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 6, January 2013)

Performance Analysis of S-Box using GF Arithmetic for AES

Akanksha Shukla
akanksha_engg2005@yahoo.co.in

Satyendra Sharma
satyendracommn@gmail.com

Abstract — **Sub-Byte transform or Substitution Box, better known as S-BOX is the most important part of Advance Encryption Standard (AES) algorithm. Many S-BOX architectures have been proposed in past based on Area consumption, Power Consumption, Speed etc. In this paper we present an optimized S-BOX architecture based on the Galois Field (GF) Operations. Proposed architecture is implemented in VHDL Using Xilinx ISE 9.2i on device XQ6VLX130T of Spartan family.**

Keywords — **S-Box, AES, Galois Field, VHDL, Spartan.**