Master's Thesis Defense

Department of Electrical and Computer Engineering

George Mason University

ANALYSIS AND INNER-ROUND PIPELINED IMPLEMENTATION OF SELECTED PARALLELIZABLE CAESAR COMPETITION CANDIDATES

By

Sanjay Deshpande

Director: Dr. Kris Gaj

Committee members: Dr. Jens-Peter Kaps and Dr. Xiang Chen

Tuesday, November 22, 2016, 1:30PM-3:00PM

ENGR 3507

Abstract:

In this thesis, we have first characterized candidates of the Competition for Authenticated Encryption, Security, Applicability, and Robustness (CAESAR). Then, we have chosen five candidates from the Round 2 and Round 3 submissions, namely SCREAM, AES-COPA, Minalpher, OCB, and AES-OTR. We first obtained the initial estimates of the Maximum Clock Frequency, Throughput, Area, and Critical path from the Basic Iterative High Speed Architecture. Then, we implemented the inner-round pipelining for all the selected algorithms to improve the Frequency and Throughput by reducing Critical path and processing multiple blocks of data simultaneously. We targeted the largest available FPGA in the student version of Xilinx ISE, i.e., Xilinx Virtex 6 XC6VLX75T-3FF784. Our results have demonstrated the improvement in the Clock Frequency by a factor varying from 28.5% for OCB to 85% for SCREAM, and the improvement in the Throughput to Area ratio (with Area expressed using LUTs) by a factor varying from 43.5% for Minalpher to 148.4% for SCREAM.