Abstract

In this paper we demonstrate an efficient and compact reconfigurable hardware implementation of the Data Encryption Standard (DES) algorithm. Our design was implemented on FPGA of device VirtexEXCV400e. As a strategy to reduce the associated design critical path, we utilized a parallel structure that allowed us to compute all the eight DES S-boxes simultaneously. The testing of the implemented design shows that it is possible to generate data in 16 clock cycles when non-pipelined approach is employed. When pipelined approach is employed on the other hand, 17 clock signals are required for the initial phase only, and one clock signal is sufficient afterwards for each data generation cycle. The Very High Speed Integrated Circuit Hardware Description Language (VHDL) is used to program the design.

References

3. Karn, P.R. (Karns DES implementation source code)
15. NIST: Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Standards Publication (2001)
17. (Revised):, A.X. National Standards for financial institution key management (wholesale), American Bankers Association (1986)
18. 8732:, I.D. Banking-key management (wholesale), Association for Payment Clearing Services (1987)

Index Terms

Computer Science

Information Sciences
Keywords

DES, FPGA, Parallel structure.