Department of Electrical Engineering & Computer Science
Master Degree Course Electronics Engineering, MSc EE

HOCHSCHULE BREMEN
UNIVERSITY OF APPLIED SCIENCES

Master 2007

Marco Antonio Zapata Millán

Optimized H/W Realization of the Advanced Encryption Standard (AES)

ABSTRACT - Masterthesis

In this Master Thesis two hardware realizations of the Advanced Encryption Standard (AES) are done. The first of them is done by using a Basic Architecture scheme. The main point of this realization is the application of composite fields operation in one of the transformations (SubBytes), it avoids the use of big blocks of memory. This realization uses 1,698 slices of a Virtex 4 chip and has a Throughput of 785 Mbps.

The second realization is optimized by applying an Inner-Round Pipelining Architecture with three stages, it allows to encrypt three 128-bits blocks of data at the same time. The key expansion module is pipelined in three stages as well. This realization uses 1,998 slices of the Virtex 4 chip and reaches a Throughput of 2.5 Gbps.

All the simulations are presented in this work and the code is added in a CD, the organization of the CD is explained in Appendix B.