

Comparative Analysis of T-box vs. S-box hardware architectures of Advanced Encryption Standard (AES)

MS CpE Scholarly Paper

By

Nitin Alabur

Advisor: Dr. Kris Gaj

Thursday, July 31 2008

Time 11:30 am

Science and Technology II, Room 230A

Abstract

AES is a cipher that has been analyzed extensively and standardized by NIST. The algorithm has been implemented with an S-box architecture which has smaller memory requirement but lower throughput due to four separate operations of shift rows, sub bytes, mix columns and add round key. The cipher has also been implemented with a T-box architecture, where the shift rows, sub bytes and the mix columns operations are performed by a single table look up. The implementation with T-box architecture has a higher throughput since there are only two operations (a look up and add round key) to be performed for every iteration and more area due to the large memory required to store the larger look up tables.

This paper will discuss the hardware implementation of AES with T-box architecture, with a key scheduling scheme that stores the precomputed round keys in the memory. It compares the T-box implementation results with the S-box and with the results obtained by Viktor Fischer and Milos Drutarovsky for the key sizes 128, 192 and 256 bits. The implementations are targeted on Xilinx Spartan3 and Virtex5 FPGAs.