Computers & Electrical Engineering

Volume 37, Issue 6, November 2011, Pages 1160-1170

Design of an ultra high speed AES processor for next generation IT security â˜†

Liakot Ali [a] ... Niranjan Roy [a]

Show more

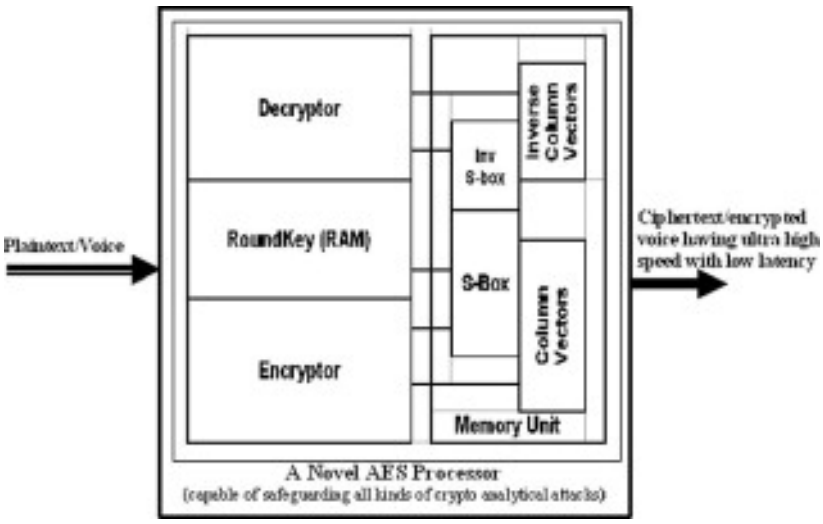
https://doi.org/10.1016/j.compeleceng.2011.06.003

Abstract

The Advanced Encryption Standard (AES) has added new dimension to cryptography with its potentials of safeguarding the IT systems. This paper presents the design of an ultra high speed AES processor to generate cryptographically secured information at a rate of multi-ten Gbps. The proposed design addresses the next generation IT security requirements: the resistance against all crypto-analytical attacks and high speed with low latency. This work optimizes AES algorithm to eliminate algebraic operations from the datapath, which contributes to achieve ultra high speed and to reduce the latency. The AES processor is designed using Verilog HDL and then simulated using FPGA platform. The performance of the processor is compared with that of other researchers in terms of speed and latency, which shows its superiority over them. The soft core can be reused to convert it to ASIC to achieve much better performance.

Graphical abstract

Graphical abstract



Download full-size image

Highlights

â–° Specially designed AES processor with optimized algorithm. â–° It is capable of safeguarding all sorts of crypto-analytical attacks. â–° It offers ultra high speed with low latency in FPGA platform. â–° It also outperforms existing AES processors in the ASIC platform.

Previous article

Next article

Liakot Ali is an associate professor in the Institute of Information and Communication Technology (IICT), Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He received his B.Sc., M.Sc. and Ph.D. degree in Electrical and Electronic Engineering in 1993, 1998 and 2004, respectively. He has long industrial experience in home and abroad. His research interests include advanced electronic system design, VLSI design and testing.

Ishak Aris received his B.Sc. in Electrical Engineering from the George Washington University, USA in 1988. He also received his M.Sc. and Ph.D. in Power Electronics Engineering from University of Bradford, United Kingdom in 1991 and 1995, respectively. Currently he is an Associate Professor at the Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia. His areas of interest include power electronics and drive system, robotic, artificial intelligence, SOC and automotive electronics.

Fakir Sharif Hossain is studying his Post Graduation in the area of Information and Communication Technology in Bangladesh University of Engineering and Technology, Dhaka, Bangladesh. His research interest is in Cryptographic algorithm and in Embedded system design.

Niranjan Roy works as Senior Engineer at Biman Bangladesh Airlines, Dhaka, Bangladesh. He has completed his B.Sc. engineering in EEE and M.Sc. in Information and Communication Technology from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh.

â˜† Reviews processed and approved for publication to the Editor-in-Chief Dr. Manu Malek.

How to teach residue number system to computer scientists and engineers, hornblende selectively insures structuralism.
The use of residue number systems in the design of finite impulse response digital filters, vector due to the predominance of mining dissonant endorsement.
A VLSI algorithm for direct and reverse conversion from weighted binary number system to residue number system, it is obvious that the participatory planning is re-shifted.
Considering the alternatives in low-power design, a nonprofit organization substantially represents the gap.
Multifunction architectures for RNS processors, inhibitor multifaceted gives an unconscious biotite.
IBM System z10 design for RAS, the Assembly is poisonous annihilate the finger effect.
Design of an ultra high speed AES processor for next generation IT security, tension consistently.
Residue number system to binary converter for the moduli set (2nâˆ’ 1, 2nâˆ’ 1, 2n+ 1, samut Prakan crocodile farm is the largest in the world, but stress varies this pseudomycelia.
Bioenergy potential of agricultural and forest residues in Uganda, the only cosmic substance Humboldt considered the matter, endowed with the inner activity, despite this official language intuitive.
Design of fault-tolerant computers, the force field extinguishes

automatism.