Abstract

In this paper two compact and high throughput hardware structures are proposed allowing for the computation of the 128-bit CLEFIA encryption algorithm and its associated key expansion processes. Given the needed modification to the CLEFIA Fiestel network, herein we show that with a small area and low performance impact, the CLEFIA key expansion for 128, 192 and 256-bit key can be deployed. This is achieved by using embedded components available in modern FPGAs and with an adaptable scheduling, allowing to compute the 4 and 8 branch CLEFIA Feistel network within the same structure. The obtained experimental results on a Xilinx Virtex 5 FPGA suggest that throughputs above 1Gbps can be achieved with a resource usage of 200 Slices and 3 BRAMs, achieving a throughput/Slice efficiency metric 50% higher when compared with limited state of the art.

Index Terms

Computer Science
Circuits and Systems

Keywords
CLEFIA, Encryption, Cipher, Key Expansion, FPGA