Hardware Implementation of High Speed RC4 Algorithm in FPGA

Abstract

This paper presents high speed and an area efficient hardware implementation of the RC4 algorithm. The proposed design uses Block RAM (BRAM) implementation to reduce the area and to increase the speed of operation hence throughput. The proposed design uses only one 256 bytes simple dual port RAM for key stream generation and it takes 3 clock cycles per byte. It supports a variable key length of from 1 byte to 256 bytes and achieves 54.8MB/s throughput at 164.6MHz operating frequency. The design is targeted on XC2V250FG256 Xilinx FPGA and met the operating frequency of 164.6MHz. The RC4 algorithm is implemented in Verilog HDL.

References


Index Terms

Computer Science
Circuits And Systems

Keywords
BRAM  CPLD  FPGA  RC4 Algorithm  Stream Cipher  Simple Dual Port RAM.