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.

References

1. Othman 0. Khalifa et al, “Communications cryptography”, presented at the RF and
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.
3. N. Ahmad and S.M. Rezaul Hasan, “Efficient integrated AES crypto-processor
architecture for 8-bit stream cipher”, in Electronics letters 2012, ©The Institution of Engineering
4. LI Zhen-rong et al, “Low-power and area-optimized VLSI implementation of AES
coprocessor for Zigbee system”, in The Journal of China Universities of Posts and
Telecommunications, Xi’an, China, 2009, pp.89-94.
5. Qiang Liu et al, “High throughput and secure advanced encryption standard on field
programmable gate array with fine pipelining and enhanced key expansion”, in IET Computers
& Digital Techniques, Tianjin, china, October 2014, pp.175-184.
6. Hua Li and Zac Friggstad, “An Efficient Architecture for the AES Mixcolumns Operation”,
8. Hua Li and Chang N. Zhang, "Efficient Cellular Automata Based Versatile Multiplier for
Thesis, department of electrical engineering, Naval Postgraduate School, Monterey, California,
December 2010.
10. Claude Carlet,"Boolean Functions for Cryptography and Error Correcting Codes",
Cambridge University Press, Eds Yves Crama and Peter Hammer, October 2010, ch 2,
pp.17-20.

Index Terms
Computer Science
System Architecture

Keywords

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