Abstract

This document gives the hardware implementation of Mix Column step in AES encryption process. The AES encryption process consists of several transformation steps such as byte substitution, shift rows, mix column and addition of round key operation step. There are two aspects to perform mix column step in AES is presented. The total operation is coded with VERILOG, synthesized and simulated using Xilinx ISE 10.1.
Hardware Implementation of Mix Column Step in AES

Index Terms

Computer Science  Communication and Networks

Keywords

AES  VLSI  Data Security  Cryptography