Effective implementation of AES-XTS on FPGA

ABSTRACT

This paper proposes an effective FPGA implementation for data storage encryption. Throughput, area and power consumption are the most important parameters to evaluate any FPGA implemented design. Our proposed design not only achieves a high throughput but also a considerable amount of throughput/area that is better compared to current implementations. The proposed implementation gives a memory based pipelined architecture. The design achieves a throughput of 5.25 Gb/sec that is relatively better than any other FPGA implementation to date. Xilinx ISE 10.1 is used as a design tool and Verilog HDL is used to code the design.

Keyword: Component; AES-XTS; Cryptography; Discryption; FPGA