**Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA**

**ABSTRACT**

In this paper, Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES) algorithm and their efficient hardware implementation in cyclone II Field Programmable Gate Array (FPGA) is analyzed with the help of Cipher Block Chaining (CBC) concept. The Data Encryption Standard (DES) has been the most extensively used encryption algorithm in recent times. Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The paper covers DES and Triple DES algorithm with Cipher Block Chaining concept, simulation results, basic FPGA technology and the implementation details of the proposed DES and Triple DES architecture. Register transfer level (RTL) of DES and Triple DES algorithm is designed, simulated and implemented separately using Verilog in different FPGA devices including Cyclone II, Spartan 3E, Vertex 5 and Vertex E series FPGAs. The results from the comparison with existing implementations show that the proposed design was efficient in all aspects.

**LANGUAGE USED:**

**TOOLS REQUIRED:**

* MODELSIM – Simulation
* XILINX-ISE – Synthesis