Abstract

In this paper, a new architecture for Advanced Encryption Standard (AES) Algorithm based on Application Specific Instruction set Processors (ASIP) design technique is proposed. The basic configuration is developed in order to reduce the execution clock pulses for the main specific instructions. According to the improvement of the first register configuration, two ASIPs are designed for AES algorithm. The second ASIP is 89% faster and have 22% less gates than the first proposed design.

References


Index Terms

Computer Science
Algorithms

Keywords  
ASIP AES algorithm RTL crypto Processor