Notice and Invitation

Oral Defense of Doctoral Dissertation

The Volgenau School of Engineering, George Mason University

Panasayya Yalla

Bachelor of Engineering, Andhra University, 2006

Master of Science, George Mason University, 2009

Methodology for Developing Lightweight Architectures for FPGAs

Friday, December 1st, 2017, 1:30PM–3:00PM

ENGR 4801

Committee

Dr. Jens-Peter Kaps, Chair

Dr. Kris Gaj

Dr. Brian L. Mark

Dr. Robert Simon

Abstract

Until now, application specific integrated circuits (ASICs) are the main platform for lightweight cryptography because of their low power consumption and good performance. However, their complex design cycle and very high non-recurring engineering cost limit them to high volume applications. In recent years, low cost and power Field Programmable Gate Arrays (FPGAs) (Xilinx: Spartan-6 and Artix-7; Altera: Cyclone-IV and -V; Actel: IGLOO and ProASIC3) have started emerging, reducing the power consumption gap between ASICs and FPGAs. FPGAs are the ideal platform for fast changing environments and lower volume applications. In spite of these advantages, very little attention has been paid to FPGAs as a target for lightweight cryptography.

Implementing algorithms for lightweight applications is a complex and time consuming task due to interdependencies of the constraints on size, power, energy, and cost. The various design choices such as interface, width of datapath, serialization, pipelining, choice of processing elements etc. determine whether the design meets these constraints. In most cases this results in designs where the datapath width is reduced. However, this is not sufficient, one has to one has to carefully evaluate the trade-off various constraints at every step of the design process. The control unit is an additional hurdle. Extensive component re-use in the datapath can lead to a very complex control logic which might negate the area savings in the datapath.

In this research, we tackle these problems in three parts. First part involves developing a generalized methodology for making early design choices and various optimizations that can be applied to datapath. The control logic optimization techniques using memories are proposed in the second part. Finally, a tool is developed which optimizes the control logic by using the existing controller or state matrix as the input and transforms it into an optimized controller. This optimized controller is a combination of traditional FSM realized using Flip-flops and combinational logic with fewer states and memories.

Using the proposed methodology, we developed lightweight architectures for block cipher Advanced Encryption Standard (AES) for three different widths, Secure Hash Algorithm-256 (SHA-256), multipurpose AES and Keccak cores, Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) candidates Ketje-Sr, Ascon-128, and Ascon-128a. The effectiveness of the optimization tool is tested using AES128 and Keccak core. We also developed hardware package which supports CAESAR hardware Application Programming Interface (API) for lightweight implementations and evaluated its benefits using Ketje-Sr and Ascon.