MS Thesis Defense

Department of Electrical and Computer Engineering

George Mason University

Tools and Experimental Setup for Efficient Hardware Benchmarking of Candidates in Cryptographic Contests

By

Farnoud Farahmand

Advisor: Dr. Kris Gaj

Date: November 21, 2016

Time: 11:00 A.M.

Location: ENGR 4801

Abstract

Hardware benchmarking of candidates competing in cryptographic contests, such as SHA-3 and CAESAR, is very important for ranking of their suitability for standardization. The observed increase in the number of algorithms qualified to the first round of the respective contests (51 in case of SHA-3 and 57 for CAESAR) inevitably brings the question of the sustainability of the current approach, based on manual coding, and its applicability to the development of future cryptographic standards. A huge amount of time is necessary to design the datapath and controller and convert them to the hardware description language (HDL) code. The other difficulty is to develop a testbench in HDL for verification purposes. High-Level Synthesis (HLS), based on the newly developed Xilinx Vivado HLS tool, offers a potential solution to the aforementioned problems. Therefore, in the first part of this thesis we investigate the following hypothesis: Ranking of candidate algorithms in cryptographic contests in terms of their performance in modern FPGAs & All-Programmable SoCs will remain the same independently whether the HDL implementations are developed manually or generated automatically using HLS tools.

In addition, one of the most essential performance metrics is the throughput, which highly depends on the algorithm, hardware implementation architecture, coding style, and options of tools. The maximum throughput is calculated based on the maximum clock frequency supported by each algorithm. A common way of determining the maximum clock frequency is static timing analysis provided by the CAD toolsets, such as Xilinx ISE, Xilinx Vivado, and Altera Quartus Prime. Finding actual maximum clock frequency utilizing static timing analysis is not a trivial task, especially in the Xilinx Vivado environment. It is extremely time consuming and tedious. As a result, in the second part of this thesis, we describe Minerva. Minerva is an automated hardware benchmarking tool which finds maximum frequency based on static timing analysis. It can be configured to target either Throughput or Throughput/Area as optimization criteria and to search through specific number of optimization strategies. The tool determines the best requested clock frequency, leading to the maximum value of the optimization target.

In the third part of the thesis, we have developed a universal testbed, which is capable of measuring the maximum clock frequency experimentally, using a prototyping board. We are targeting cryptographic hardware cores, such as implementations of SHA-3 candidates. Our testbed is designed using a Zynq platform and takes advantage of software/hardware co-design and Advanced eXtensible Interface (AXI).