Abstract

FPGA implementation of Advanced Encryption Algorithm for 128 bits is presented in this paper for high speed applications. It explores pipelining and sub-pipelining to gain speed optimization without increasing area considerably. It concentrates on placement of the pipelining registers rather than just increasing its number to gain speed. An encryptor with 8 stages of sub-pipelining for each round unit using the proposed architecture gives a throughput of 24.33 Gbps on Xilinx XCV1000 e-8 bg560 device and that of 29.99 Gbps on XC3S4000-5fg676 device.

Refer
ences

- FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001
- K. Gaj and P. Chodowiec, "Comparison of the hardware performance of the AES
  candidates using reconfigurable hardware", Presented at Proc. 3rd AES Conf. (AES3).
- J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA implementation and
  performance evaluation of the AES block cipher candidate algorithm finalist",
  presented at Proc. 3rd AES Conf. (AES3).
- H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/sec VLSI
  implementation of the AES Rijndael algorithm", in Proc. CHES 2001, Paris, France,
- M. McLoone and J. V. McCanny, "Rijndael FPGA implementation utilizing look-up
- V. Fischer and M. Drutarovsky, "Two methods of Rijndael implementation in
- Akashi Satoh, Sumio Morioka, Kohji Takano and Seiji Munetoh, "A Compact
  Rijndael Hardware Architecture with S-Box Optimization.", Springer-Verlag Berlin
  Heidelberg, 2001
  implementation of Rijndael encryption with composite field arithmetic",
- Xinmiao Zhang and Keshab K. Parhi, "High-Speed VLSI Architectures for the AES
  Algorithm", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 12,
  No. 9, September 2004.
  memoryless 17.8 Gbps AES-128 encryptor", in Proc. Int. Symp. Field-Programmable
- G. P. Saggese, A. Mazzeo, N. Mazocca, and A. G. M. Strollo, "An FPGA
  based performance analysis of the unrolling, tiling and pipelining of the AES algorithm",
- F. Standaert, G. Rouvroy, J. Quisquater, and J. Legat, "Efficient implementation
  of Rijndael encryption in reconfigurable hardware: Improvements & design tradeoffs",
- Naga M. Kosaraju, Murali Varanasi and Saraju P. Mohanty, "A High-Performance
  VLSI Architecture for Advanced Encryption Standard (AES) Algorithm",
  IEEE Proceedings of the 19th International Conference on VLSI Design (VLSID’06).
- Amruta Page, P. V. Srinivas Shastry, "AES-128 Key Expansion with LUT and
  OTF S-Box", International Journal of Computer Technology and Electronics Engineering
- Edwin NC Mui, "Practical Implementation of Rijndael S-Box Using Combinational
  Logic.",
- Marian Cretu1 and Cristian-Gabriel Apostol, "A Modified Version of Rijndael
  Algorithm Implemented to Analyze the Cyphertexts Correlation for Switched
  S-Boxes", IEEE conference on Communication (COMM), Bucharest, 2012

Index Terms

Computer Science
Information Sciences

Keywords

Rijndael  Aes  Pipelining  Sub-pipelining  S-box.