(#19) A Novel Implementation Strategy for AES Algorithm on FPGA

B.M.S.B Basnayake[1], Prabhath Buddhika[2]

[1,2]Faculty of Engineering, NSBM Green University, Sri Lanka

Abstract

Traditional methods of keeping data secure, while effective, face certain challenges. Information must be processed quickly and in real-time. This becomes a big problem during the use of the Advanced Encryption Standard (AES) algorithm. It is widely used in the modern world. encryption protocol due to the increasing complexity and volume of AES, Data acceleration requires new methods for designing and implementing encryption systems. High-performance encryption makes it difficult to integrate FPGA-based systems Programs that must work in real time. With specific optimization of FPGA architecture. The goal of AES work is to find the right balance between the use of computing resources. It also meets the need for energy-efficient and fast data processing.

Keywords: *AES Algorithm, FPGA, Encrypting, pipeline, optimizing*