Abstract

FPGA implementation of Advanced Encryption Algorithm for 128 bits is presented in this paper for high speed applications. It explores pipelining and sub-pipelining to gain speed optimization without increasing area considerably. It concentrates on placement of the pipelining registers rather than just increasing its number to gain speed. An encryptor with 8 stages of sub-pipelining for each round unit using the proposed architecture gives a throughput of 24.33 Gbps on Xilinx XCV1000 e-8 bg560 device and that of 29.99 Gbps on XC3S4000-5fg676 device.

Refer
High Speed Architecture Implementation of AES using FPGA

References

- K. Gaj and P. Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware"); Presented at Proc. 3rd AES Conf. (AES3).

- Edwin NC Mui, "Practical Implementation of Rijndael S-Box Using Combinational Logic");

Index Terms

Computer Science    Information Sciences

Keywords

Rijndael  Aes  Pipelining  Sub-pipelining  S-box.