IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 4, November 2012)

Area optimized S-BOX Architecture for Advance Encryption Standards

Nimmi Gupta Tarun Verma

nimmi.gupta877@gmail.com *tarunindia@rediff.com*

***Abstract*— This paper presents an area optimized for composite field arithmetic based SubBytes transformation (Sbox) used in Advanced Encryption Standard (AES) encryption. The proposed architecture is based on pre-computation technique. Implementation is proposed on FPGA using Xilinx ISE on XC3S 400-5 and results are shown in the paper.**

***Keywords*—AES, S-BOX, Sub-Byte, Encryption.**