Abstract

Mohamed B Abdelhalem Osman

A Design for an FPGA Implementation of Rijndael Cipher

Our aim is to simulate the Rijndael cipher using Field Programmable Gate Array (FPGA) to achieve low cost, ease of implementation, availability “FPGAs can be bought off the shelf“, high flexibility including capability of frequent modifications of hardware, and low cost of the final product. We propose a modified implementation of Rijndael, the Advanced Encryption Standard (AES) based on the fact that any FPGA includes built in memory block where we store all the results of the fixed operations. The modification gives an 11% reduction in area and 25% increase in speed (throughput) compared with the original design. Our design gives the highest throughput and area utilization over all the Iterative Looping (IL) based FPGA implementations. In the original design, the decryption algorithm was not implemented. Our implementation of the decryption algorithm gives better results than the other IL based FPGA implementations.