International J. of Multidispl.Research & Advcs. in Engg.(IJMRAE),
ISSN 0975-7074, Vol. 5, No. III (July 2013), pp. 103-112

A SECURE IMPLEMENTATION OF NONLINEAR AES S-BOX AND MIX-COLUMN TRANSFORMATION WITH THE ENHANCEMENT OF BIOMETRICS

V. GOPI[1] AND E. LOGASHANMUGAM[2]
[1] Research Scholar, St. Peter's University, Chennai, india
[2] Professor and Head, Dept of ECE, Sathyabama University, Chennai, India

Abstract

Cryptography plays an important role in the security of data. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. The need for privacy has become a major priority and important for communication in all fields. Widespread use of personal communications devices has only increased demand for a level of security on previously insecure communications The urgency for secure exchange of digital data resulted in large quantities of different encryption algorithms which can be classified into two groups: asymmetric encryption algorithms (with public key algorithms) and symmetric encryption algorithms (with private key algorithms) [1]. In this paper, we use FPGA chips to realize high data throughput AES hardware architecture is proposed by partitioning the ten rounds into sub-blocks of repeated AES modules. In this paper we have detailed the alternative design of both direct, inverse MixColumn transforms and high secure nonlinear S-box required in the AES hardware implementation.

Keywords : Encryption, Security processor, Architecture, FPGA, Cryptography, AES, cipher.