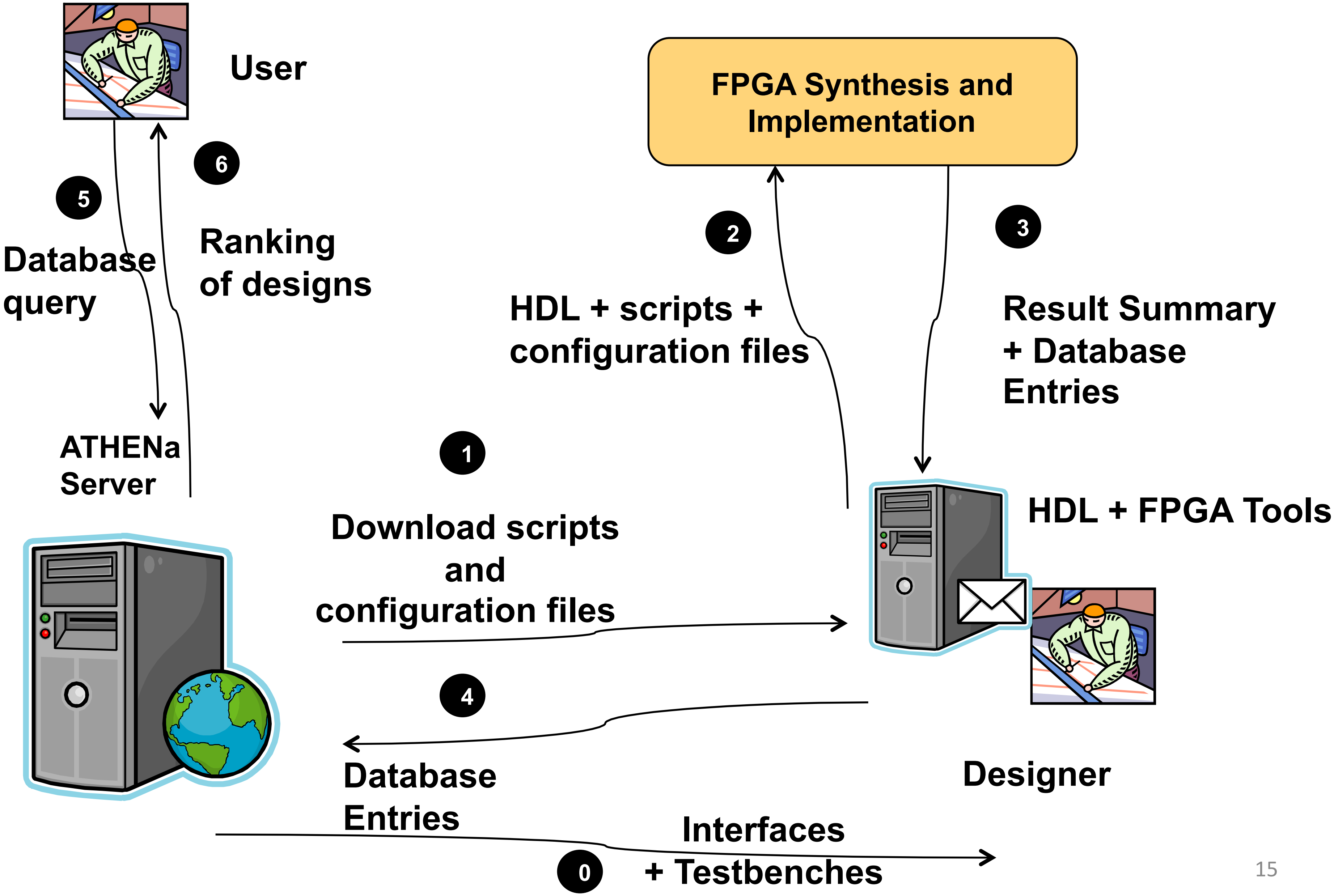
Currently under development at George Mason University.

Why Athena?

"The Greek goddess Athena was frequently called upon to settle disputes between the gods or various mortals. Athena Goddess of Wisdom was known for her superb logic and intellect. Her decisions were usually well-considered, highly ethical, and seldom motivated by self-interest."

from "Athena, Greek Goddess of Wisdom and Craftsmanship"

Basic Dataflow of ATHENa



User

5 Database query

6 Ranking of designs

ATHENa Server

FPGA Synthesis and Implementation

2 HDL + scripts + configuration files

3 Result Summary + Database Entries

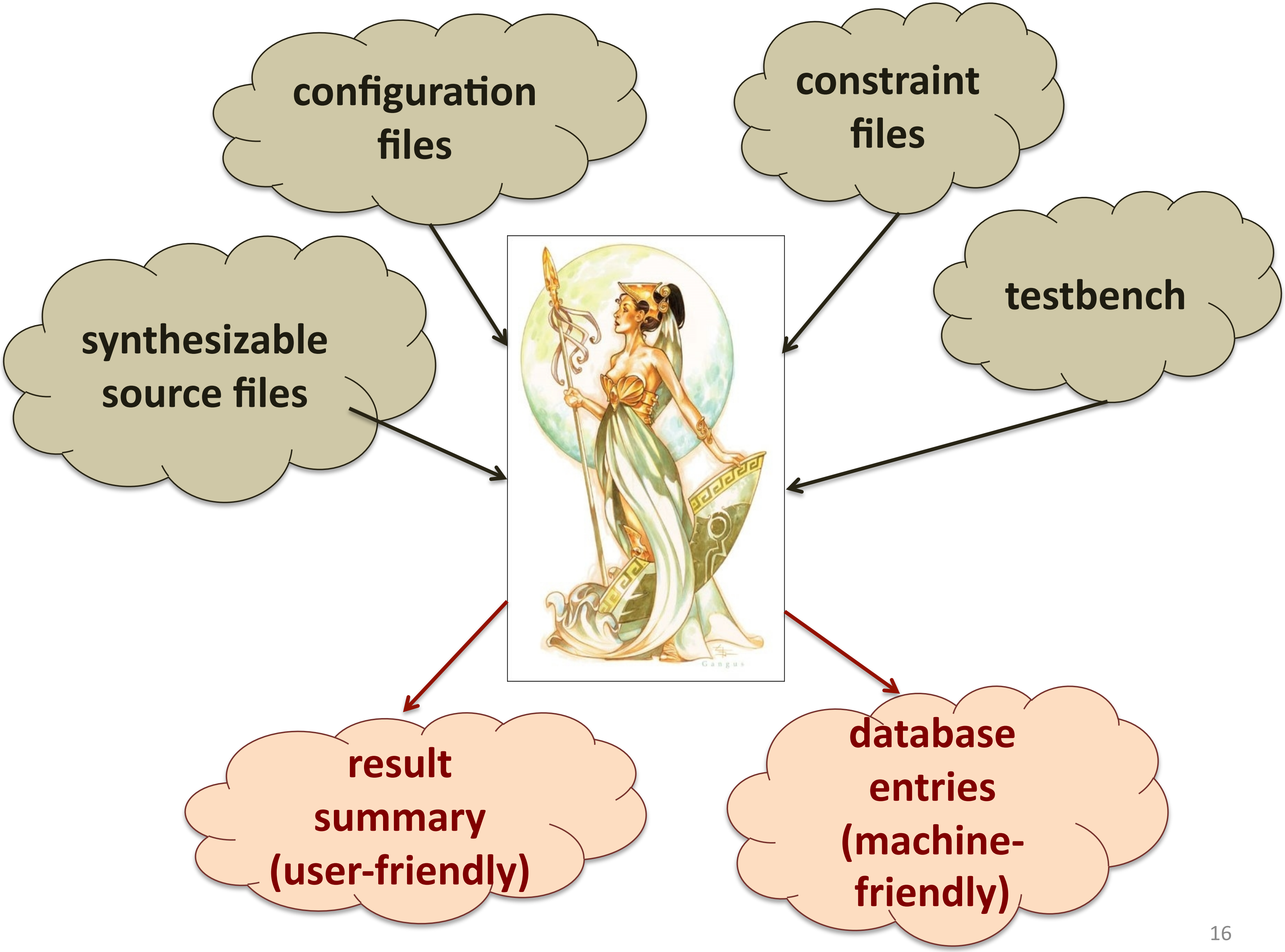
1 Download scripts and configuration files

HDL + FPGA Tools

4 Database Entries

Designer

0 Interfaces + Testbenches



configuration files

constraint files

synthesizable source files

testbench

result summary (user-friendly)

database entries (machine-friendly)

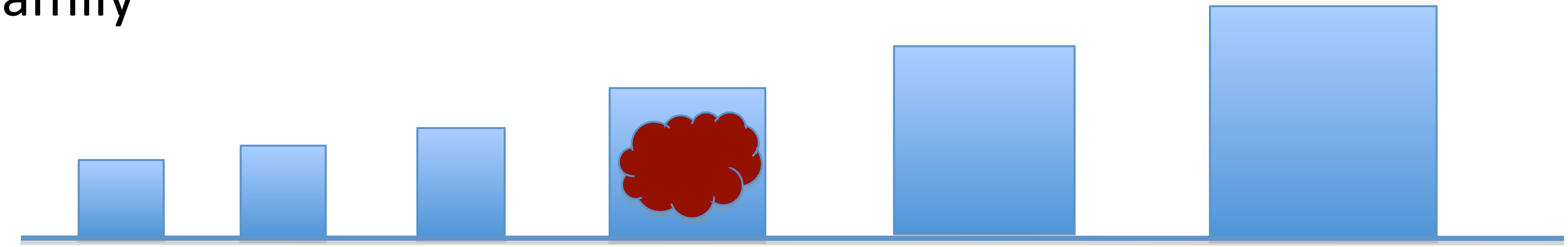
ATHENa Major Features (1)

- synthesis, implementation, and timing analysis in **batch mode**
- support for devices and tools of **multiple FPGA vendors**:

XILINX. ALTERA.

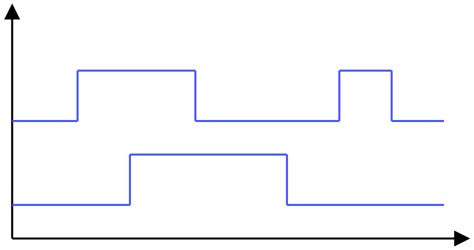
- generation of results for **multiple families** of FPGAs of a given vendor

- automated choice of a **best-matching device** within a given family



ATHENa Major Features (2)

- **automated verification** of designs through simulation in batch mode



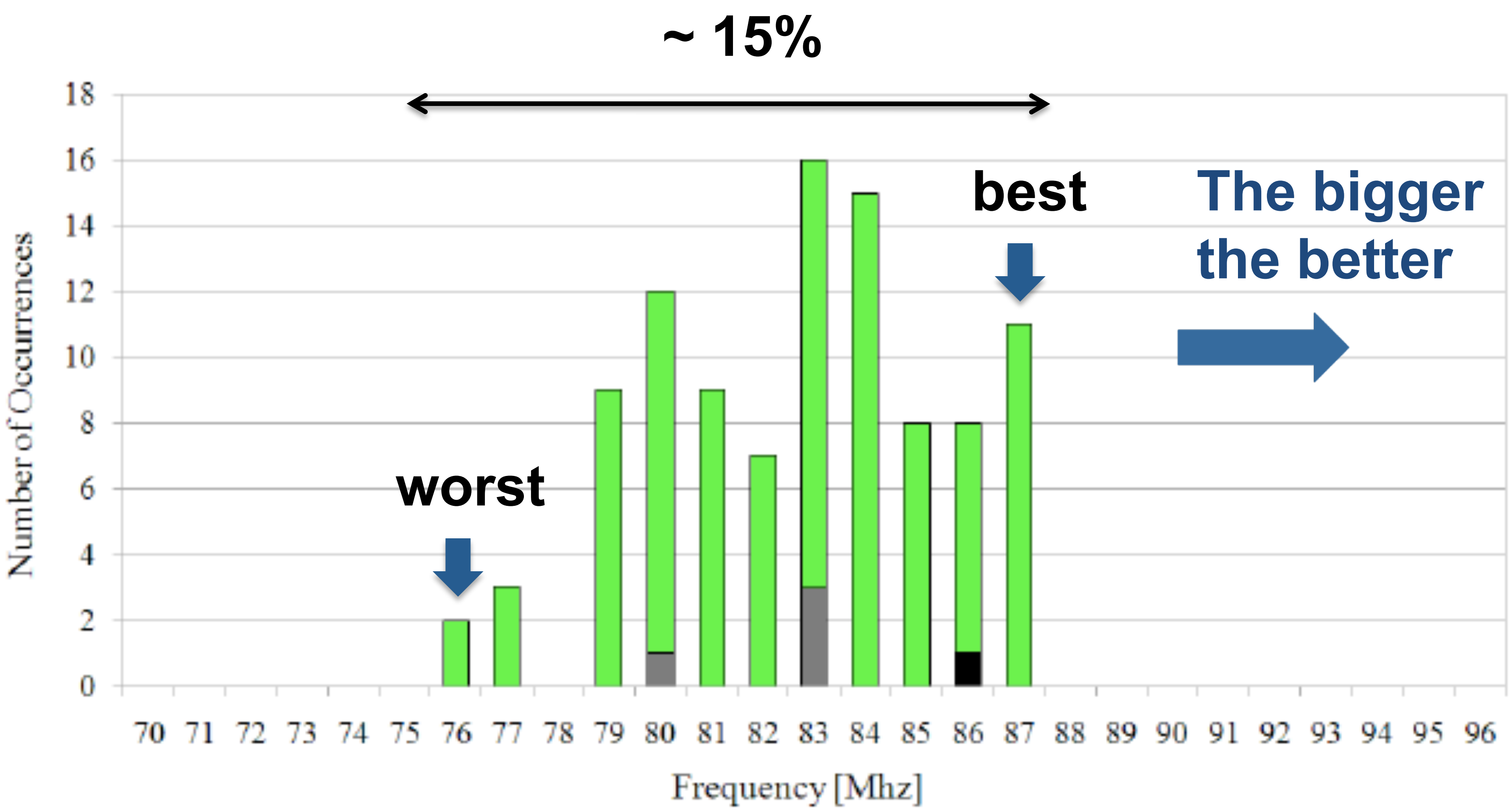
OR

- support for **multi-core processing**
- automated **extraction and tabulation of results**
- several **optimization strategies** aimed at finding
  - optimum options of tools
  - best target clock frequency
  - best starting point of placement

Multi-Pass Place-and-Route Analysis

GMU SHA-256, Xilinx Spartan 3

100 runs for different placement starting points



~ 15%

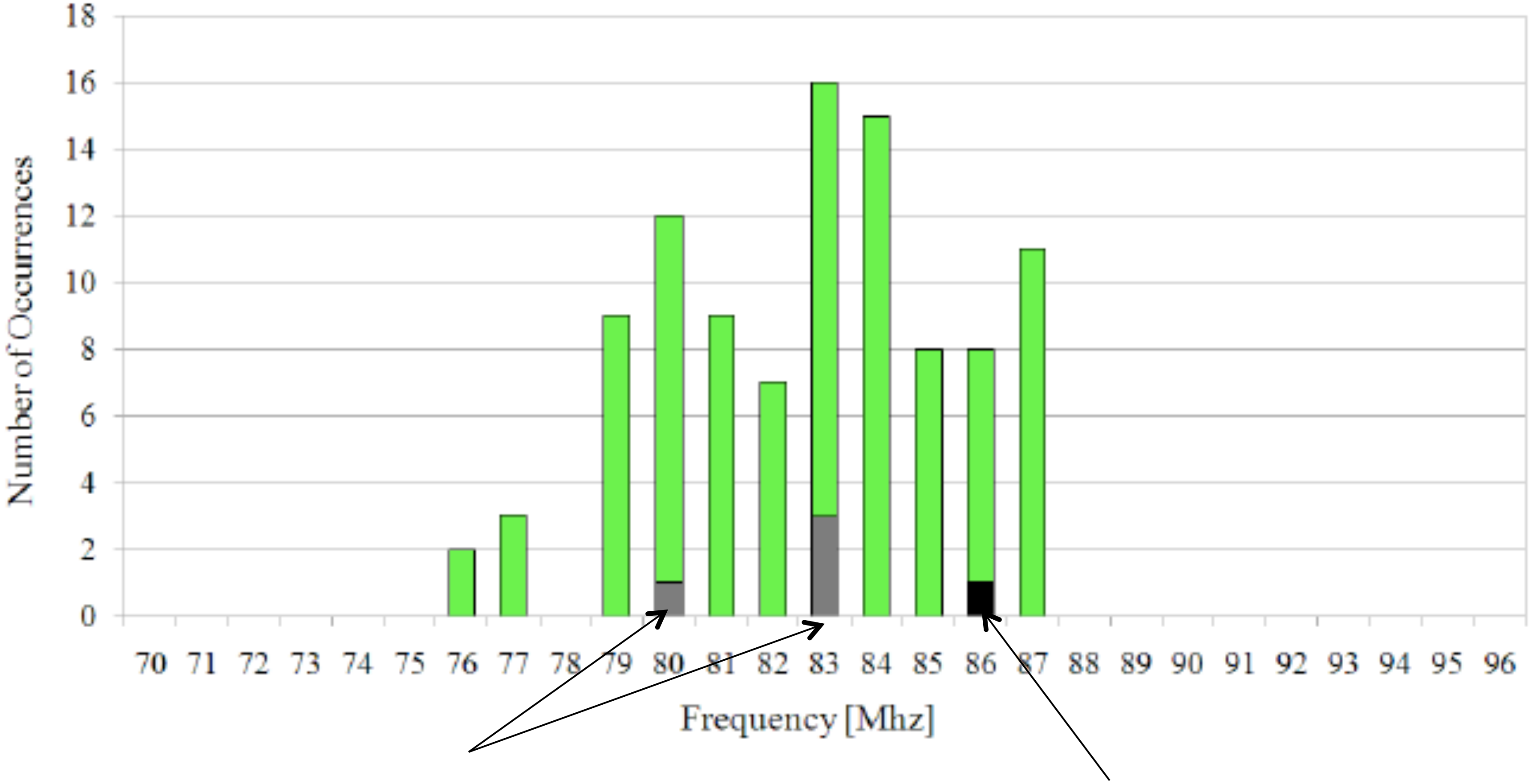
best

worst

The bigger the better

19

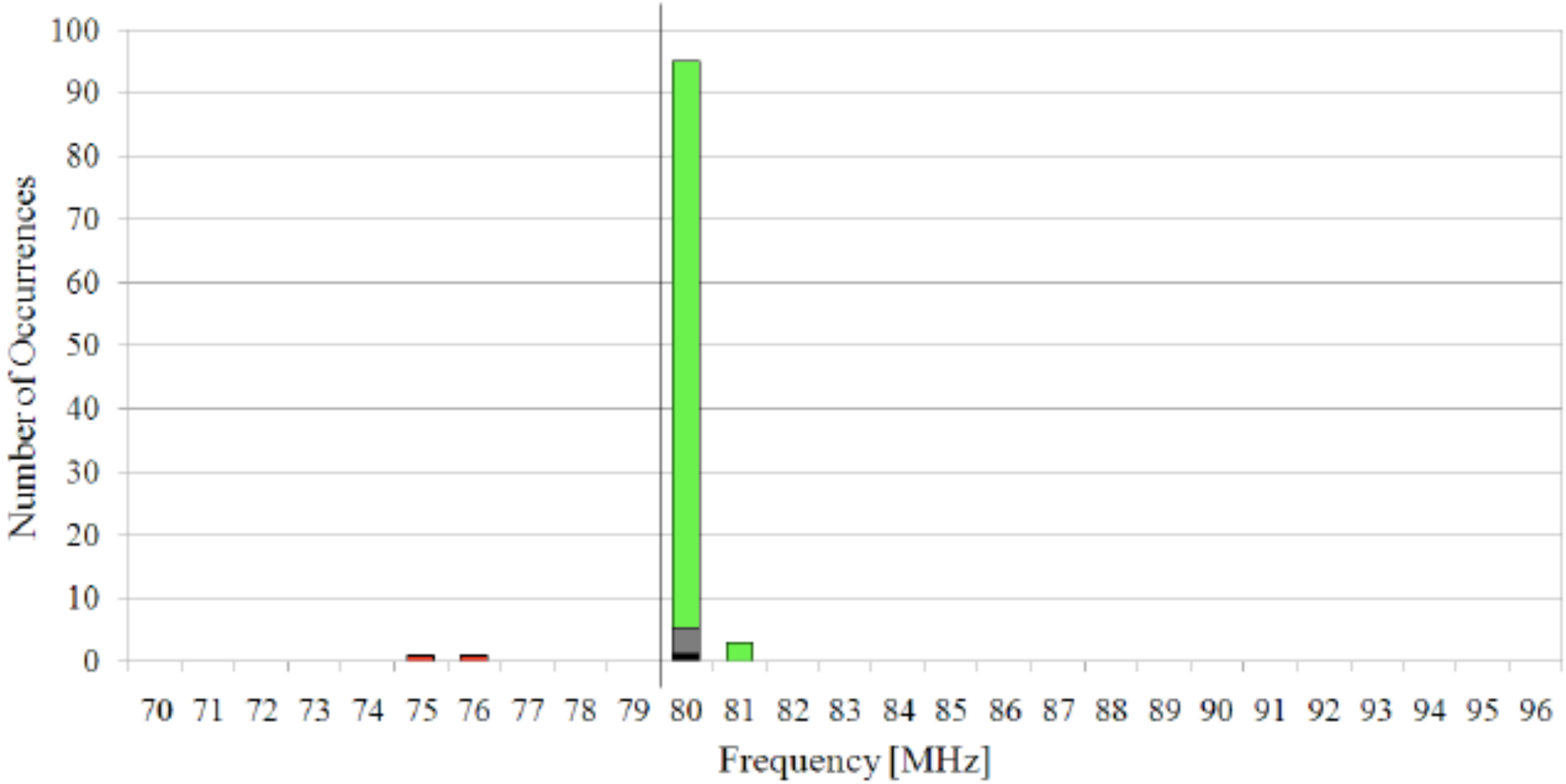
Results for default target clock frequency



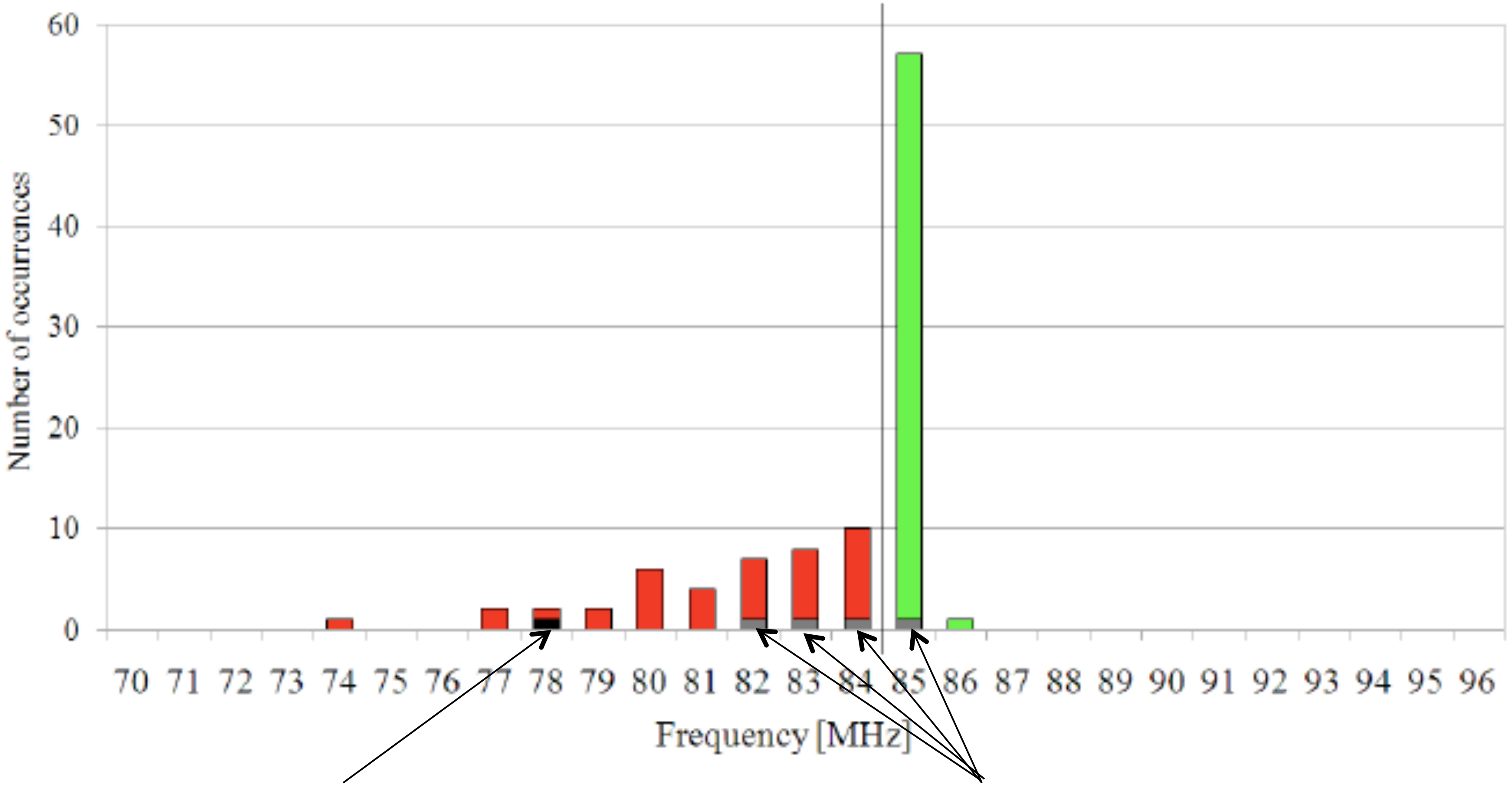
preselected COST_TABLEs (21, 41, 61, 81)

default COST_TABLE (1)

Results for target clock frequency = 80 MHz



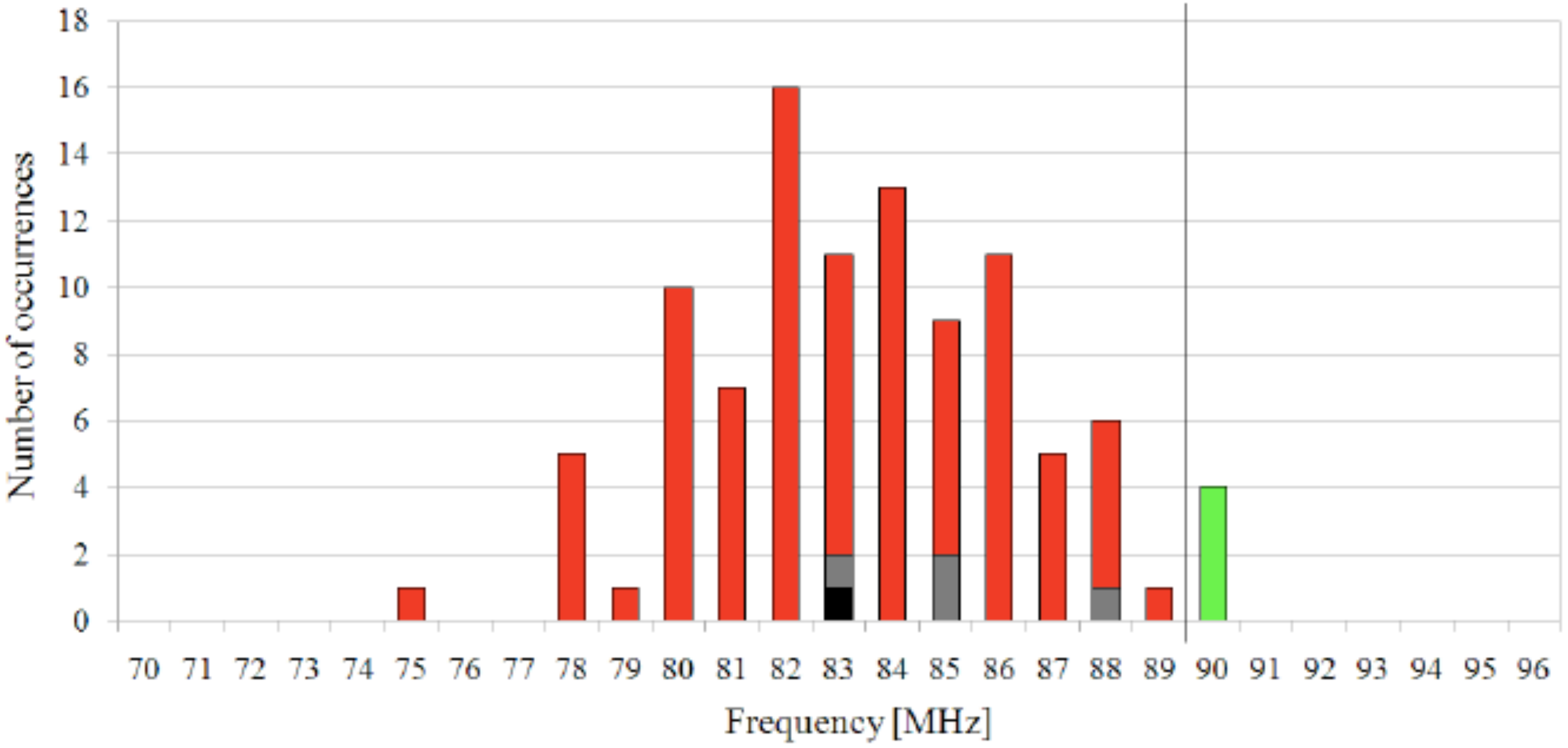
Results for target clock frequency = 85 MHz



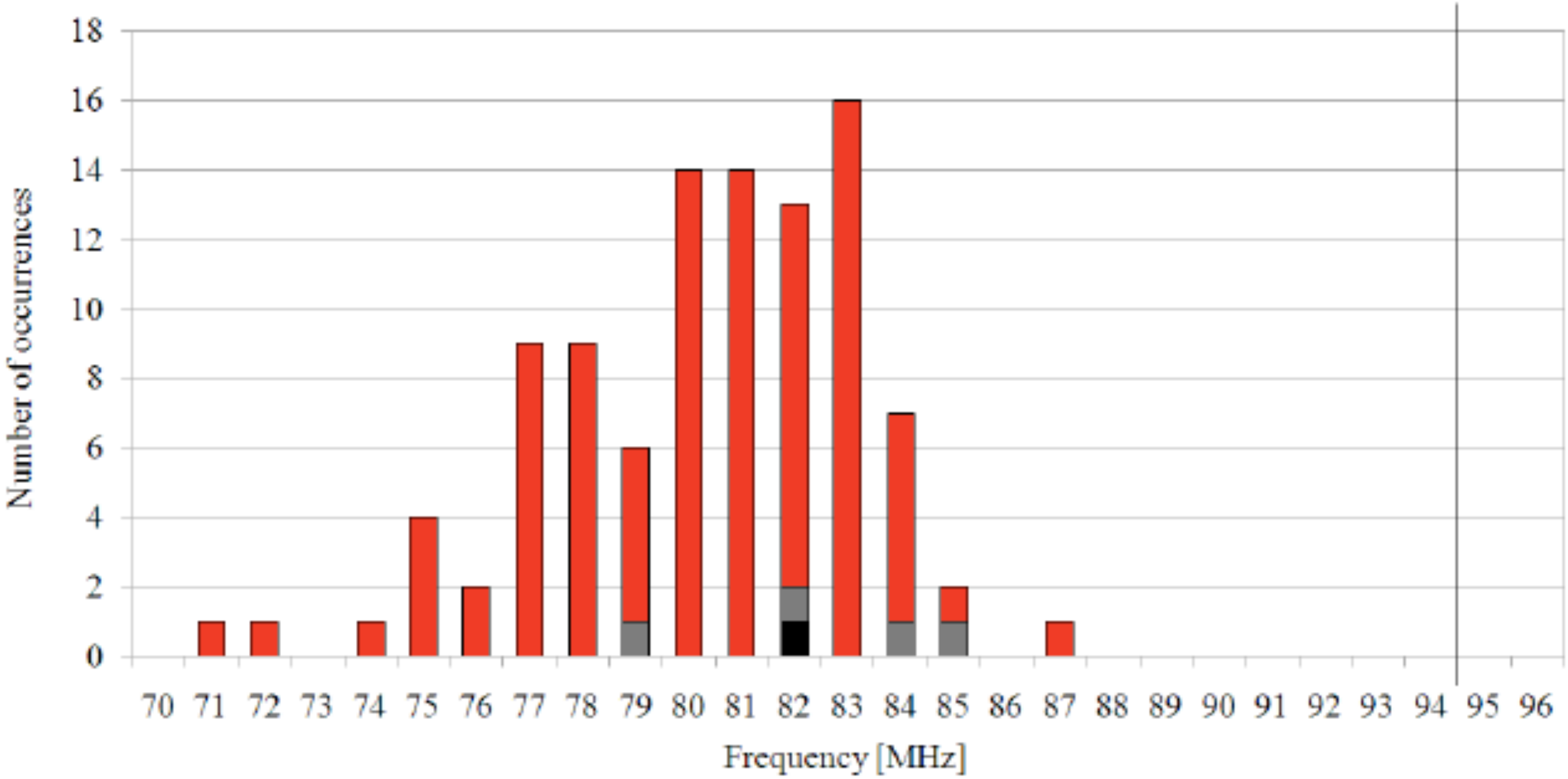
default COST_TABLE (1)

preselected COST_TABLEs (21, 41, 61, 81)

Results for target clock frequency = 90 MHz



Results for target clock frequency = 95 MHz



Optimization Strategy Used for Xilinx Devices

1. Frequency search

   Search for the highest requested clock frequency that is met with a single run of tools.

2. Exhaustive search

   Search for the best combination of the following options

   - optimization target for synthesis: area, speed
   - optimization target for mapping: area, speed
   - optimization effort level for placing and routing: medium, high

3. Placement search

   Search for the best starting point for placement, using 4 additional values of the COST_TABLE {21, 41, 61, 81}.

Total number of runs = 15-20

Optimization Strategy Used for Altera Devices

1. Exhaustive search

   Search for the best combination of the following options:

   - Synthesis optimization: speed, area, balanced
   - Optimization effort: auto, fast
   - Implementation effort: standard, auto

2. Placement search

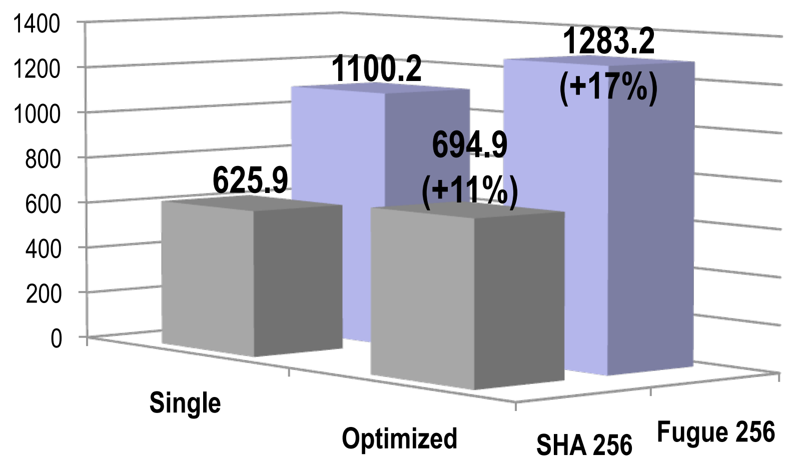
   Search for the best starting point of placement,
   using 4 additional values of SEED {2001, 4001, 6001, 8001}.

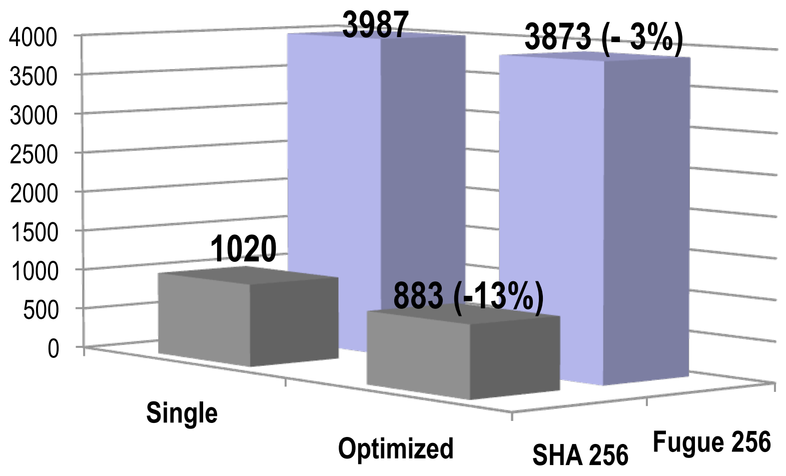
Total number of runs = 16

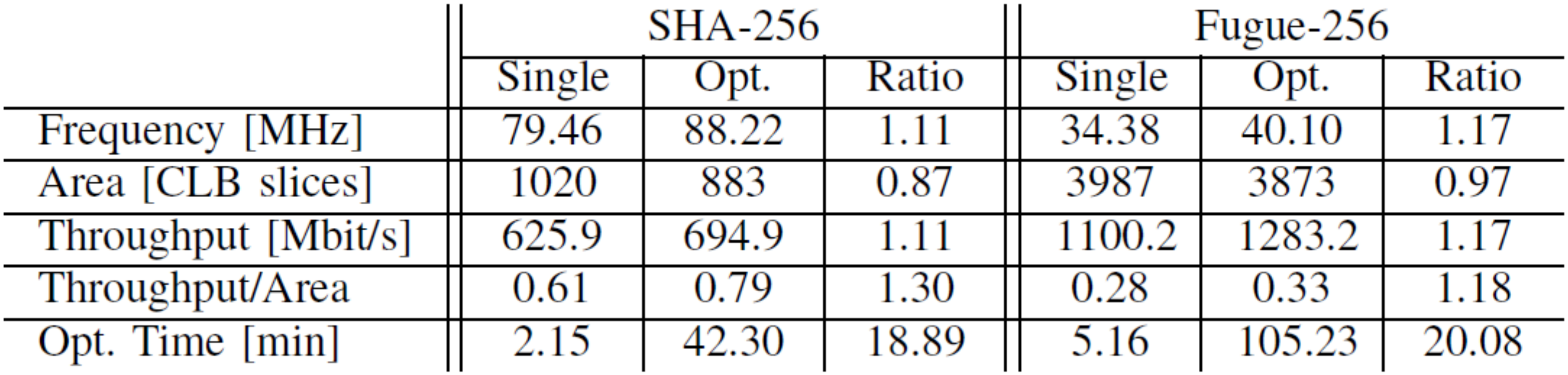
Benchmarking Goals Facilitated by ATHENa

1. comparing multiple cryptographic **algorithms**
2. comparing multiple hardware **architectures or implementations** of the same cryptographic algorithm
3. comparing various hardware **platforms** from the point of view of their suitability for the implementation of a given algorithm, such as a choice of an FPGA device or FPGA board for implementing a particular cryptographic system
4. comparing various **tools and languages** in terms of quality of results they generate (e.g. Verilog vs. VHDL, Synplicity Synplify Pro vs. Xilinx XST, ISE v. 10.2 vs. ISE v. 9.1)

Algorithm Comparison: SHA-256 vs. Fugue on Xilinx Spartan 3

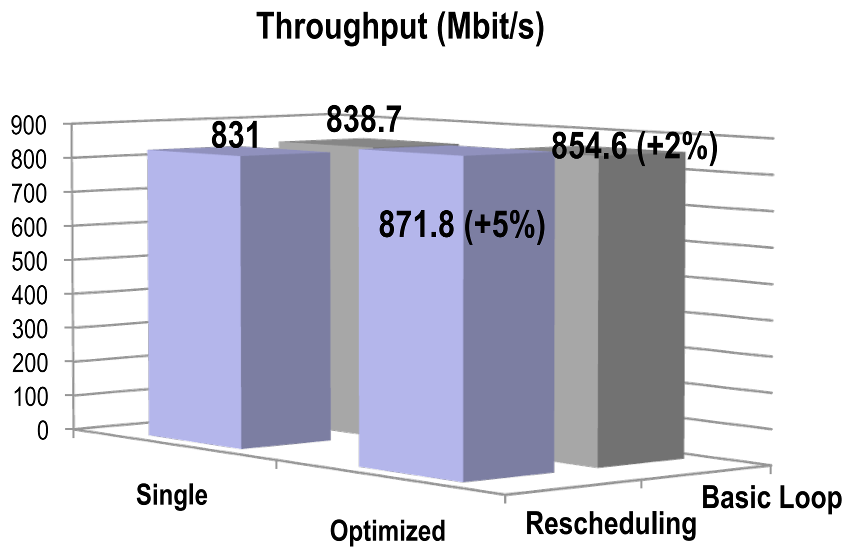

Throughput (Mbit/s)

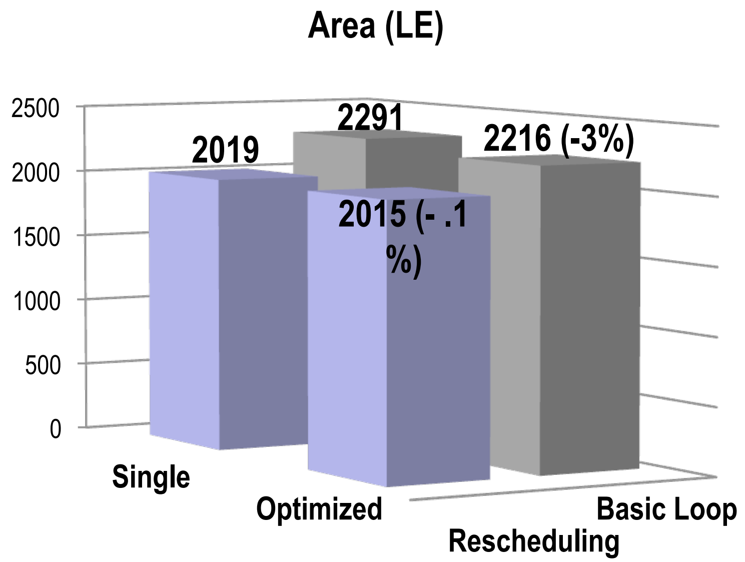

Area (CLB slices)

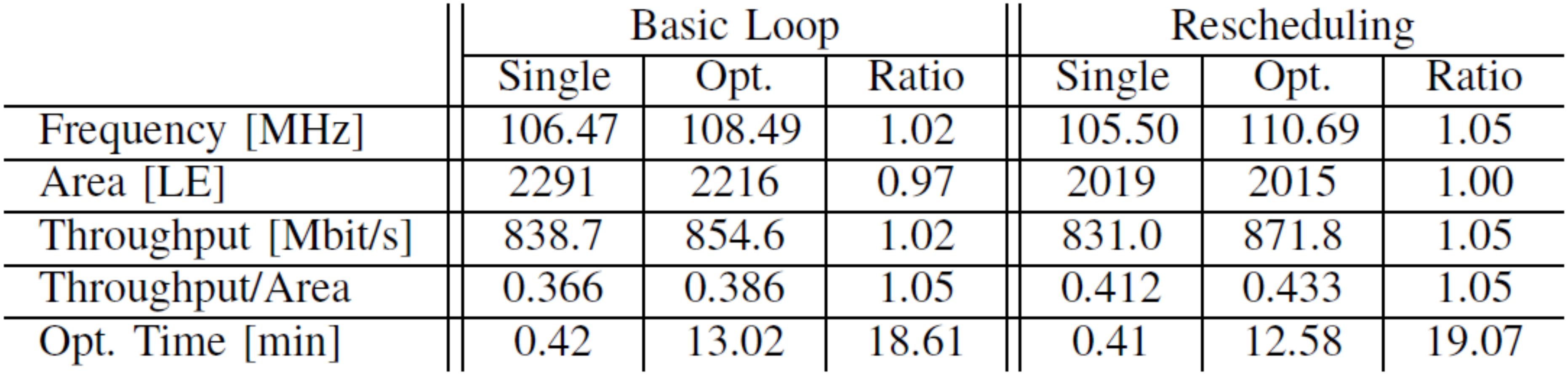


	SHA-256			Fugue-256		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	79.46	88.22	1.11	34.38	40.10	1.17
Area [CLB slices]	1020	883	0.87	3987	3873	0.97
Throughput [Mbit/s]	625.9	694.9	1.11	1100.2	1283.2	1.17
Throughput/Area	0.61	0.79	1.30	0.28	0.33	1.18
Opt. Time [min]	2.15	42.30	18.89	5.16	105.23	20.08

Architecture Comparison: SHA-256
Basic Loop vs. Rescheduling on Altera Cyclone II

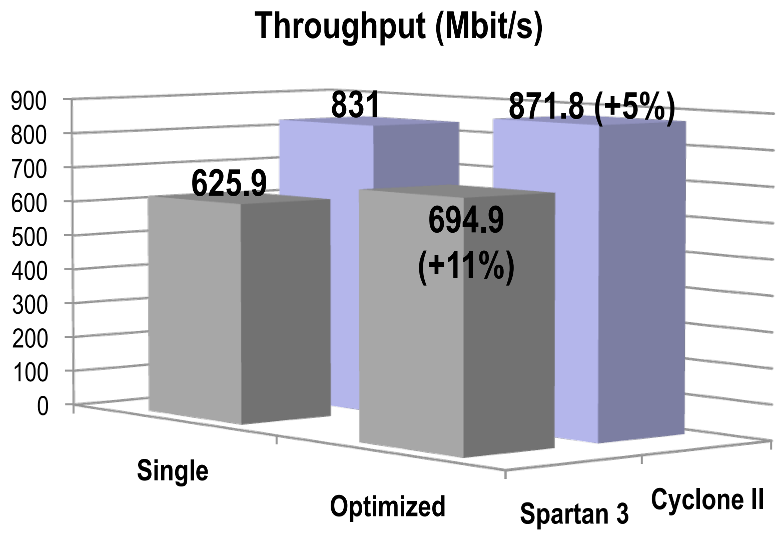


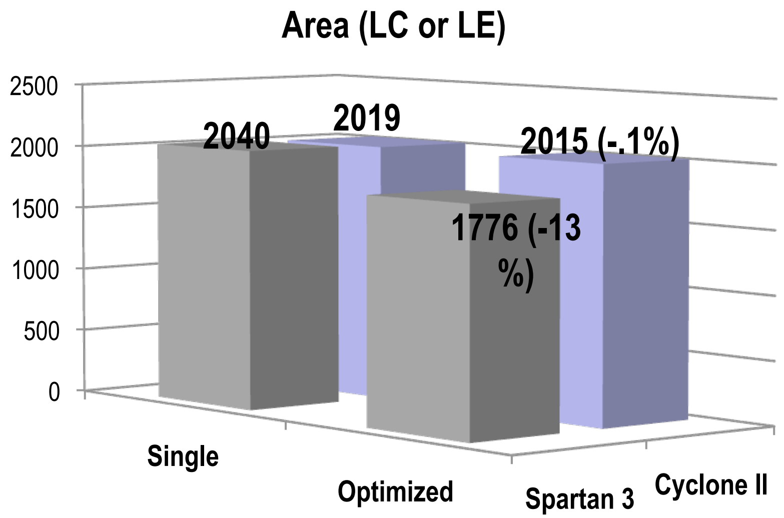


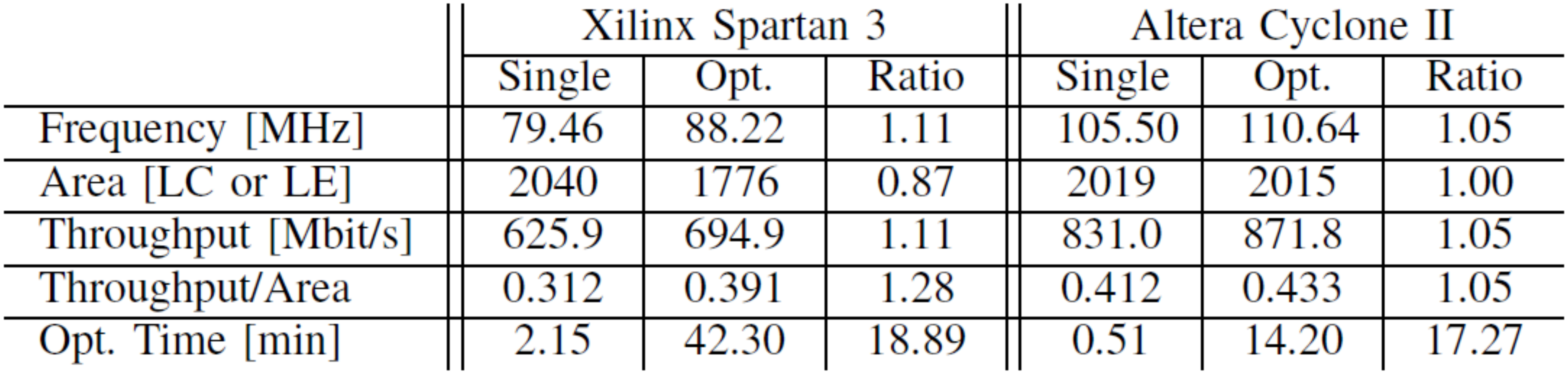


	Basic Loop			Rescheduling		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	106.47	108.49	1.02	105.50	110.69	1.05
Area [LE]	2291	2216	0.97	2019	2015	1.00
Throughput [Mbit/s]	838.7	854.6	1.02	831.0	871.8	1.05
Throughput/Area	0.366	0.386	1.05	0.412	0.433	1.05
Opt. Time [min]	0.42	13.02	18.61	0.41	12.58	19.07

Platform Comparison: SHA-256
Xilinx Spartan 3 vs. Altera Cyclone II

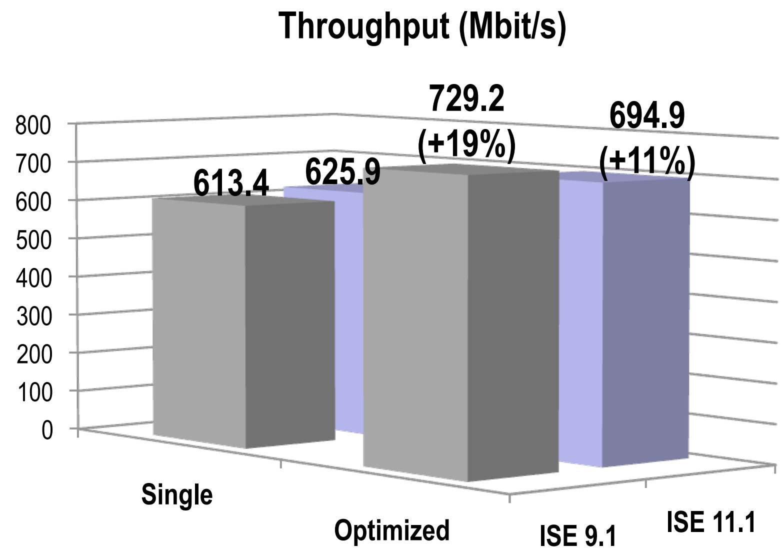


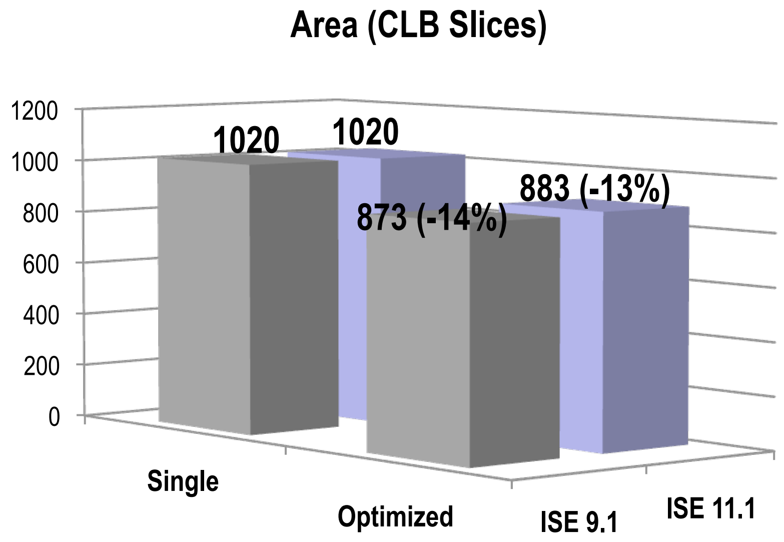


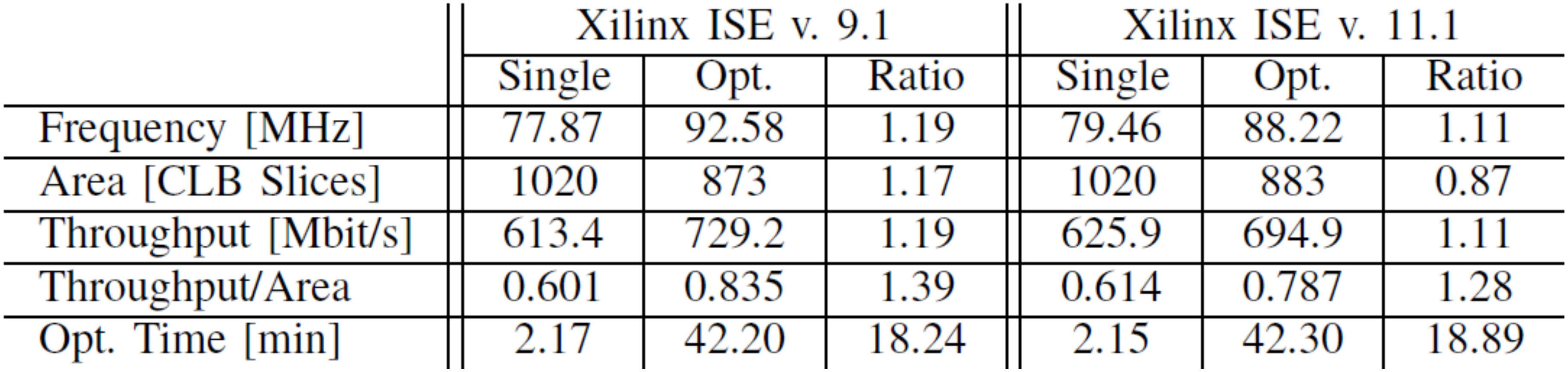


	Xilinx Spartan 3			Altera Cyclone II		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	79.46	88.22	1.11	105.50	110.64	1.05
Area [LC or LE]	2040	1776	0.87	2019	2015	1.00
Throughput [Mbit/s]	625.9	694.9	1.11	831.0	871.8	1.05
Throughput/Area	0.312	0.391	1.28	0.412	0.433	1.05
Opt. Time [min]	2.15	42.30	18.89	0.51	14.20	17.27

Tool Comparison: SHA-256 Rescheduling with ISE 9.1 vs. ISE 11.1



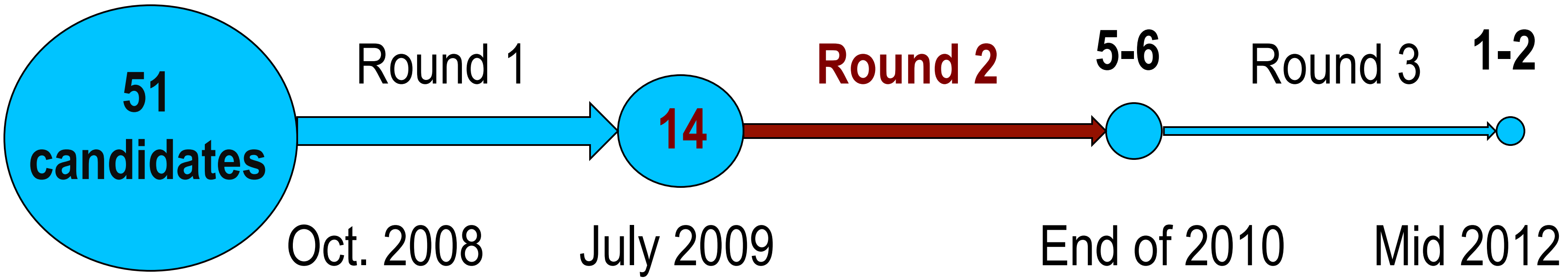




	Xilinx ISE v. 9.1			Xilinx ISE v. 11.1		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	77.87	92.58	1.19	79.46	88.22	1.11
Area [CLB Slices]	1020	873	1.17	1020	883	0.87
Throughput [Mbit/s]	613.4	729.2	1.19	625.9	694.9	1.11
Throughput/Area	0.601	0.835	1.39	0.614	0.787	1.28
Opt. Time [min]	2.17	42.20	18.24	2.15	42.30	18.89

Benchmarking of 14 Round-2 SHA-3 Candidates

- Timeline



- High-speed implementations of all 14 Round 2 SHA-3 candidates and the current standard SHA-2 developed and evaluated using ATHENa
- Results reported at CHES 2010 and at the SHA-3 conference organized by NIST

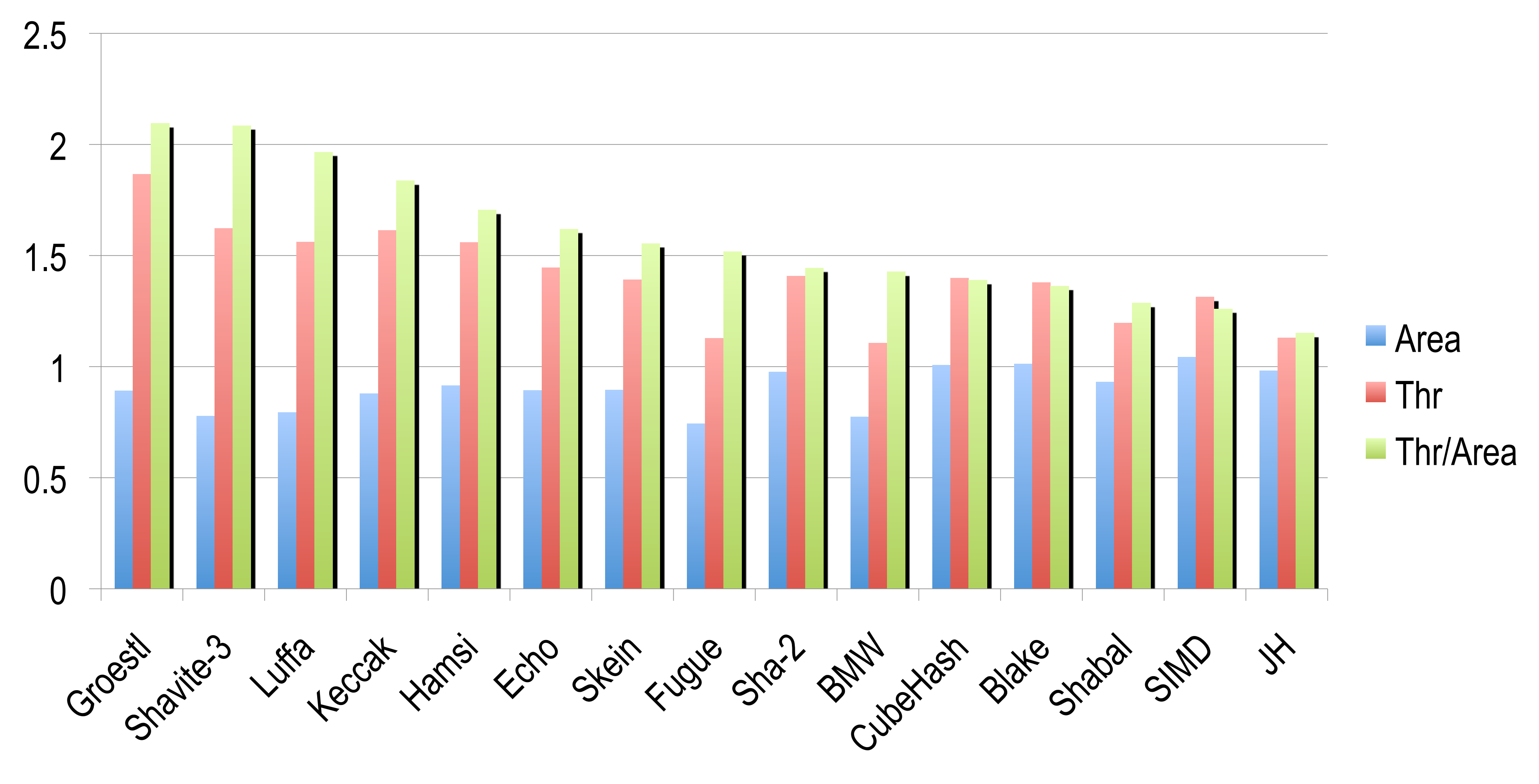
Generation of Results Facilitated by ATHENa

- batch mode of FPGA tools

vs.

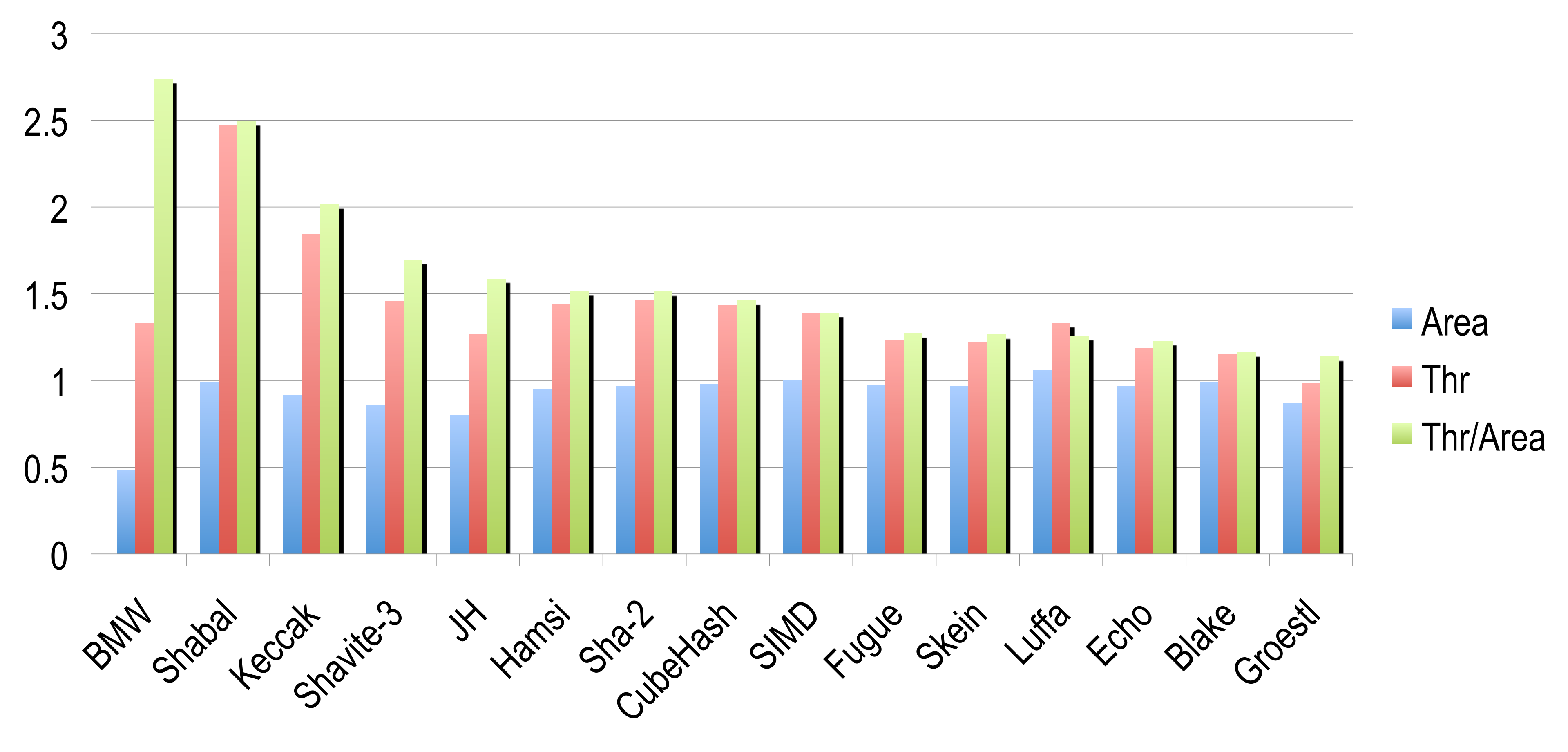
- ease of extraction and tabulation of results
  - Excel, CSV (available), LaTeX (coming soon)
- optimized choice of tool options
  - GMU_Xilinx_optimization_1 strategy

Relative Improvement of Results from Using ATHENa Virtex 5, 256-bit Variants of Hash Functions



Ratios of results obtained using ATHENa suggested options vs. default options of FPGA tools

Relative Improvement of Results from Using ATHENa Virtex 5, 512-bit Variants of Hash Functions



Ratios of results obtained using ATHENa suggested options vs. default options of FPGA tools

Most Important Features of ATHENa

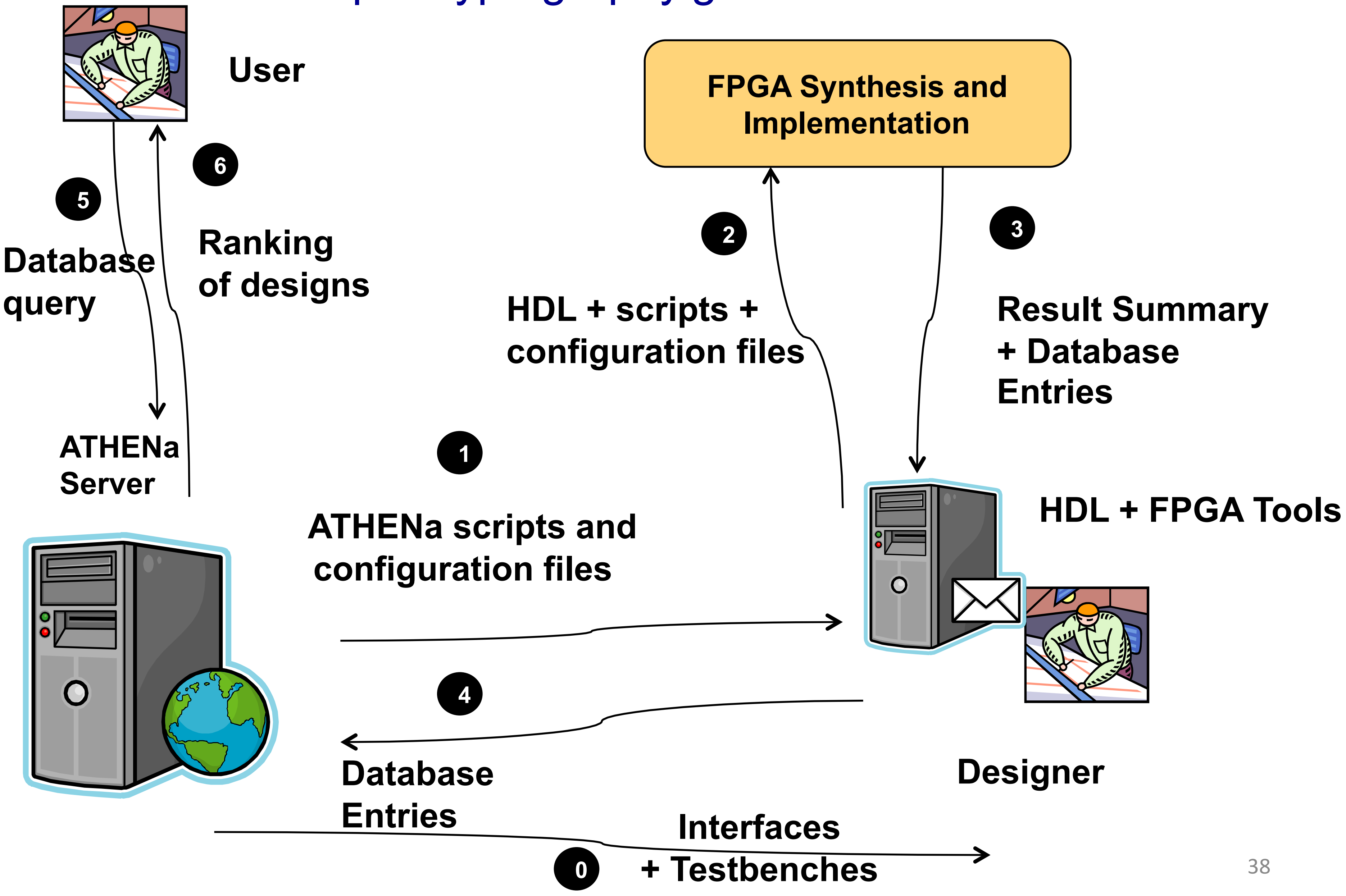
- comprehensive
- automated
- collaborative
- practical
- distributed
- optimized
- with a single point of contact

Our Environment will Serve

- **Researchers** – fair, automated, and comprehensive comparison of new algorithms, architectures, and implementations with previously reported work
- **Designers** – informed choice of technology (FPGA, ASIC, microprocessor) and a specific device within a given technology
- **Developers and Users of Tools** – comprehensive comparison across various tools; optimization methodologies developed and comprehensively tested as a part of this project
- **Standardization Organizations** (such as NIST) – evaluation of existing and emerging standards; support of contests for new standards; comprehensive and easy to locate database of results

Invitation to Use ATHENa

http://cryptography.gmu.edu/athena



User

ATHENa Server

HDL + FPGA Tools

Designer

FPGA Synthesis and Implementation

0 Interfaces + Testbenches

1 ATHENa scripts and configuration files

2 HDL + scripts + configuration files

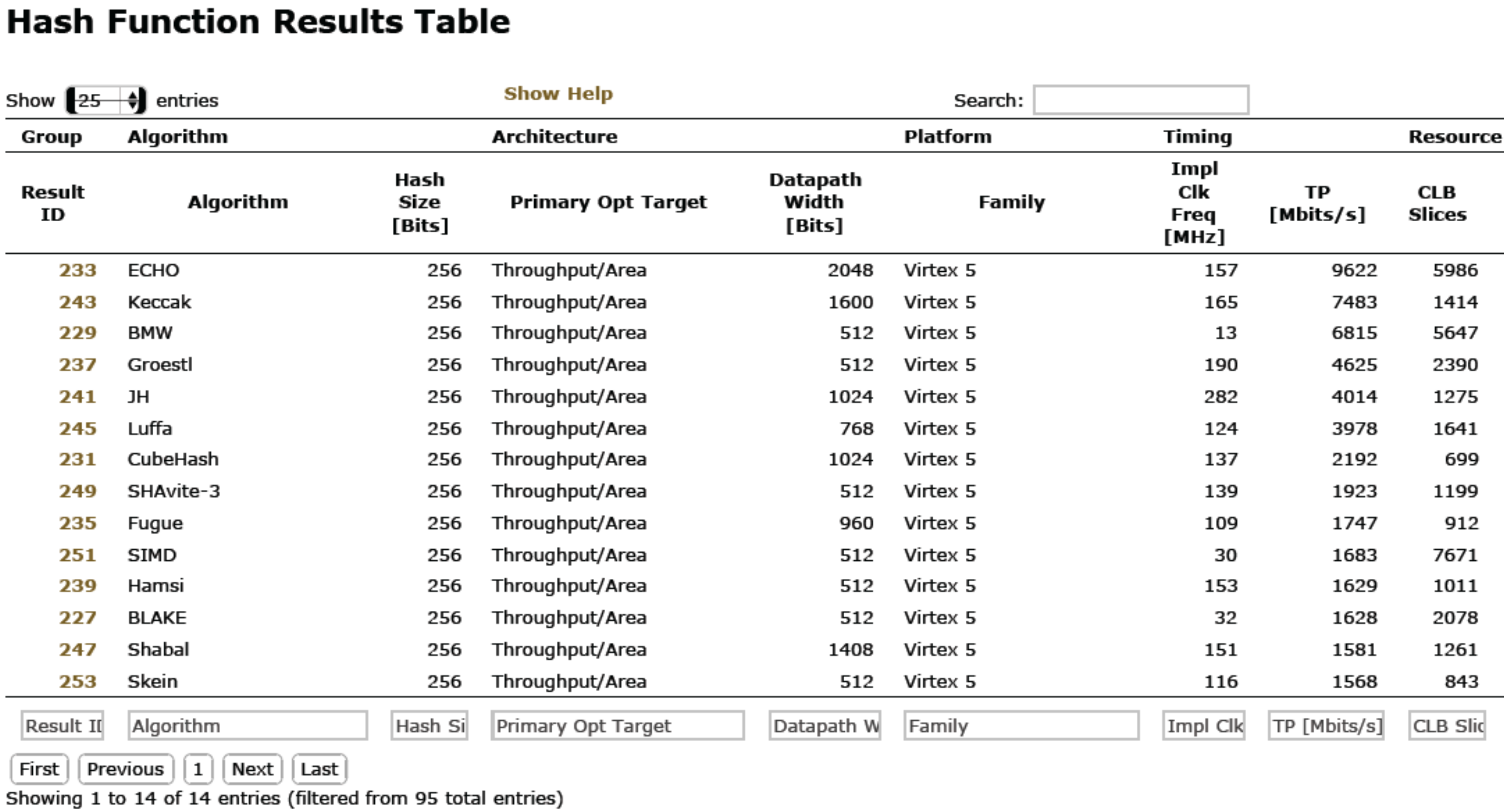
3 Result Summary + Database Entries

4 Database Entries

5 Database query

6 Ranking of designs

Hash Function Results Table



Show 25 entries Show Help Search:

Group	Algorithm		Architecture		Platform	Timing		Resource
Result ID	Algorithm	Hash Size [Bits]	Primary Opt Target	Datapath Width [Bits]	Family	Impl Clk Freq [MHz]	TP [Mbits/s]	CLB Slices
233	ECHO	256	Throughput/Area	2048	Virtex 5	157	9622	5986
243	Keccak	256	Throughput/Area	1600	Virtex 5	165	7483	1414
229	BMW	256	Throughput/Area	512	Virtex 5	13	6815	5647
237	Groestl	256	Throughput/Area	512	Virtex 5	190	4625	2390
241	JH	256	Throughput/Area	1024	Virtex 5	282	4014	1275
245	Luffa	256	Throughput/Area	768	Virtex 5	124	3978	1641
231	CubeHash	256	Throughput/Area	1024	Virtex 5	137	2192	699
249	SHAvite-3	256	Throughput/Area	512	Virtex 5	139	1923	1199
235	Fugue	256	Throughput/Area	960	Virtex 5	109	1747	912
251	SIMD	256	Throughput/Area	512	Virtex 5	30	1683	7671
239	Hamsi	256	Throughput/Area	512	Virtex 5	153	1629	1011
227	BLAKE	256	Throughput/Area	512	Virtex 5	32	1628	2078
247	Shabal	256	Throughput/Area	1408	Virtex 5	151	1581	1261
253	Skein	256	Throughput/Area	512	Virtex 5	116	1568	843
Result II	Algorithm	Hash Si	Primary Opt Target	Datapath W	Family	Impl Clk	TP [Mbits/s]	CLB Slic

Showing 1 to 14 of 14 entries (filtered from 95 total entries)

Future Work

- Additional FPGA Vendors
- More Efficient and Effective Heuristic Optimization Algorithms
- Support for Linux
- Graphical User Interface
- Application to Comparison and Optimization of Other Cryptographic Primitives (e.g., public key cryptosystems)
- Adapting ATHENa to Other Application Domains

  (Digital Signal Processing, communications, etc.)

Thank you!

Questions?

Questions?

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