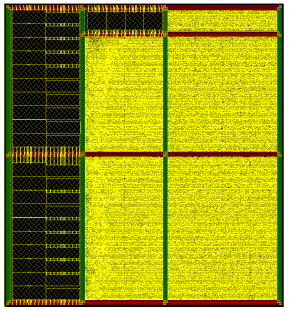
ATHENa – Automated Tool for Hardware EvaluatioN:

Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware using FPGAs

Kris Gaj, Jens-Peter Kaps,
Venkata Amirineni, Marcin Rogawski,
Ekawat Homsirikamol,
Benjamin Y. Brewster, John Pham,
and Michal Varchola

Modern Benchmarking: Natural Progression of Tools

Software | **FPGAs** | **ASICs**



eBACS

D. Bernstein,
T. Lange

?

?

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

http://cryptography.gmu.edu/athena

Set of scripts 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

FPGA Synthesis and Implementation

6

5

Database query

Ranking of designs

2

3

HDL + scripts + configuration files

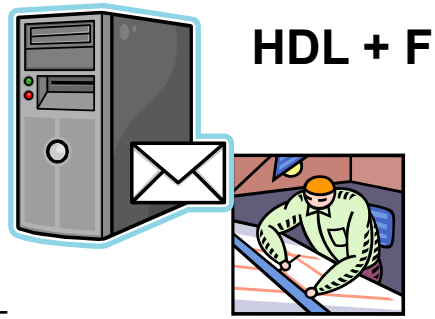
Result Summary + Database Entries

ATHENa Server

1

Download scripts and configuration files

HDL + FPGA Tools



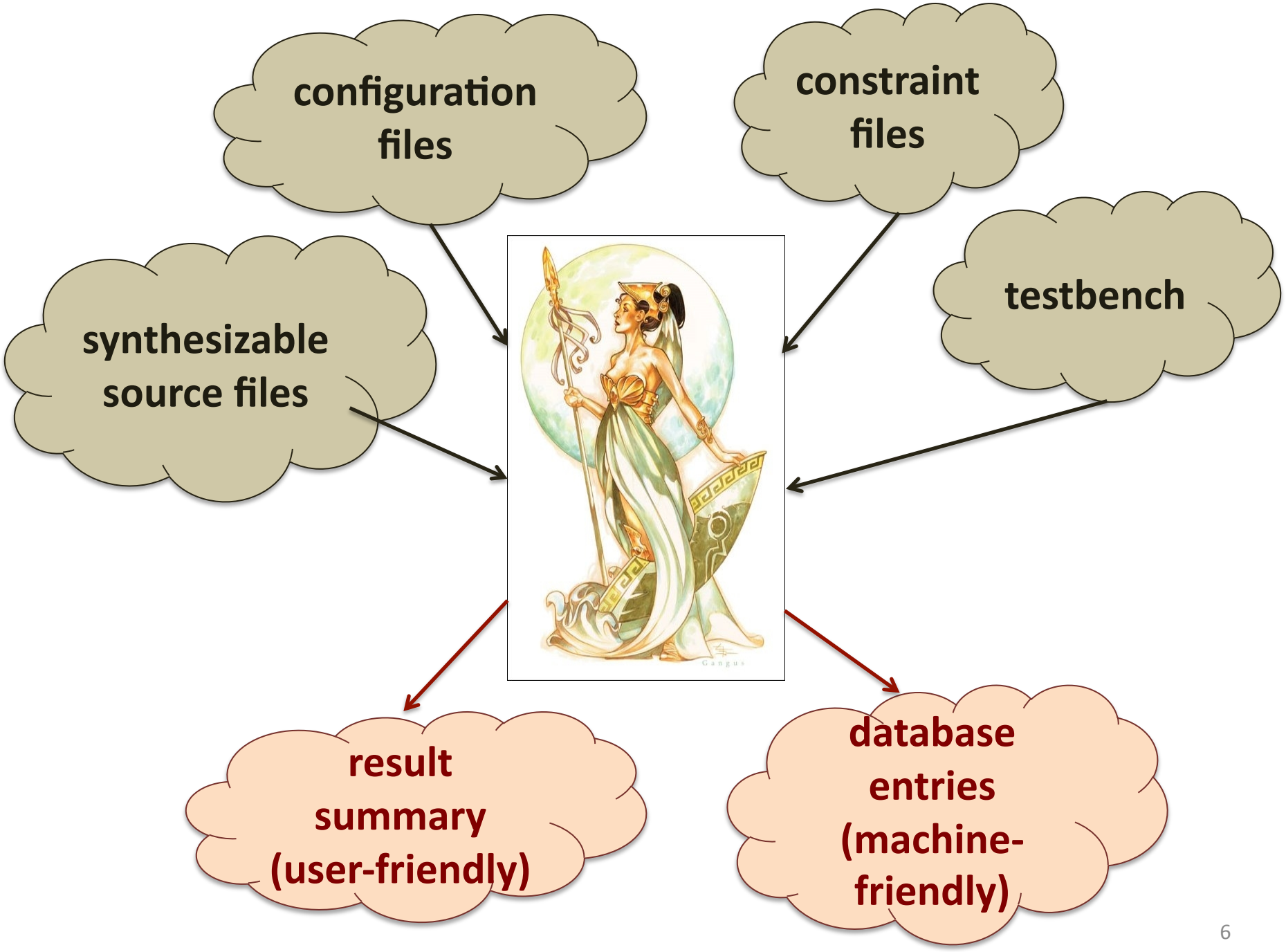
4

Database Entries

Designer

0

Interfaces + Testbenches

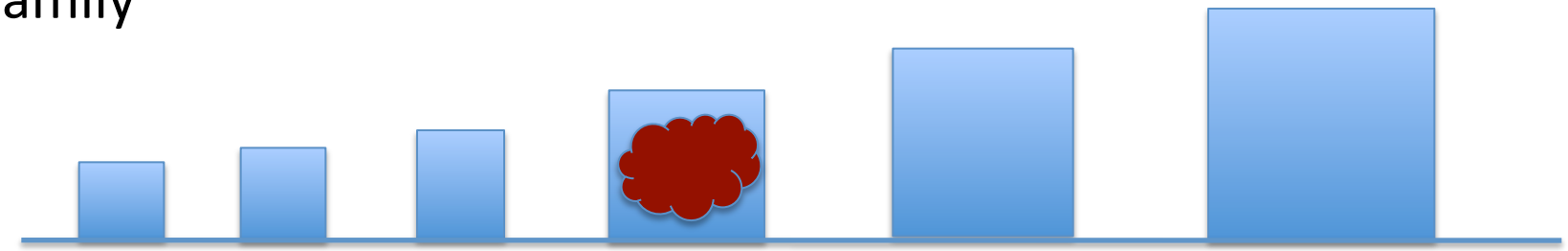

configuration files
constraint files
synthesizable source files
testbench
result summary (user-friendly)
database entries (machine-friendly)

ATHENa Major Features (1)

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

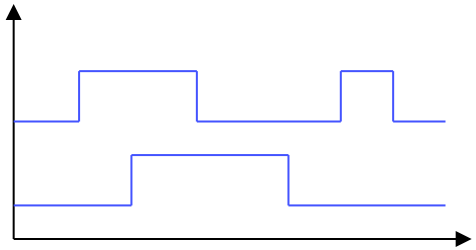
- generation of results for **multiple families** of FPGAs of a given vendor

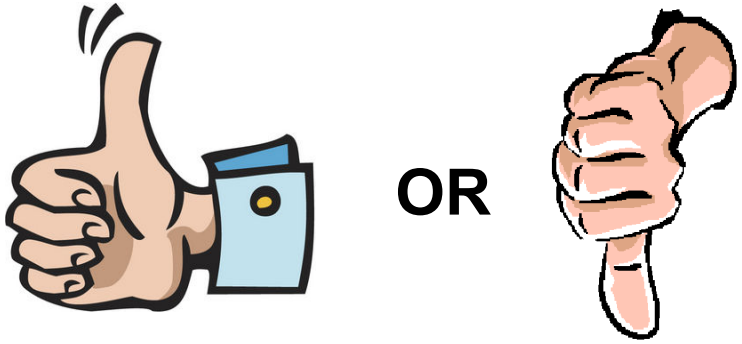
- automated choice of a **best-matching device** within a given family



ATHENa Major Features (2)

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



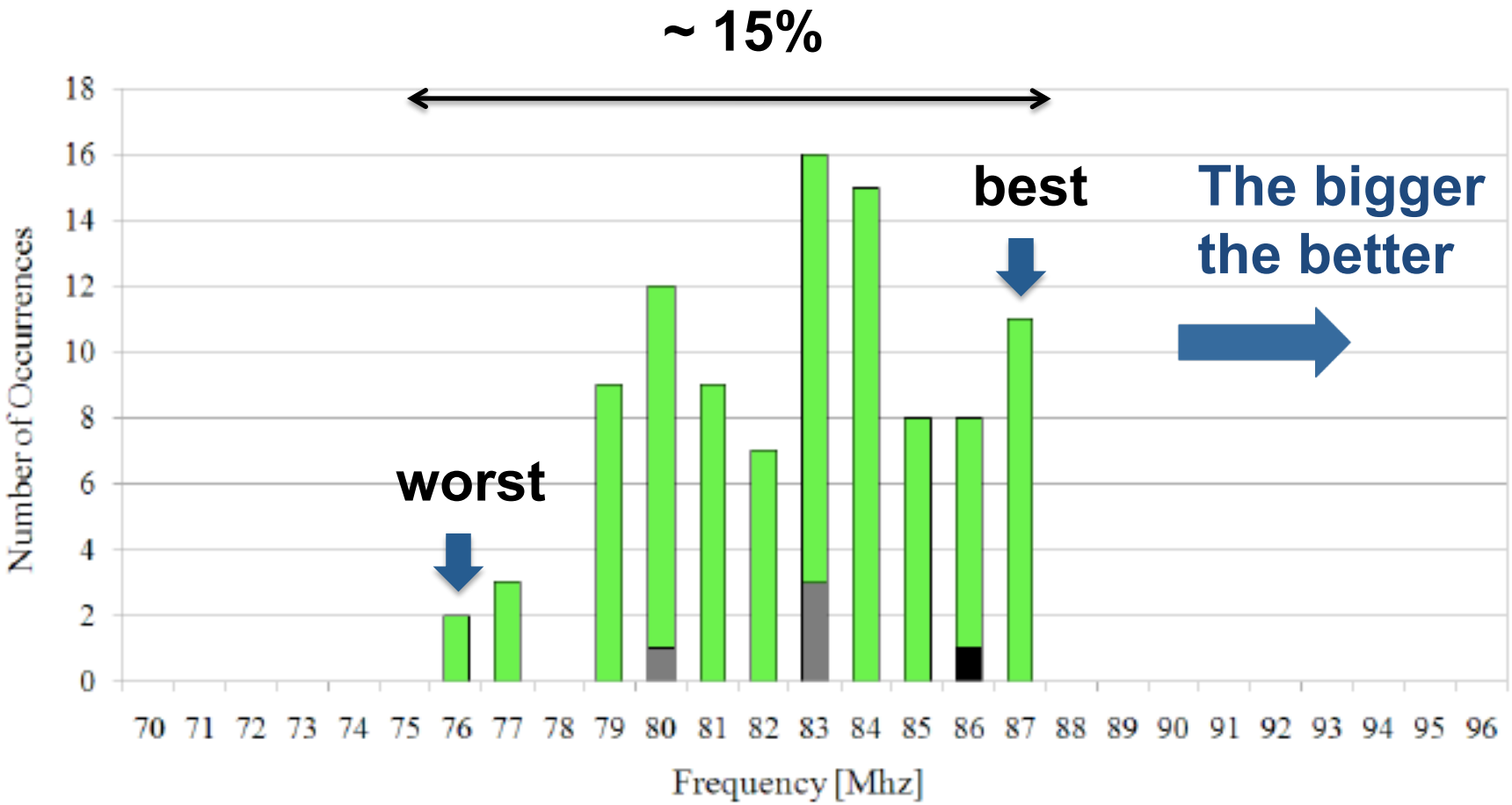


- support for **multi-core processing**
- several **optimization strategies:**
  - **exhaustive search** for optimum options of tools
  - **placement search** for the best starting point of placement
  - **frequency search** for the best requested clock frequency
  - more strategies under development

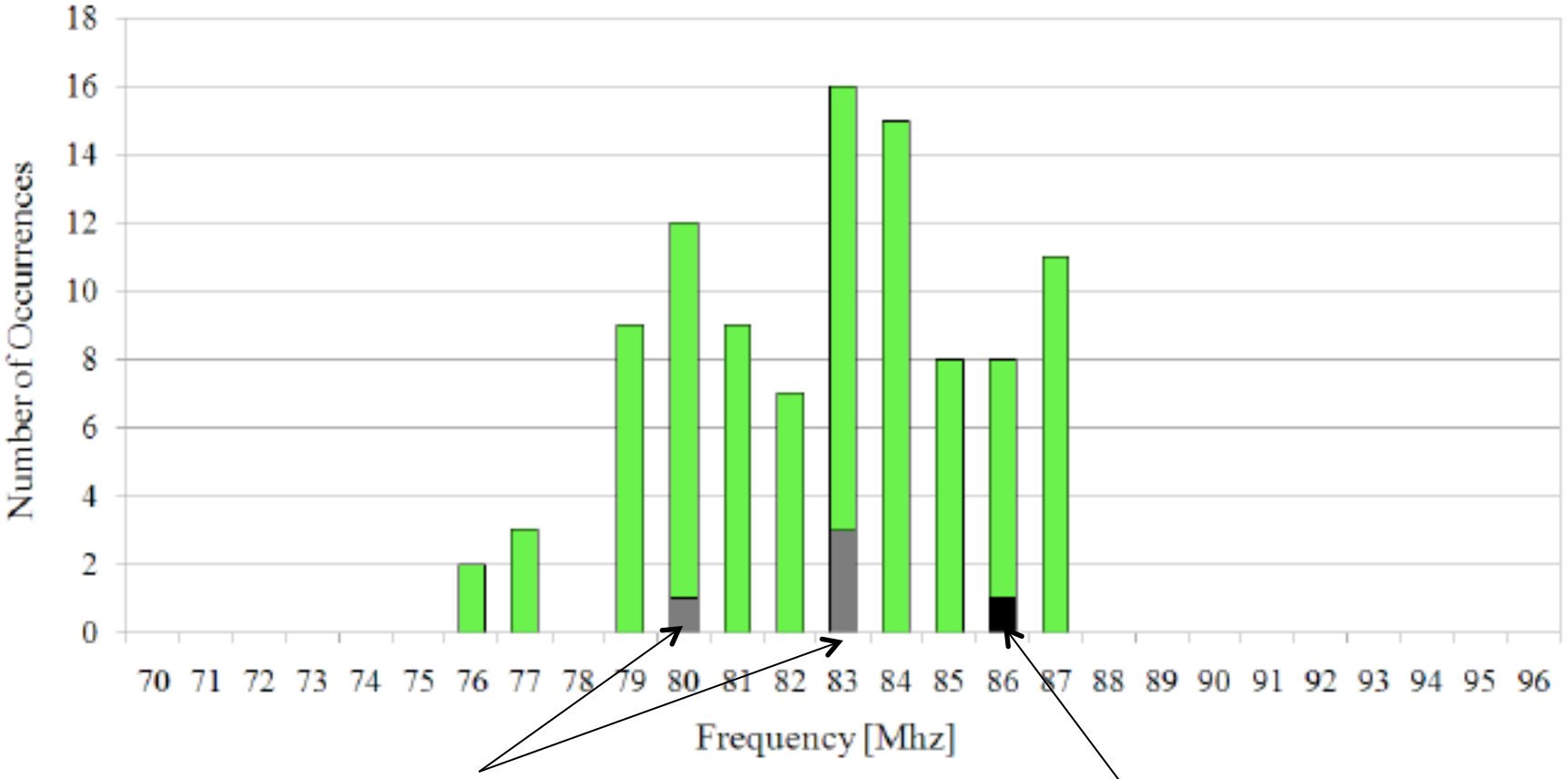
Multi-Pass Place-and-Route Analysis

GMU SHA-256, Xilinx Spartan 3

100 runs for different placement starting points



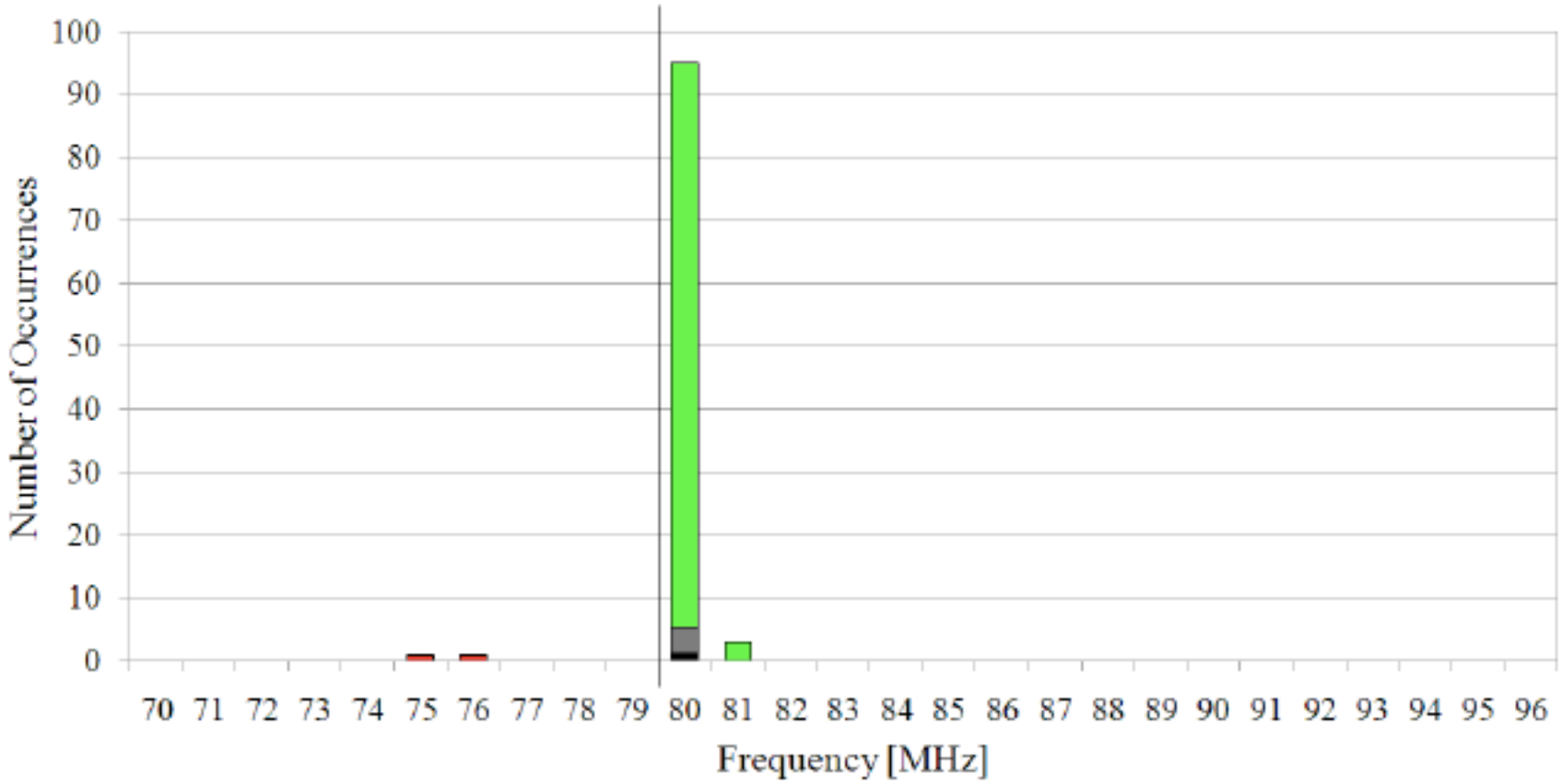
Results for default target clock frequency



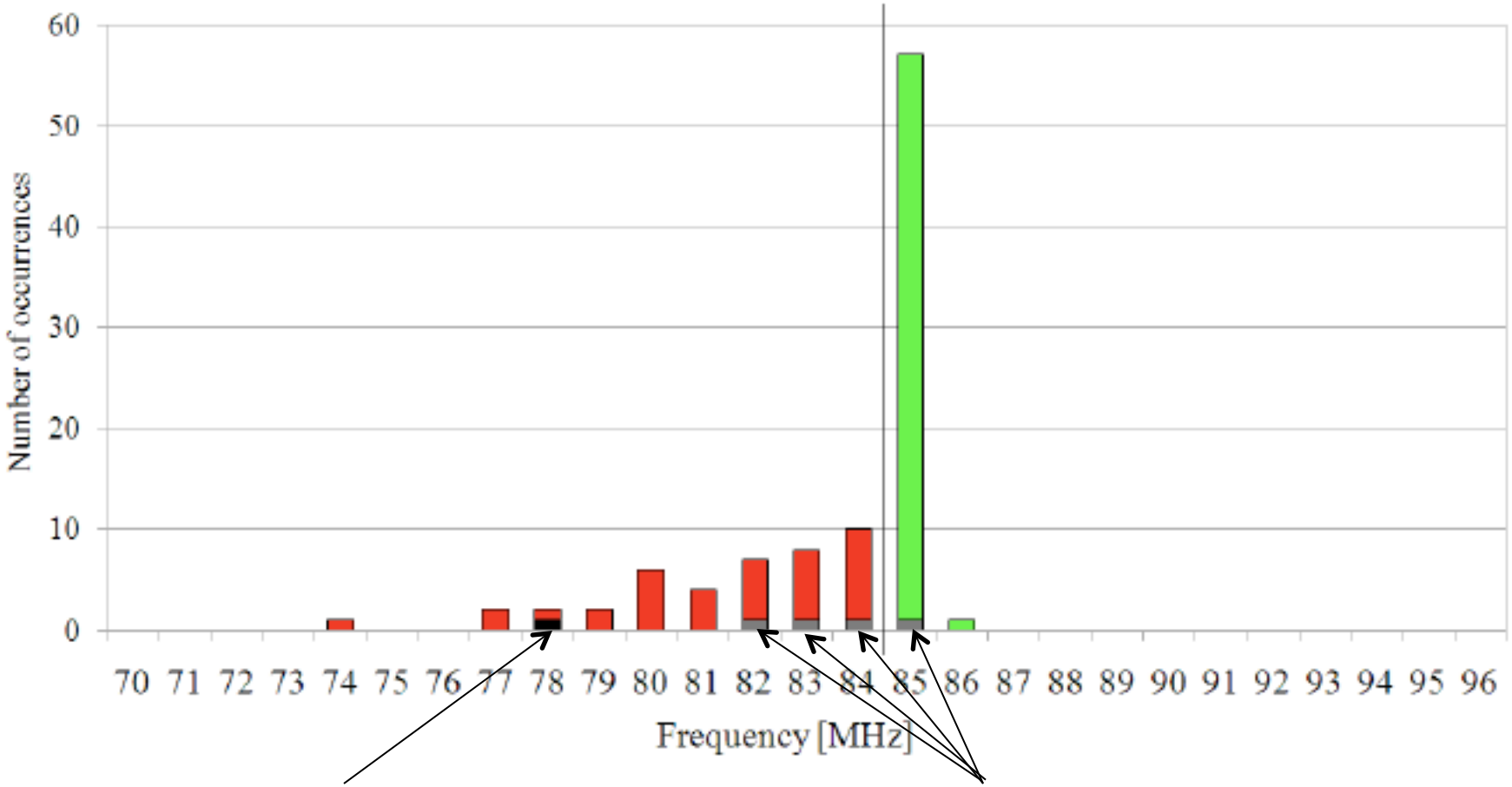
preselected COST_TABLEs (21, 41, 61, 81)

default COST_TABLE (1)

Results for target clock frequency = 80 MHz



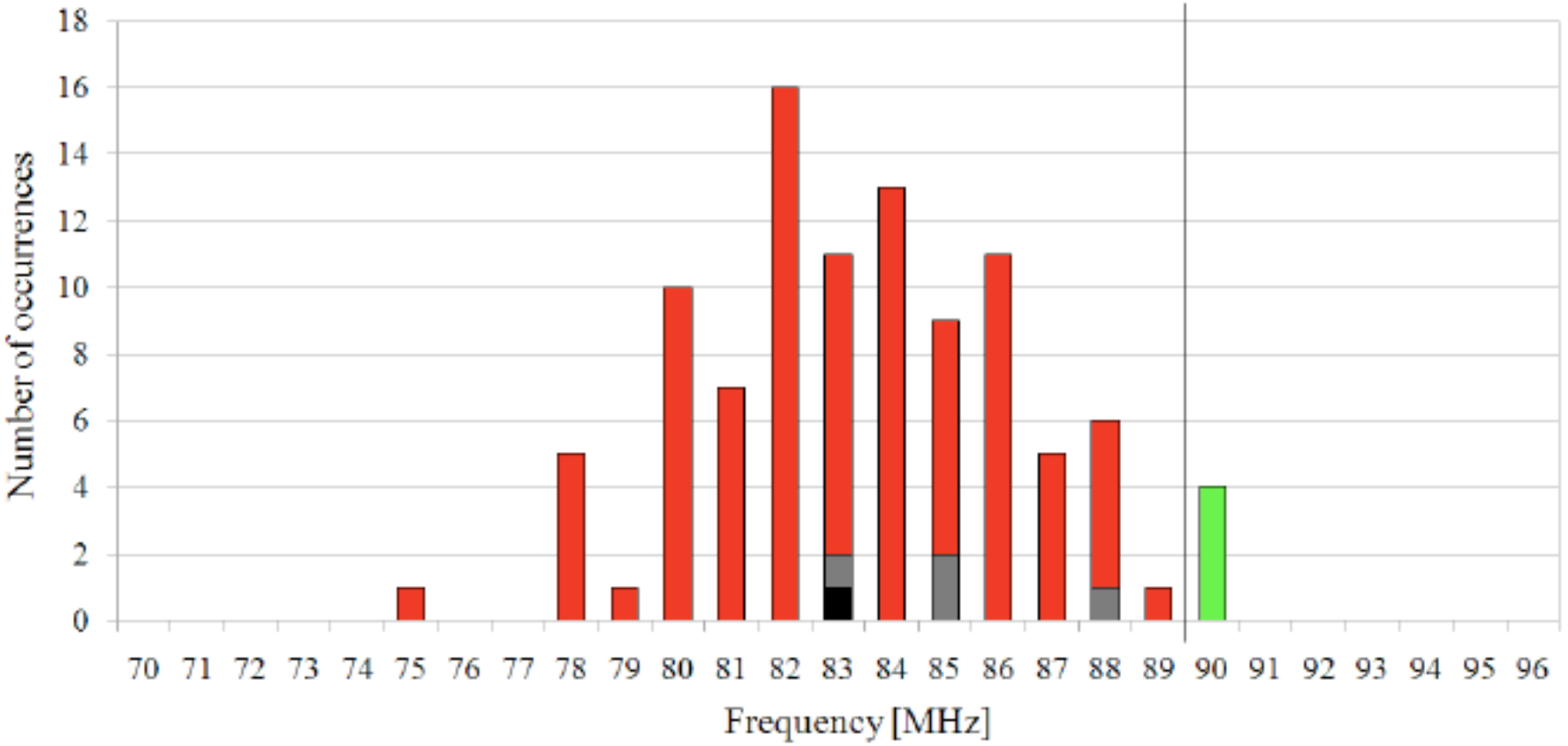
Results for target clock frequency = 85 MHz



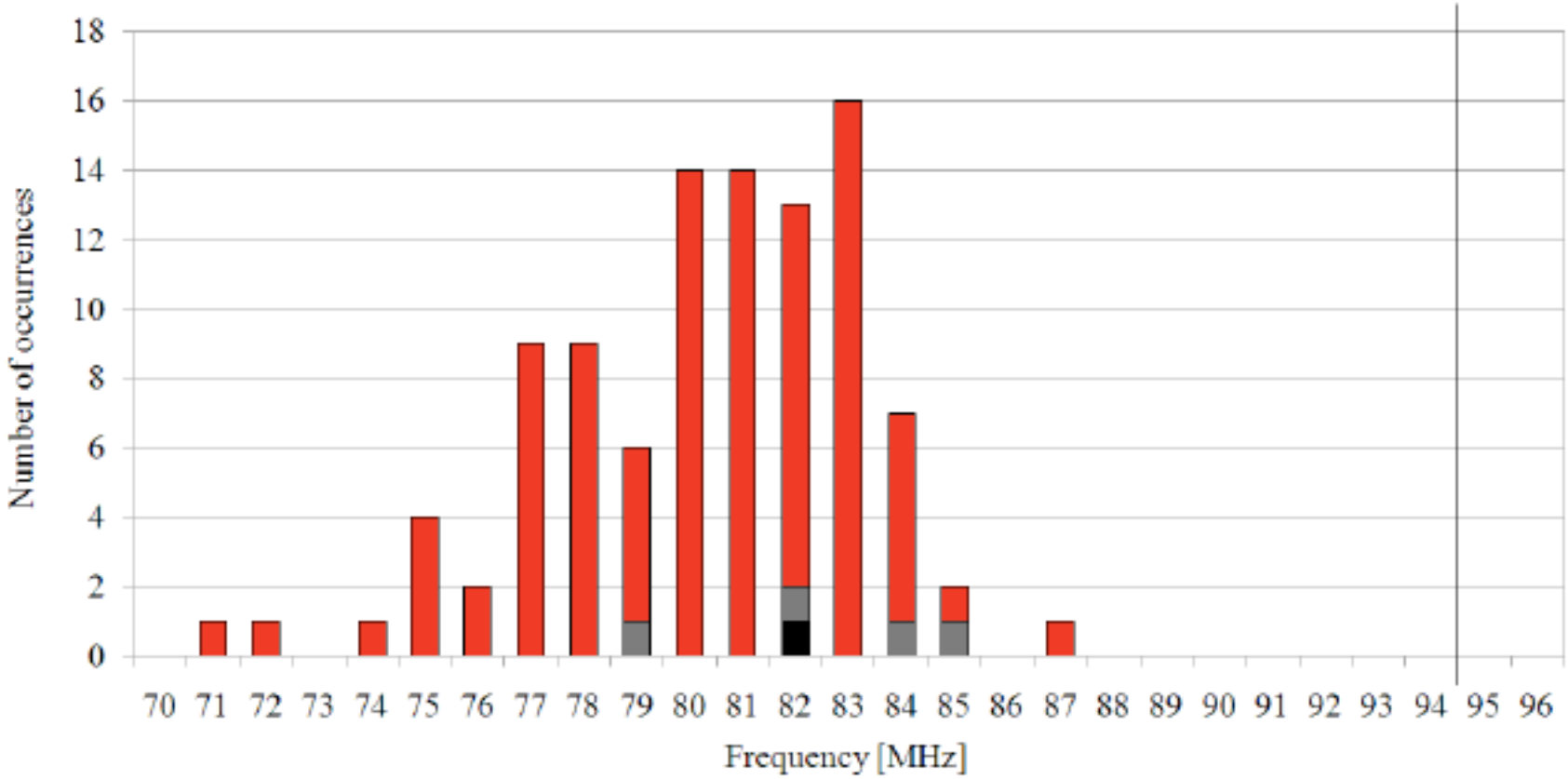
default COST_TABLE (1)

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

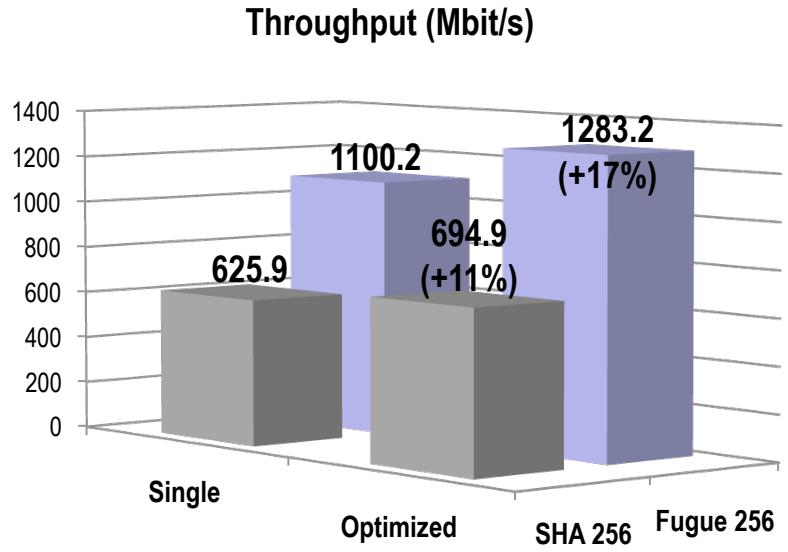
   Search for the best starting point of placement,
   using 4 additional values of SEED {2001, 4001, 6001, 8001}.

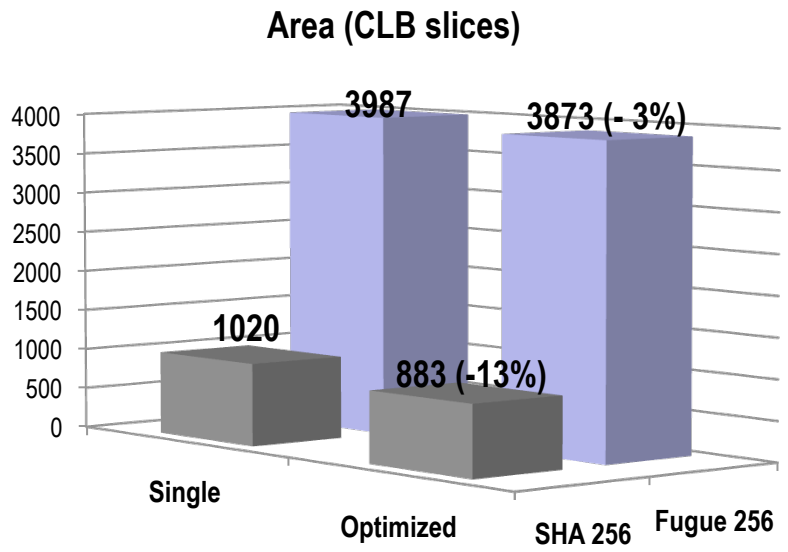
Total number of runs = 16

Goals

1. comparing multiple cryptographic **algorithms** competing in the contests for national and international standards, such as SHA-3 contest
2. comparing multiple hardware **architectures or implementations** of the same cryptographic algorithm, such as a paper for CryptArchi or CHES
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. Synplicity Synplify Pro vs. Xilinx XST, Verilog vs. VHDL vs. AHDL), ISE v. 10.2 vs. ISE v. 9.1, etc.)

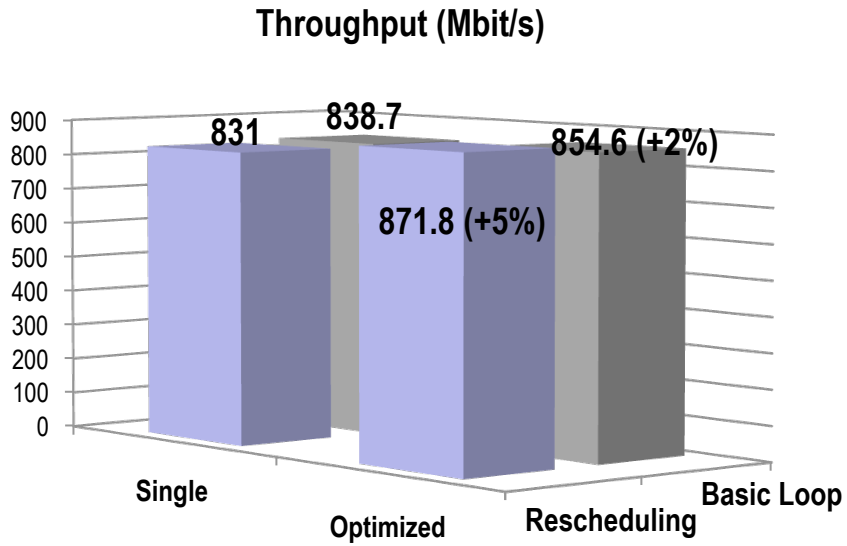
Algorithm Comparison: SHA-256 vs. Fugue on Xilinx Spartan 3

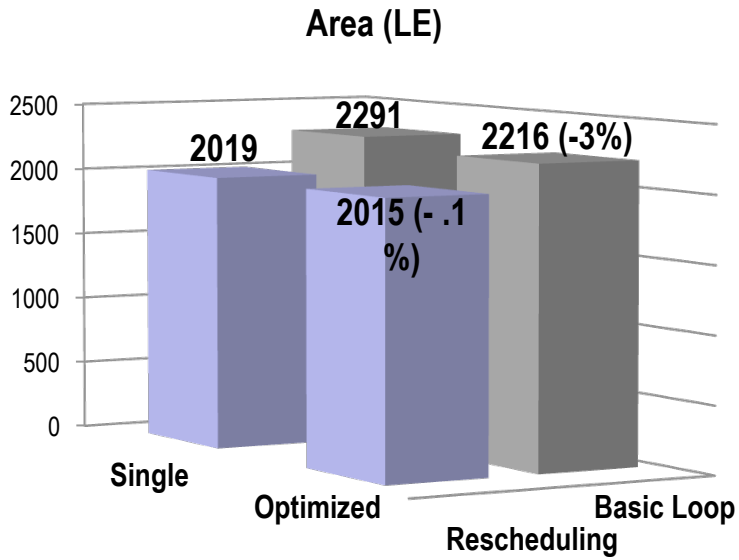




	SHA-256			Fugue-256		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	79.46	88.22	1.11	34.38	40.10	1.17
Area [CLB slices]	1020	883	0.87	3987	3873	0.97
Throughput [Mbit/s]	625.9	694.9	1.11	1100.2	1283.2	1.17
Throughput/Area	0.61	0.79	1.30	0.28	0.33	1.18
Opt. Time [min]	2.15	42.30	18.89	5.16	105.23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

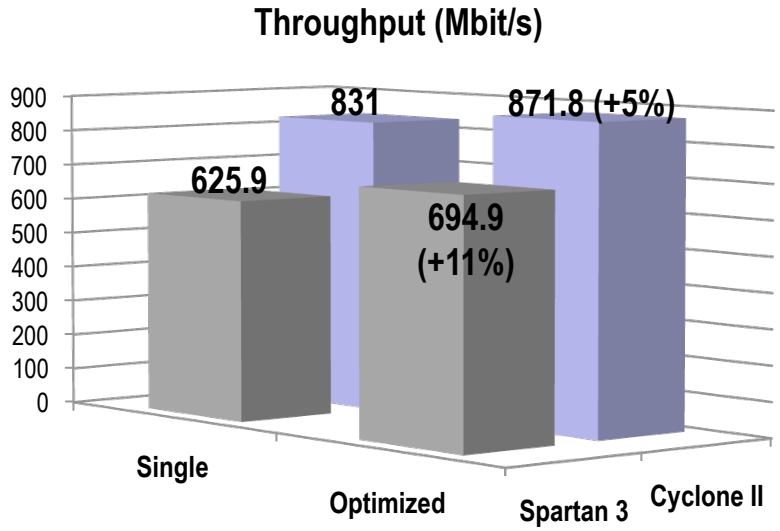
Architecture Comparison: SHA-256
Basic Loop vs. Rescheduling on Altera Cyclone II

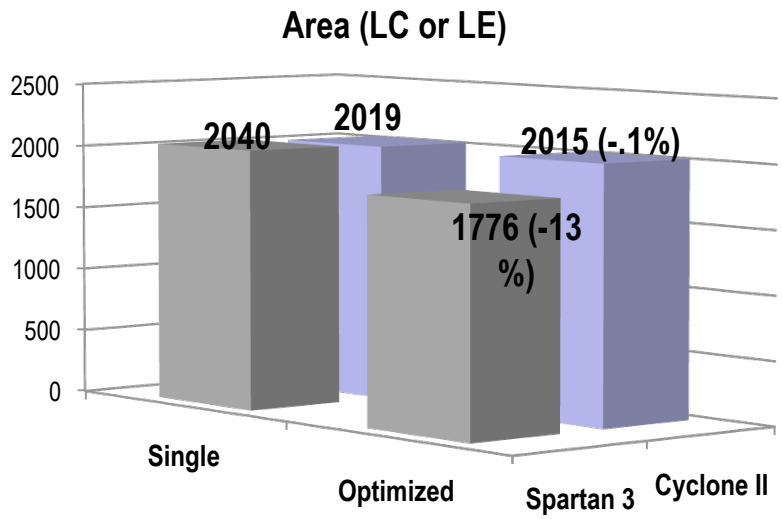




	Basic Loop			Rescheduling		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	106.47	108.49	1.02	105.50	110.69	1.05
Area [LE]	2291	2216	0.97	2019	2015	1.00
Throughput [Mbit/s]	838.7	854.6	1.02	831.0	871.8	1.05
Throughput/Area	0.366	0.386	1.05	0.412	0.433	1.05
Opt. Time [min]	0.42	13.02	18.61	0.41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

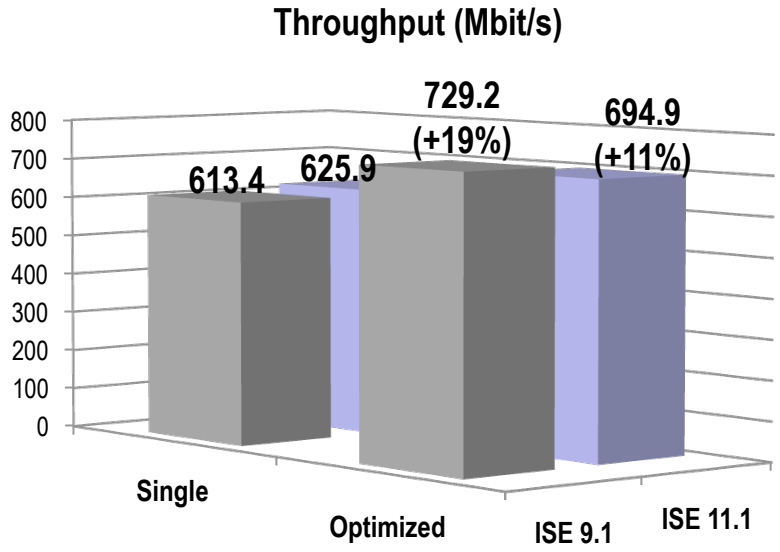
Platform Comparison: SHA-256
Xilinx Spartan 3 vs. Altera Cyclone II

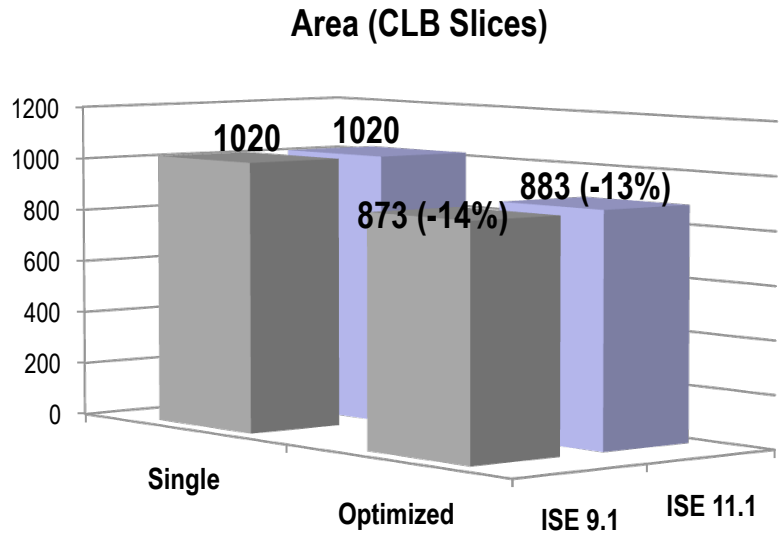




	Xilinx Spartan 3			Altera Cyclone II		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	79.46	88.22	1.11	105.50	110.64	1.05
Area [LC or LE]	2040	1776	0.87	2019	2015	1.00
Throughput [Mbit/s]	625.9	694.9	1.11	831.0	871.8	1.05
Throughput/Area	0.312	0.391	1.28	0.412	0.433	1.05
Opt. Time [min]	2.15	42.30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

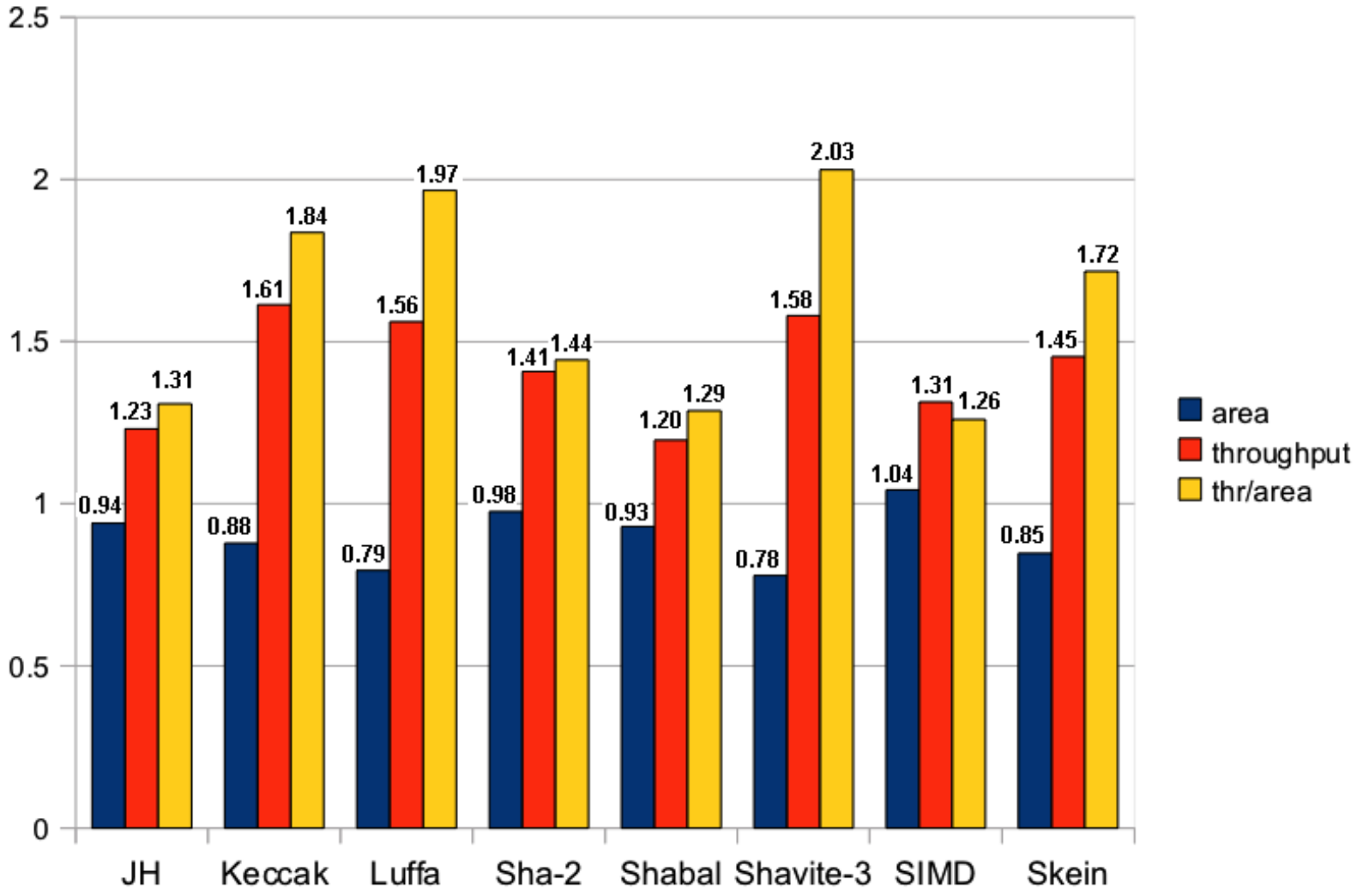
Tool Comparison: SHA-256 Rescheduling with ISE 9.1 vs. ISE 11.1



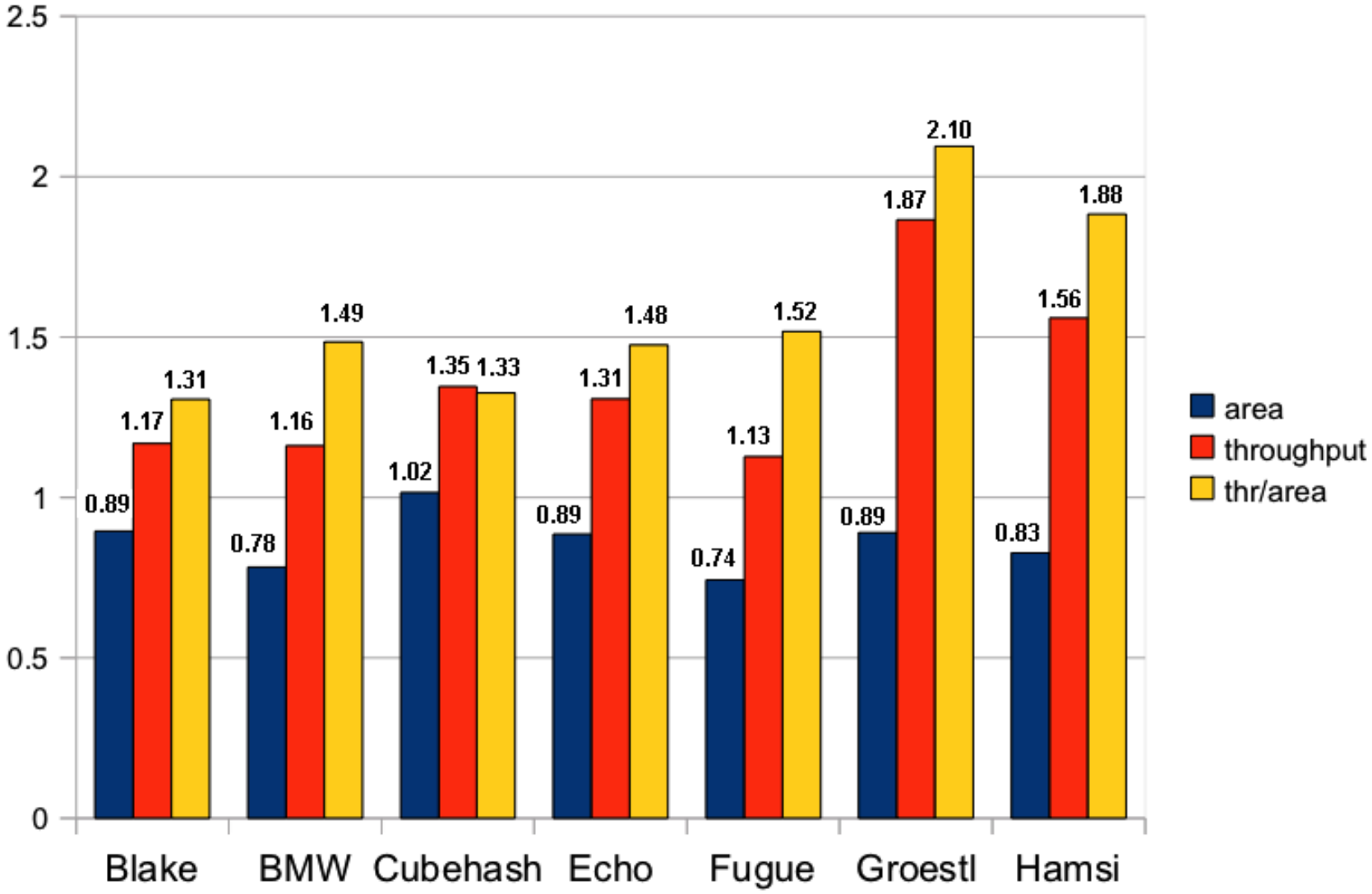


	Xilinx ISE v. 9.1			Xilinx ISE v. 11.1		
	Single	Opt.	Ratio	Single	Opt.	Ratio
Frequency [MHz]	77.87	92.58	1.19	79.46	88.22	1.11
Area [CLB Slices]	1020	873	1.17	1020	883	0.87
Throughput [Mbit/s]	613.4	729.2	1.19	625.9	694.9	1.11
Throughput/Area	0.601	0.835	1.39	0.614	0.787	1.28
Opt. Time [min]	2.17	42.20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

Relative Improvement for SHA-3 Candidates (1)



Relative Improvement for SHA-3 Candidates (2)



Future Work

- Support for additional synthesis tools (e.g., Synplify Pro)
- Support for new devices (Spartan 6, Virtex 6, Cyclone IV, Stratix IV)
- Additional FPGA Vendors (Actel)
- 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