Abstract

Proposed work presents high performance architecture for LILI-II stream cipher. This cipher uses 128 bit key and 128 bit IV for initialization of two LFSR. Proposed architecture uses single clock for both LFSRs, so this architecture will be useful in high speed communication applications. Presented architecture uses four bit shifting of LFSRD in single clock cycle without losing any data items from function FC. Proposed architecture is coded by using VHDL language with CAD tool Xilinx ISE Design Suite 13.2 and targeted hardware is Xilinx Virtex5 FPGA having device xc4vlx60, with package ff1148. Proposed architecture achieved throughput of 224.7 Mbps at 224.7 MHz frequency.

**Index Terms**

Computer Science  
Circuits And Systems

**Keywords**

LILI  Stream cipher  clock controlled  FPGA  LFSR.