Abstract

Lightweight cryptography is an interesting phenomenon that provides the perfect trade-off among security, higher throughput, low-power consumption, and compactness. Designing lightweight cryptography is a challenging issue. In this paper, Mixcolumn operation in the Advanced Encryption Standard (AES) is modified based on cellular automata functions. AES lacks compactness, but have good accessibility than the other algorithms. Security analysis like bent functions, Fast Walsh Transform method is followed to verify the security in modified AES algorithm. Hardware implementation of modified AES offers efficient memory space and area consumption. Comparative study of traditional mixcolumn architecture and Cellular automata based mixcolumn architecture are made through the hardware simulation in Xilinx, to show FPGA implementation of AES results as lightweight cipher, in terms of memory requirement.

2. Deng Tang et al, “Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties”, in Journal of design, codes and cryptography, china, April 2013, pp. 77-91.


Index Terms

Computer Science System Architecture

Keywords

Lightweight cryptography, Mixcolumn, AES, cellular automata, security, area consumption, FPGA.