Hardware implementation of RC4A stream cipher

ABSTRACT

Cryptography is the only practical method for protecting information transmitted through communication networks. The hardware implementation of cryptographic algorithms plays an important role because of growing requirements of high speed and high level of secure communications. Implementation of cryptographic algorithms on hardware runs faster than on software and at the same time offering more intrinsic security. This paper presents efficient hardware implementation of new stream cipher, RC4A. The proposed hardware implementation achieves a data throughput up to 22.28 MB/sec at frequency of 33.33 MHz and the performance in terms of throughput to area ratio equal to 0.37. The implementation is also parameterized in order to support variable key lengths, 8-bit to 512-bit. The cipher was designed using Verilog hardware description language and implemented into a single Altera APEXTM 20K200E Field Programmable Gate Array (FPGA).

Keyword: Cryptography; FPGA; RC4A; Security; Stream cipher; Throughput; Verilog HDL