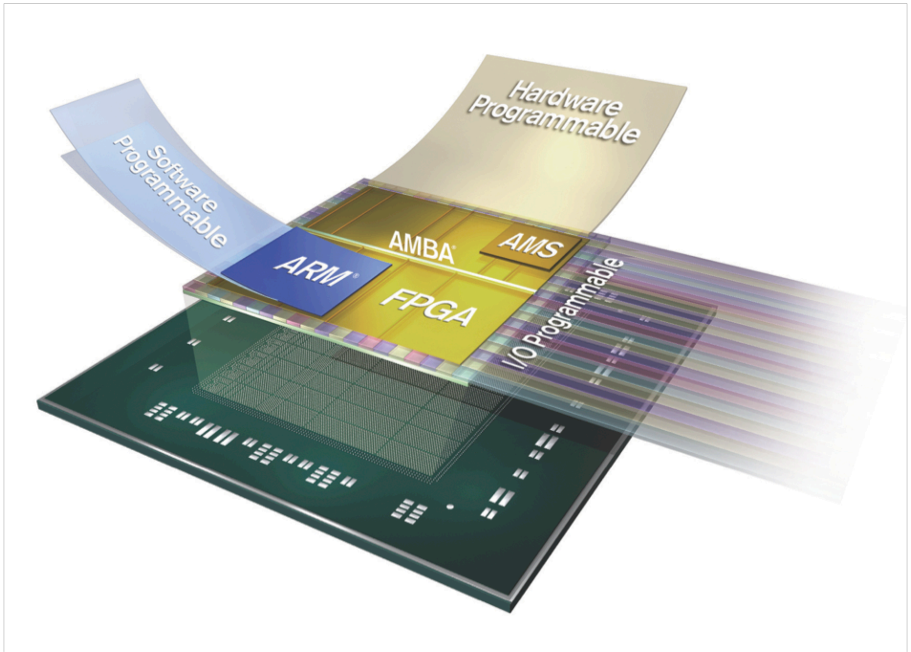
A Zynq-based Testbed for the Experimental Benchmarking of Algorithms Competing in Cryptographic Contests



<u>Farnoud Farahmand</u>,
Ekawat Homsirikamol,
and Kris Gaj
George Mason University
USA

Based on work partially supported by NSF under Grant No. 1314540

Introduction

- Recent cryptographic contests

  SHA-3 (2007-2012): hash functions
  CAESAR (2013-2018): authenticated ciphers

- Evaluation in hardware essential to determine a winner
- Primary hardware performance metrics
  - Maximum throughput (a function of maximum clock frequency)
  - Area (resource utilization)
- Maximum clock frequency can be determined using
  - Static timing analysis using FPGA tools
  - Experimental measurement using a prototyping board

Why Experimental Measurement?

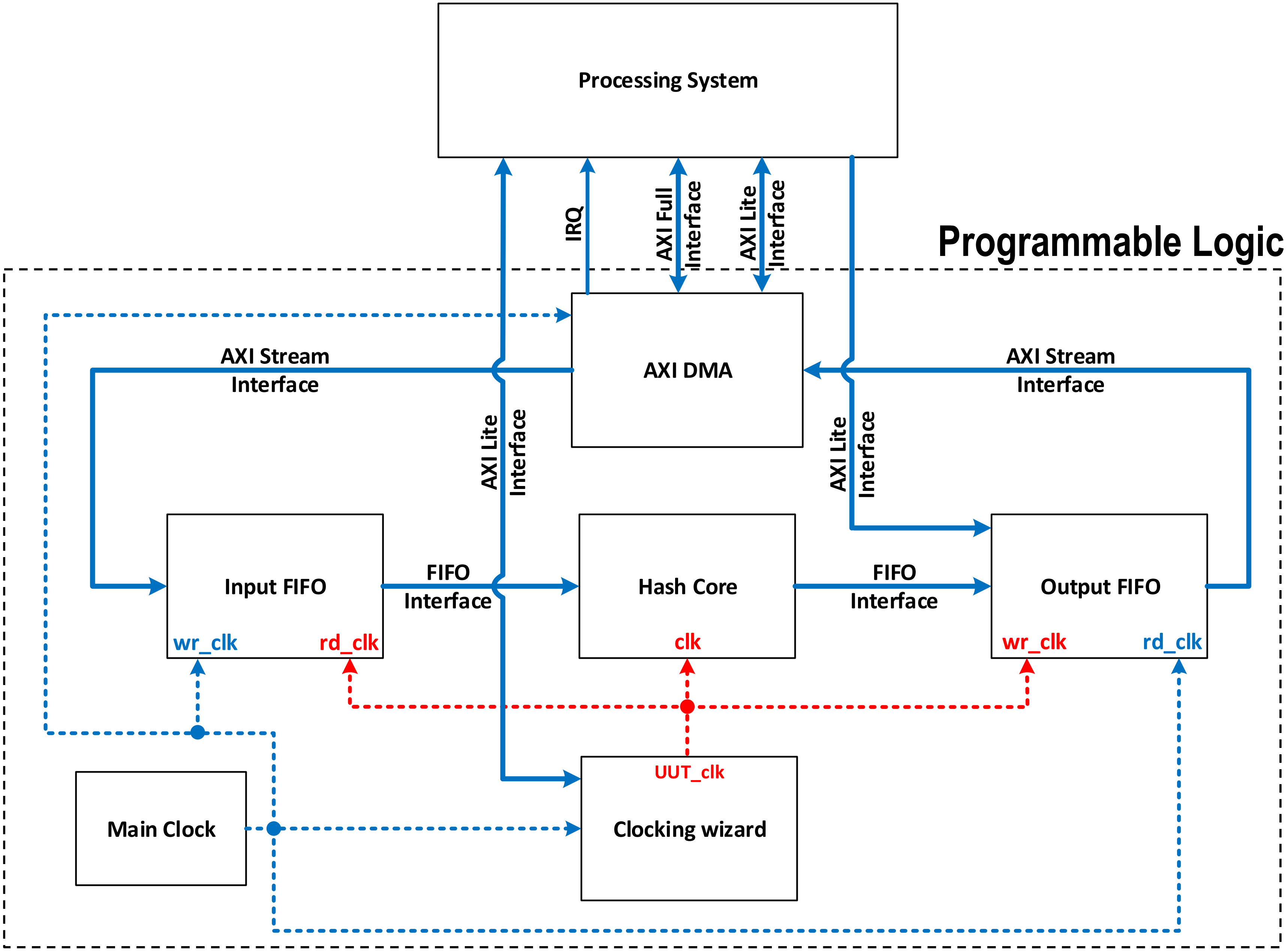
- Practical validation of the hardware API used by a hardware accelerator

- Measurements of throughput can take into account an overhead of the communication interface

- Verification of the worst-case values of the maximum clock frequency, reported by static timing analysis (possible new insights about the tools)

- Speed-up of the software/hardware codesign vs. purely software implementation

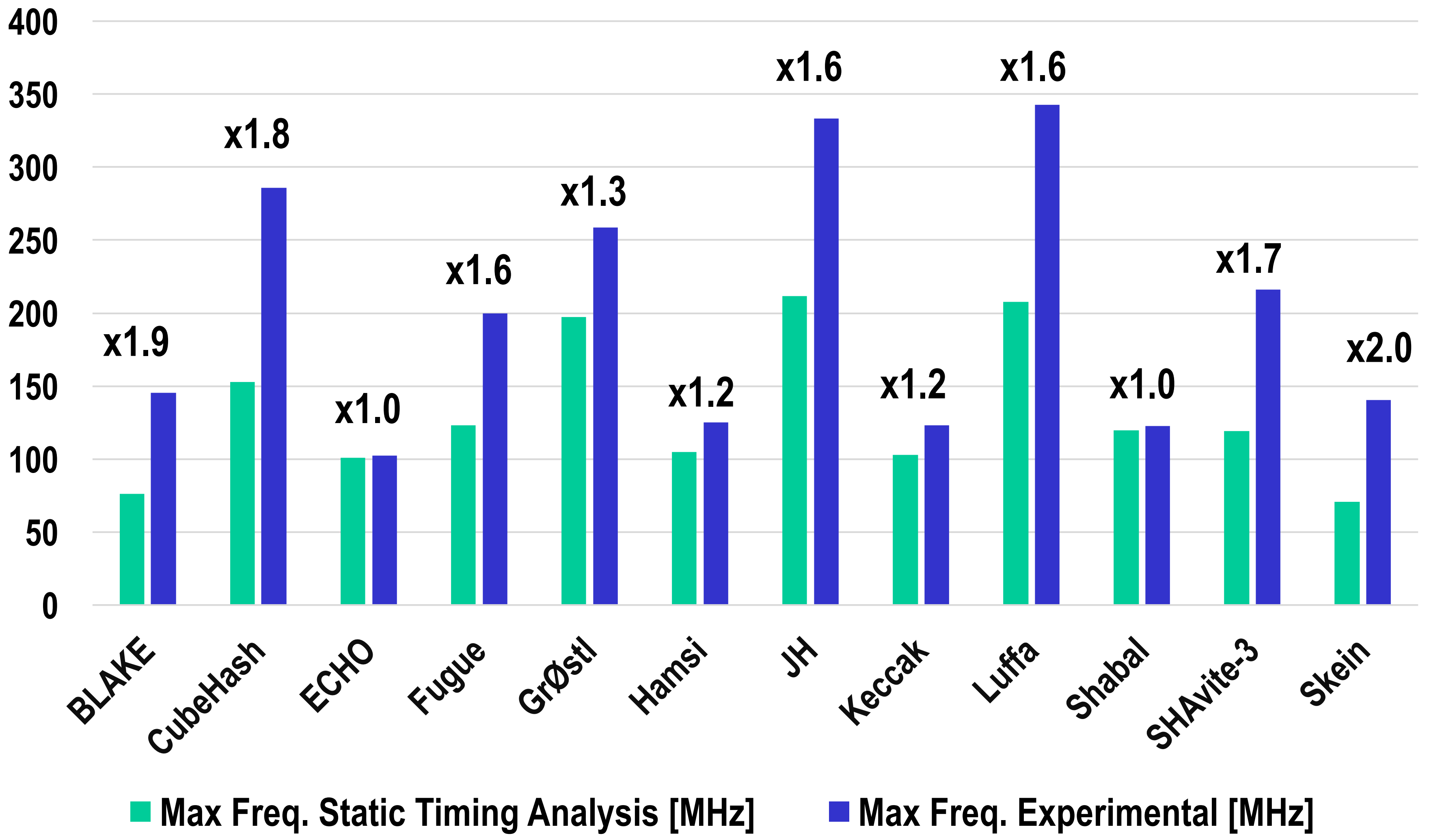
Experimental Testbed Based on Zynq



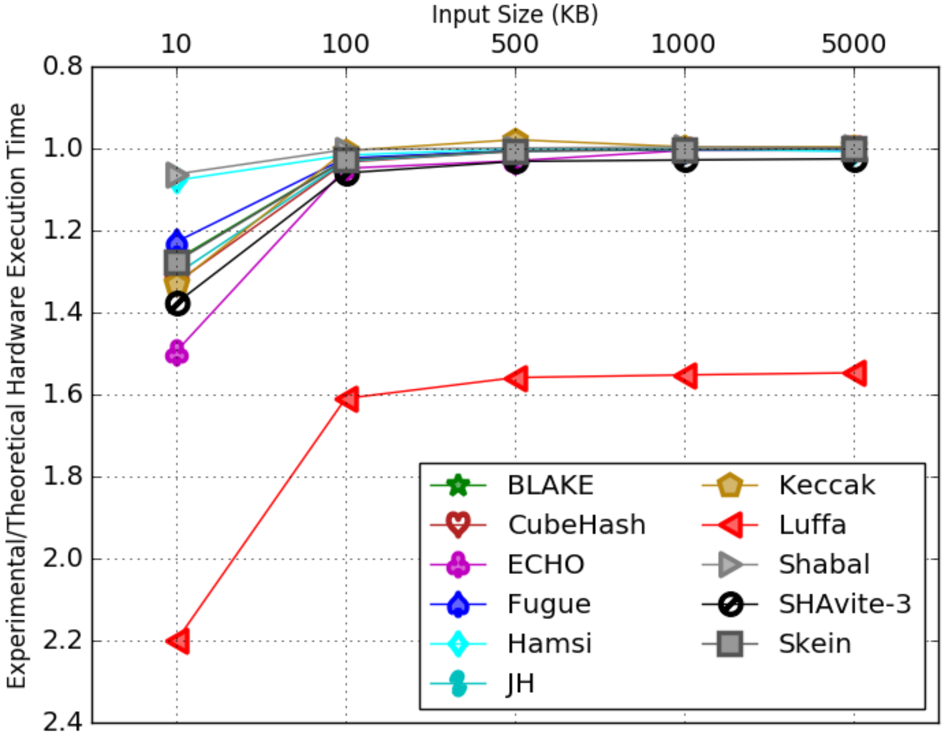
Our Test Case

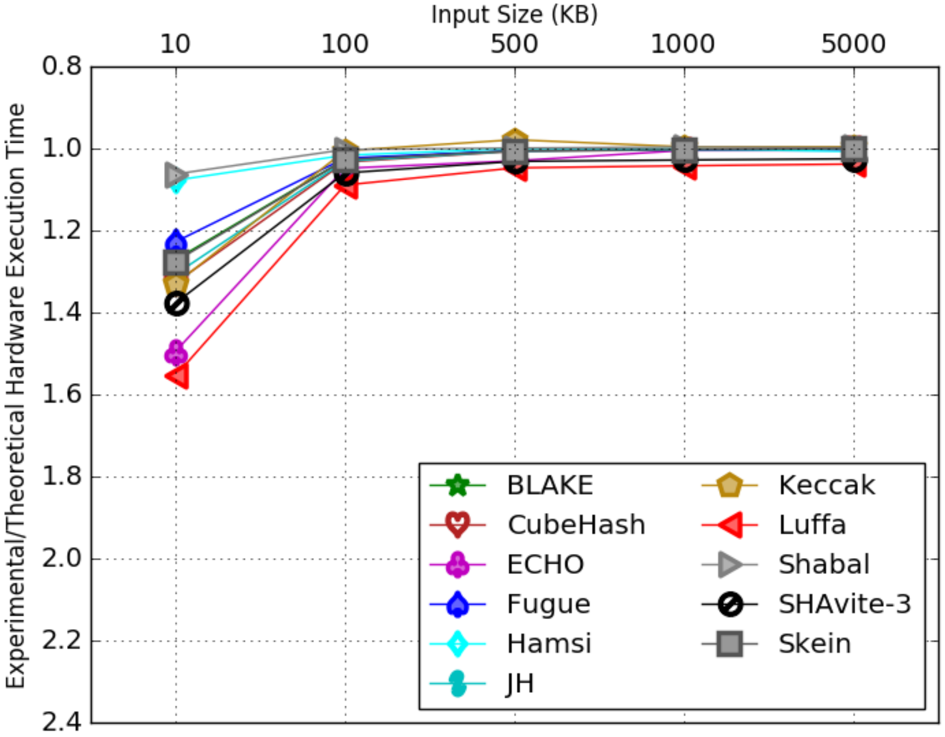
- 12 Round 2 SHA-3 candidates (all except BMW and SIMD)
- Basic iterative architecture
- GMU Hardware Interface for hash core
- Open-source RTL implementations developed in 2010-2012 (Ekawat Homsirikamol and Marcin Rogawski from GMU)
- Xilinx Vivado 2015.4
- Zynq 7020 on ZedBoard with 667 MHz clock

Results: Maximum Frequency



Results: Communication Overhead





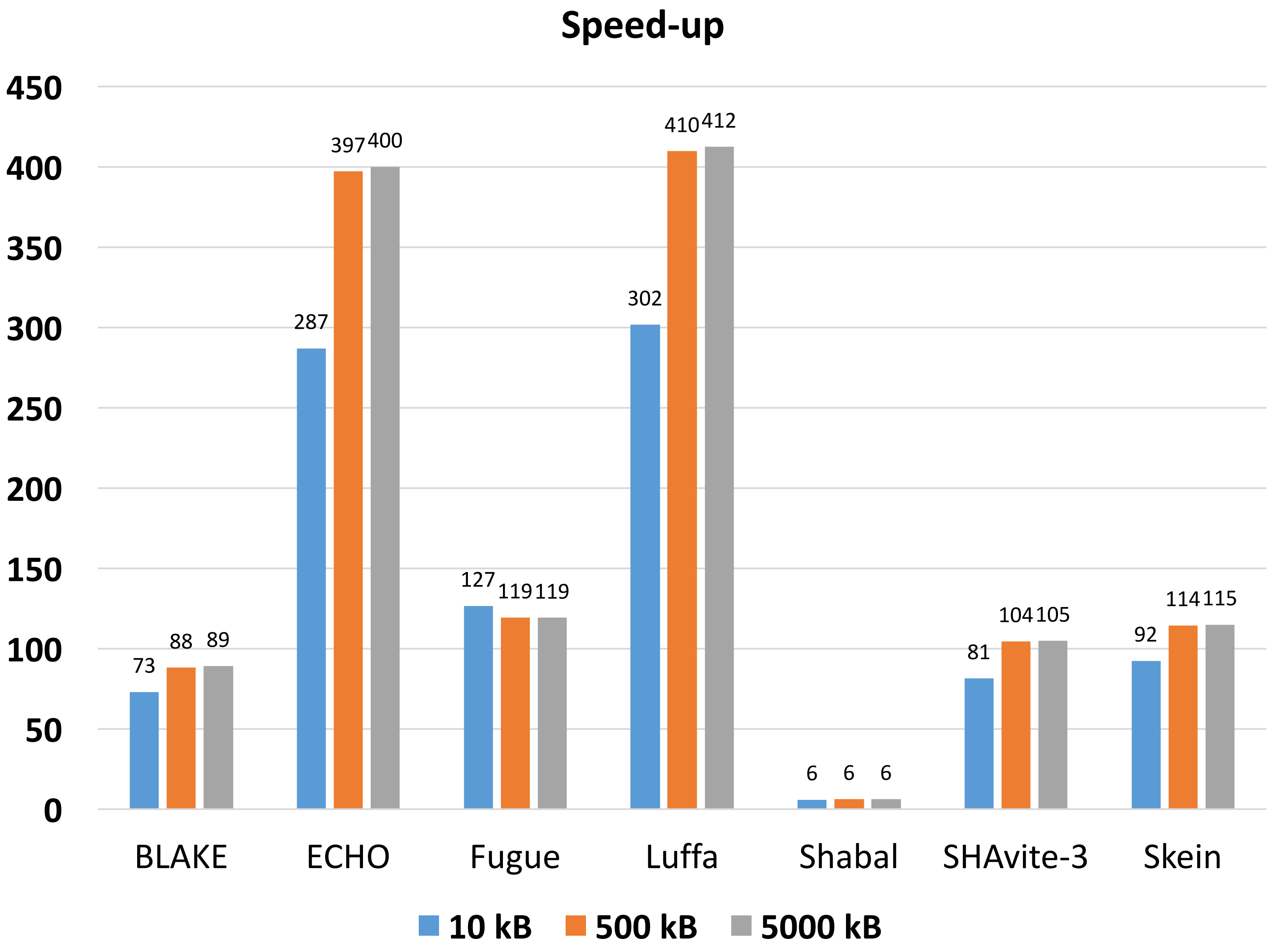
DMA core running at 100MHz for all algorithms

Max supported throughput:
64 * 100MHz = 6.4 Gbit/s

DMA core running at 150MHz for Luffa and 100MHz for all other algorithms

Max supported throughput:
64 * 150MHz = 9.6 Gbit/s

Results: Hardware/Software Speed up



Conclusions

- A novel experimental testbed, based on Xilinx Zynq, for evaluating hardware performance of cryptographic algorithms competing in cryptographic contests, such as SHA-3, CAESAR, etc.

- Case study based on 12 Round 2 SHA-3 candidates demonstrated that:
  - The maximum experimental clock frequency was always higher than the post-place and route frequency calculated by Vivado, using static timing analysis. The ratio a strong function of an algorithm.
  - Communication overhead below 5% for 100 kB messages and negligible for messages above 500 kB
  - Significant, but very algorithm dependent, speed up vs. software.