World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:09, 2017

Improved Hash Value Based Stream CipherUsing Delayed Feedback with Carry Shift Register

Authors : K. K. Soundra Pandian, Bhupendra Gupta

Abstract : In the modern era, as the application data's are massive and complex, it needs to be secured from the adversary attack. In this context, a non-recursive key based integrated spritz stream cipher with the circulant hash function using delayed feedback with carry shift register (d-FCSR) is proposed in this paper. The novelty of this proposed stream cipher algorithm is to engender the improved keystream using d-FCSR. The proposed algorithm is coded using Verilog HDL to produce dynamic binary key stream and implemented on commercially available FPGA device Virtex 5 xc5vlx110t-2ff1136. The implementation of stream cipher using d-FCSR on the FPGA device operates at a maximum frequency of 60.62 MHz. It achieved the data throughput of 492 Mbps and improved in terms of efficiency (throughput/area) compared to existing techniques. This paper also briefs the cryptanalysis of proposed circulant hash value based spritz stream cipher using d-FCSR is against the adversary attack on a hardware platform for the hardware based cryptography applications.

Keywords : cryptography, circulant function, field programmable gated array, hash value, spritz stream cipher
Conference Title : ICCNS 2017 : International Conference on Cryptography and Network Security
Conference Location : Tokyo, Japan
Conference Dates : September 07-08, 2017