Abstract

Main fundamental directions which are considered as important for practical ciphers are (1) security, (2) speed, and (3) cost for implementations. To realize these fundamental directions CLEFIA is designed. Clefia is a first block cipher employing the Diffusion Switching Mechanism (DSM) to enhance the immunity against the differential attack and the linear attack. Clefia uses lightweight components for efficient software and hardware implementations. This paper proposes compact and high speed hardware implementation for block cipher clefia-128. This hardware architecture uses minimum hardware resources and maximum frequency of 135.452 Mhz, through which we can achieve a throughputs of 17 Gbit/s

References

8. Toru Akishita and Harunaga Hiwatari “Very Compact Hardware Implementations of the Block cipher CLEFIA” Sony Corporation
10. Takeshi Sugawara, Naofumi Homma, Takafumi Aoki and Akashi Satoh “High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA”

**Index Terms**

Computer Science Security

**Keywords**

Clefia, DSM, Encryption, FPGA and VHDL