

**ECE Department
MS CpE Scholarly Paper Presentation**

**Friday, July 25th, 2008
1:00 PM
STII Room 230A**

**Implementation and Comparative Analysis of AES as
a STREAM Cipher**

**By
Bin ZHOU**

Advisor: Dr. Kris Gaj

Abstract

Advanced Encryption Standard (AES) is the current encryption standard adopted by U.S. government, which plays an important role in today's cryptographic systems. AES is usually considered a block cipher; however, by using different operating modes, it can be easily turned into a stream cipher. Nevertheless, how well AES could perform as a stream cipher in a resource restricted environment compared to other modern stream ciphers has remained unclear. In this paper, the motivation for implementing AES as a stream is introduced. On-the-fly key scheduling schemes are used and various compact architectures are studied. Pure logic based and ROM based S-Boxes are implemented for the purpose of comparison in terms of speed and area. Pipelined architecture is also studied in order to achieve a better throughput. Different memory schemes are considered, including 2-bank distributed RAM, 2-bank block RAM, shift-register in LUTs, 1-bank registers and dual-port memory. 8-bit, 32-bit, 64-bit datapath versions are implemented in order to find the architecture with the best throughput/area ratio. The whole design is targeted to Xilinx Spartan 3 FPGAs, and developed with synthesizable VHDL code. The performance results are compared with eSTREAM cipher candidates and also with other implementations of AES, showing that our implementation has a potential to meet the modern stream cipher requirements.