

# AES Implementations Optimized for Mid-Range FPGAs

ECE Scholarly Paper Presentation

Bryan M. Sobczyk

Advisor: Dr. Jans-Peter Kaps

Wednesday, December 9, 2009

4 PM

The Engineering Building, Rm. 3202

## Abstract

The Rijndael Algorithm was chosen for the Advanced Encryption Standard (AES) in 2001 and formally published in FIPS Publication 197. Since Rijndael was released as a candidate a number of cores were created to test and benchmark the algorithm in both hardware and software. Rijndael was chosen partly based on its ability to be efficiently implemented in Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). A survey of openly licensed AES cores were found to not fully take advantage of ROM blocks to simplify and shorten critical paths in the algorithm's rounds. In ASIC design, heavy use of combinational logic is advantageous while in FPGA designs each logic cell has local memory available and all free logic cells are equally valuable for design use. This paper will present a T-box design that will utilize FPGA memory to create a core compatible with a standard 32-bit bus width that will sustain a throughput of 20 Mbyte/sec.