# ATHENa - Automated Tools for Hardware EvaluatioN

Kris Gaj[1], Jens-Peter Kaps[1], Venkata Amirineni[1], Ekawat Homsirikamol[1], Marcin Rogawski[1], Rajesh Velegalati[1], and Michal Varchola[2]

[1]George Mason University, USA

[2]Technical University of Kosice, Slovakia

## Motivation

Comparison of FPGA implementations of cryptographic algorithms that is

- **fair** : based on objective criteria
- **comprehensive** : based on multiple FPGA devices and CAD software tools
- **automated** : all tools run in a batch mode, without user supervision
- **reliable** : reproducible
- **does not require revealing the code** : practical, acceptable for majority of designers

## Previous Work

**eBACS: E**CRYPT **B**enchmarking of **C**ryptographic **S**ystems
http://bench.cr.yp.to

Project to compare **software implementations** of cryptographic algorithms developed by: Daniel J. Bernstein and Tanja Lange (2006-present)

- ❖ multiple types of cryptographic algorithms
- ❖ standardized function arguments (APIs)
- ❖ measurements performed on multiple machines (currently over 70)
- ❖ choice of best compilation options (from among over 1200 different combinations)
- ❖ time measured in clock cycles/byte for multiple input/output sizes
- ❖ output suitable for easy computer processing

| Software | FPGAs |
|---|---|
| **few major vendors** | |
| Intel, AMD | Xilinx, Altera |
| **free software tools** | |
| GNU compilers | Xilinx WebPACK<br>Altera Quartus Web Edition |
| **multiple options of tools** | |
| **low-level optimizations possible but not portable** | |
| assembly language | IP cores, manual placement & routing |

| Software | FPGAs |
|---|---|
| **Optimization target** | |
| execution time, memory | speed, area, power, balanced |
| **Optimization of** | |
| optimum sequence of instructions | optimum structure of the circuit |
| **Memory management** | |
| multiple levels of memory hierarchy | simple memory hierarchy |
| **Execution Time** | |
| measured directly | calculated based on results of timing analysis |

## Proposed Solution

### ATHENa – Automated Tool for Hardware EvaluatioN

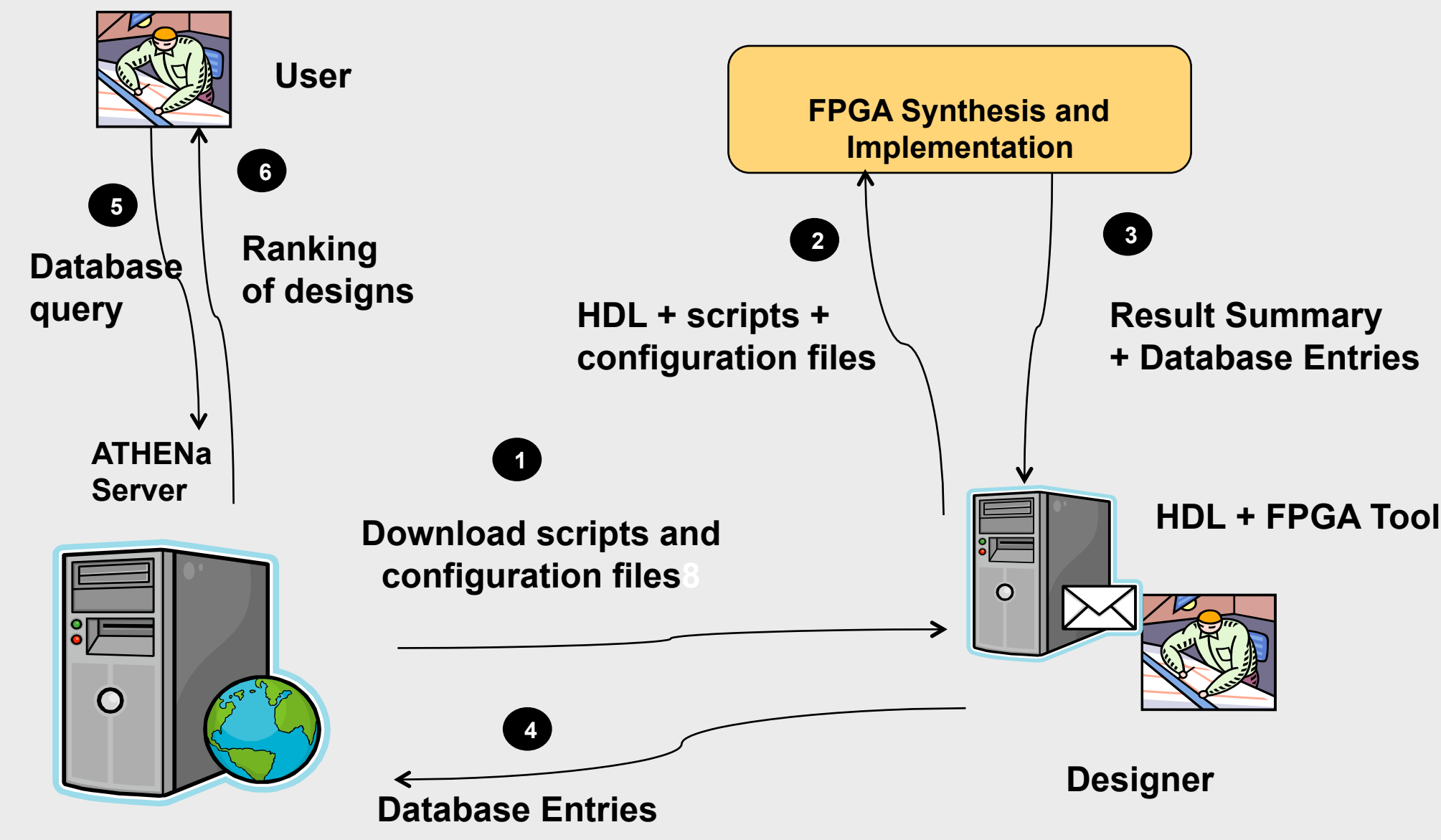
Set of scripts written in Perl aimed at an AUTOMATED generation of OPTIMIZED results for MULTIPLE hardware platforms, currently under development at George Mason University.

The first proof-of-concept version available at
http://cryptography.gmu.edu/athena

### ATHENa Allows Comparing

- ❖ **Algorithms**, e.g. candidates in the SHA-3 contest
- ❖ **Architectures and implementations,** e.g., basic iterative vs. unrolled, GMU implementation vs. Bochum implementation
- ❖ **Hardware platforms,** e.g. Xilinx Virtex 6 vs. Altera Stratix IV
- ❖ **Languages and tools,** e.g., VHDL vs. Verilog vs. AHDL, Synplify Pro vs. Xilinx XST

### 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

## Major Features

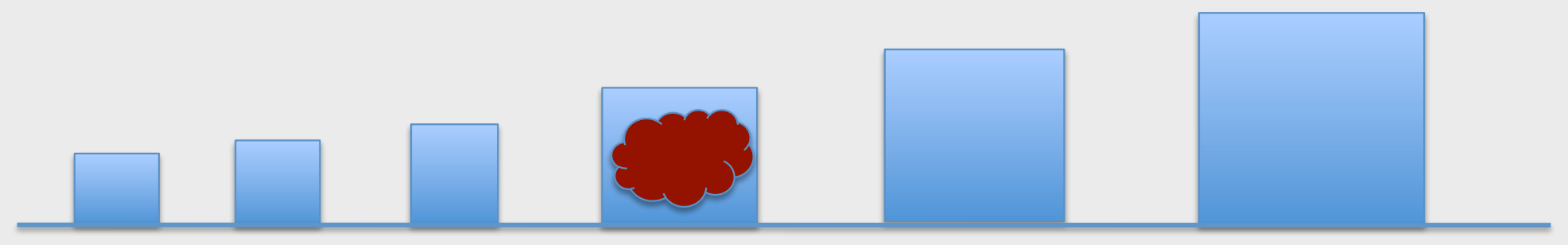
- ❖ synthesis, implementation, and timing analysis in the **batch mode**
- ❖ support for devices and tools of **multiple FPGA vendors**:

XILINX ALTERA Actel POWER MATTERS

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

VIRTEX VIRTEX-II PRO SPARTAN SPARTAN-II

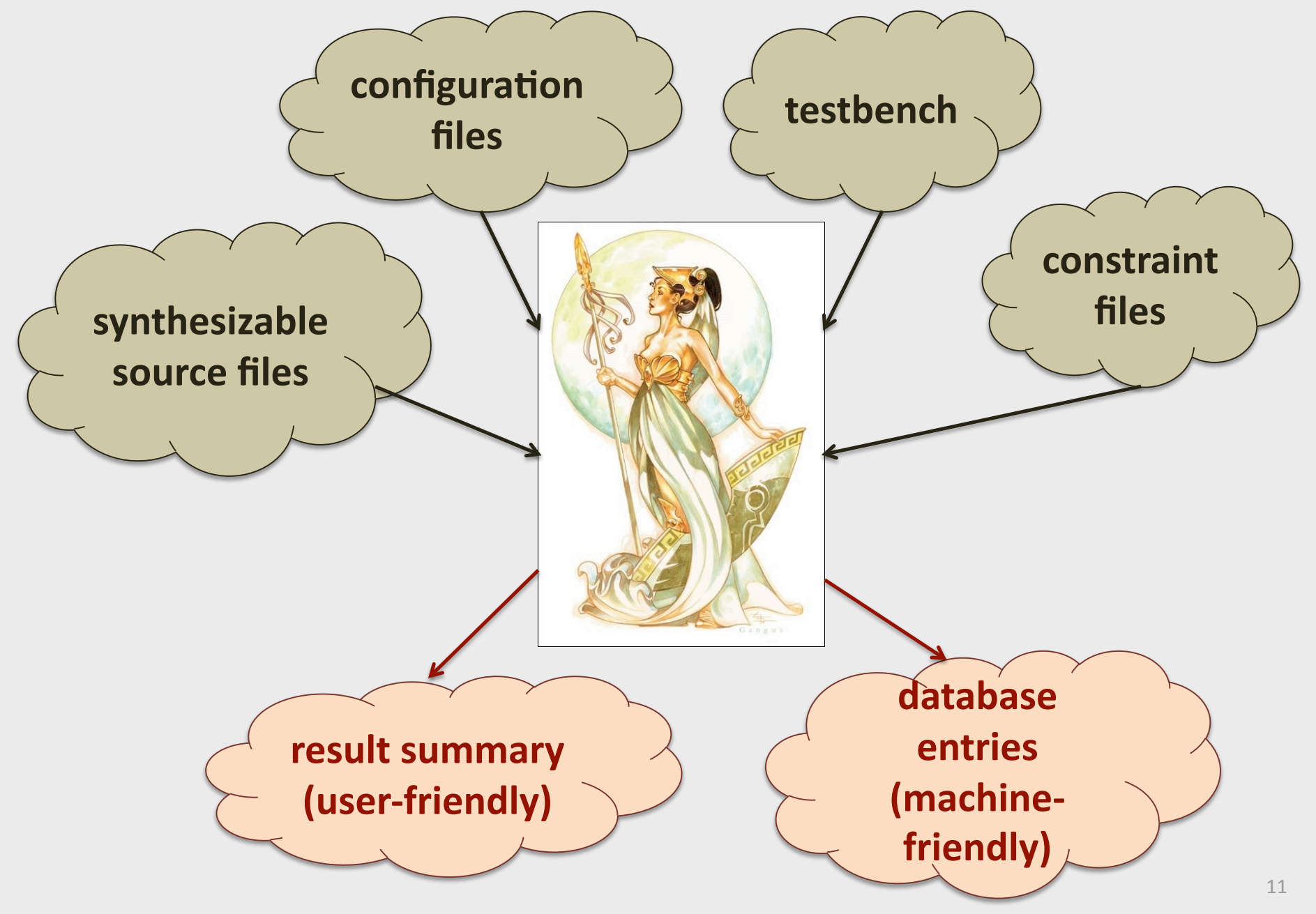
- ❖ automated choice of a **best-matching device** within a given family



### Under Development

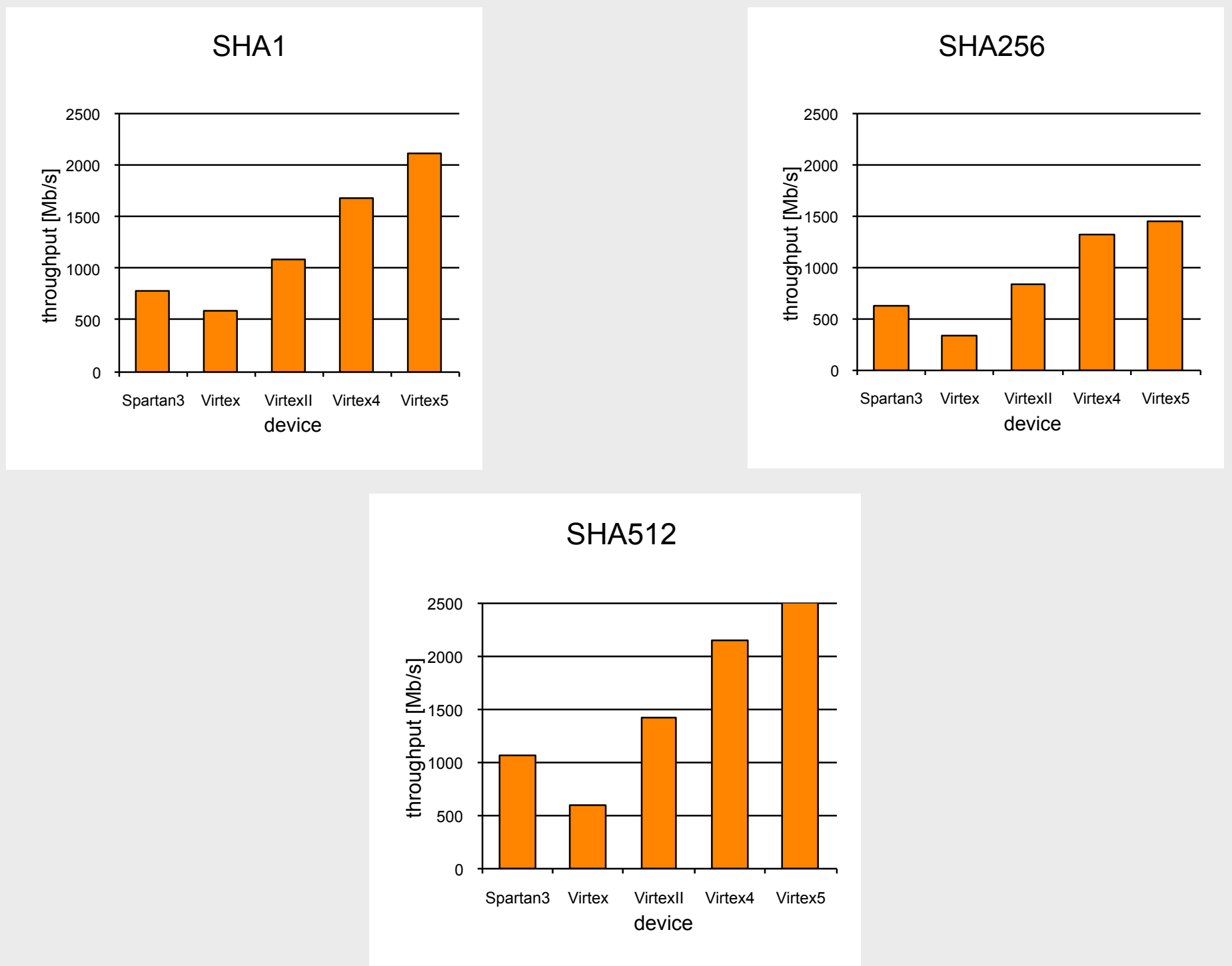
- ❖ **automated verification** of the design through simulation in the batch mode

- ❖ **exhaustive search** for optimum options of the tools
- ❖ **heuristic optimization algorithms** aimed at maximizing selected performance measures (e.g., speed, area, speed/area ratio, power, cost, etc.)

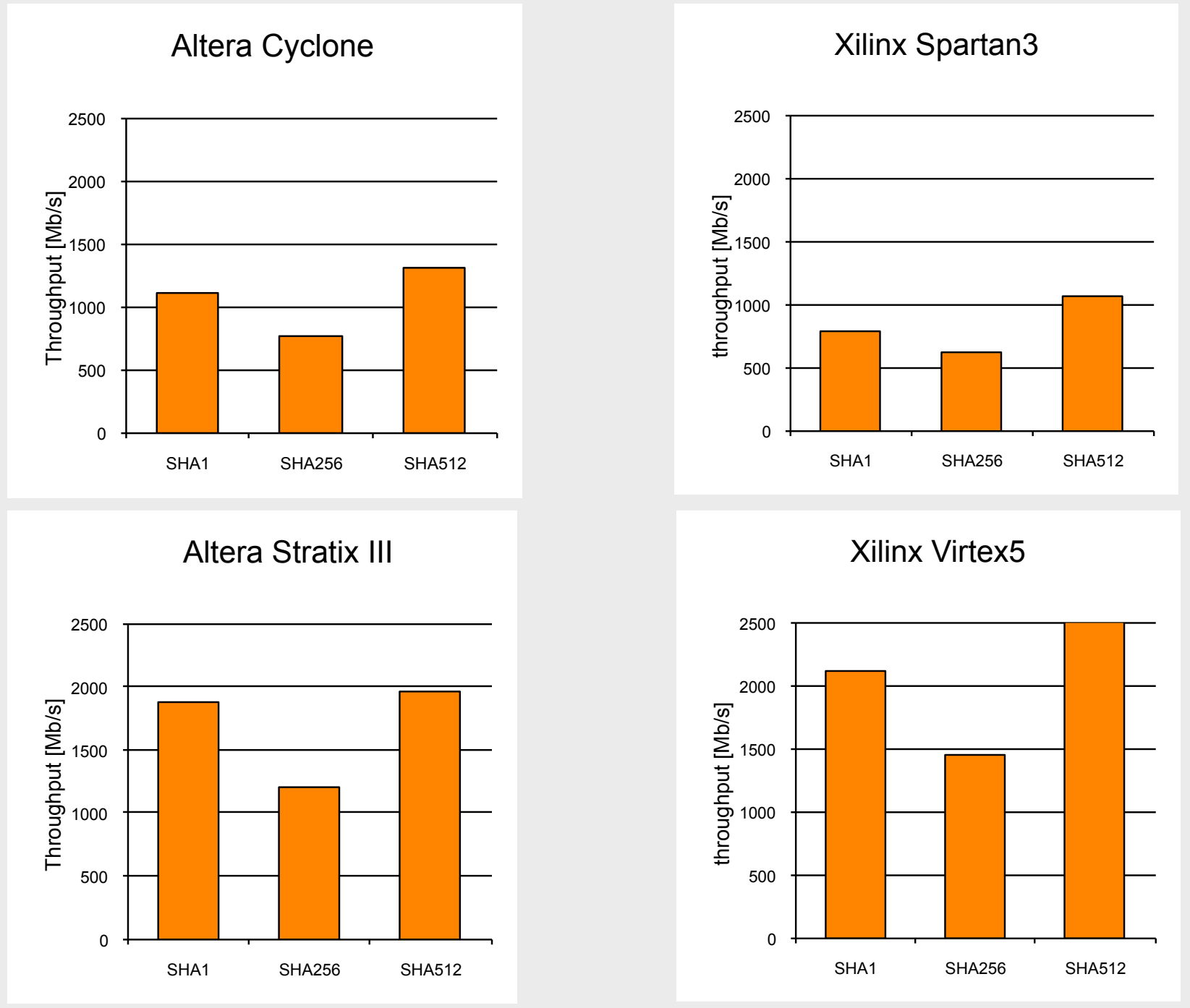

configuration files
testbench
synthesizable source files
constraint files
result summary (user-friendly)
database entries (machine-friendly)
11

## Results

### Results for Hash Functions SHA-1 and SHA-2 Xilinx FPGAs

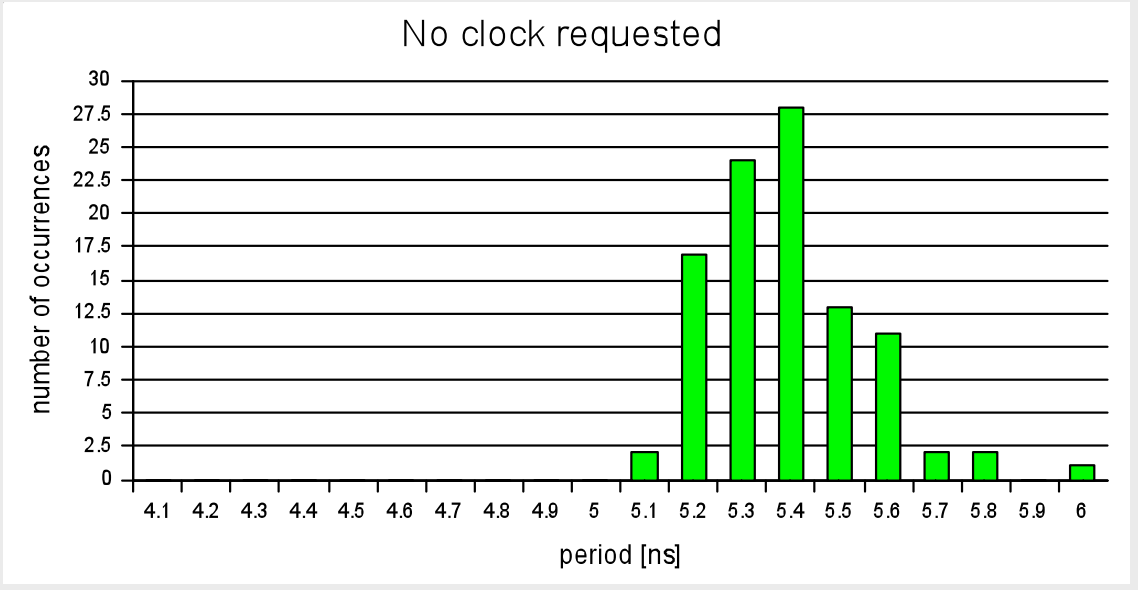


### Results for Hash Functions SHA-1 and SHA-2 Xilinx vs. Altera FPGAs

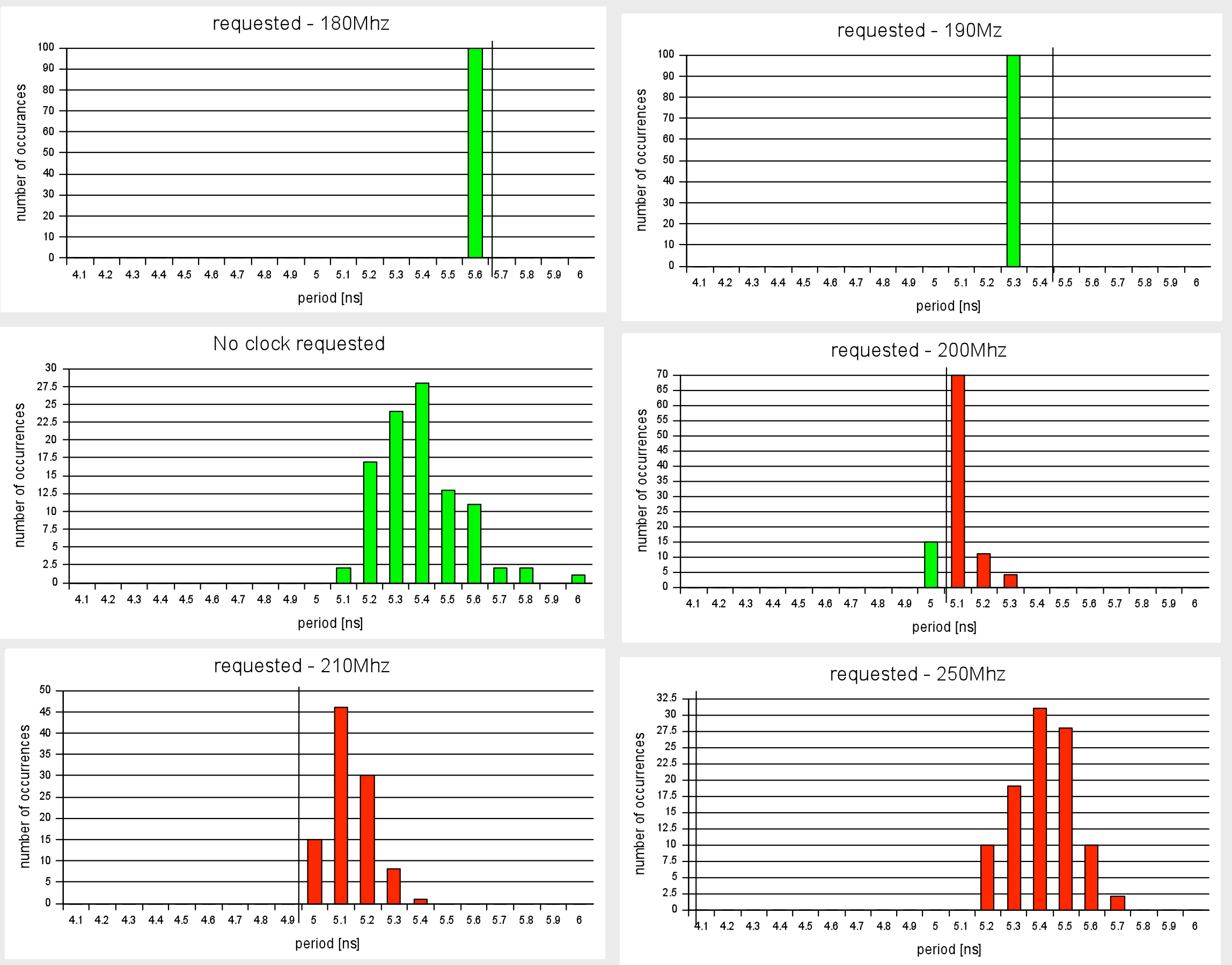


### Multi-Pass Place-and-Route Analysis

GMU SHA-512, Xilinx Virtex 5



### Dependence of Results on Requested Clock Frequency



Note : smaller is better

## Applications & Extensions

### Short-Term Application – SHA-3 Contest

- ✤ analysis of 14 hash functions qualified to the second round of the **SHA-3 contest**

**BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, Skein**

- ✤ GMU students **implementing, optimizing, and benchmarking all 14 candidates** in Fall 2009
- ✤ **Comparison vs.** existing optimized implementations of **SHA-1 and SHA-2 standards**
- ✤ **VHDL codes and results** of analysis **published at the ATHENa web site by December 31, 2009**

### Possible extensions

- ✤ standard-cell ASICs
- ✤ actual experimental measurements in hardware (power and energy consumption, latency, throughput)
- ✤ taking into account resistance to side-channel attacks
- ✤ other fields (e.g. DSP)

## Conclusions

- ✤ We propose a tool for a fair, comprehensive, reliable, and practical evaluation of cryptographic hardware
- ✤ Hope to discourage naive and/or dishonest comparisons, provide transparency, and overcome objective difficulties
- ✤ The proof-of-concept beta version 0.1 available at http://cryptography.gmu.edu/athena
  Subsequent versions made available as the tool matures.
- ✤ All scripts and configuration file templates will be made available in public domain (GPL) through the project web site.