Design of an Ultra High Speed AES Processor for Next Generation IT Security.

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.

Item Type: Article