Abstract

Cryptography method which is used to increasing of information security voice and also teks on GSM communications mobile system is using with A5 algorithm cryptography. A5 algorithm is kind symetry algoritm where key is use for encryption and decryption process is same. A5 algorithm is divided into A5/1, A5/2, and the new version is A5/3..

This final project presents a design of A5/2 algorithm which can doing encryption and decryption process in one system. The design is using LFSR *(Linear Feedback Shift Register*) operation mode which used as generating concevutive random number, and will be modeled with using VHDL (*Very High Speed Integrated Circuit Hardware Language*) language. The design is will be simulated using Aldec Active HDL 3.5 and also synthesized using Xilinx ISE 8.1i, and device target using FPGA Virtex-4 XC4VLX25-10SF363C series.

This final project design implementation result by using device target FPGA Virtex-4 XC4VLX25-10SF363C series show *top level entity* capable work on maximum frequency 198,159 MHz and required slices 2% (292 out of 10,752), and also required 6% IOBs (15 out of 240).

Keywords : *Cryptography, GSM (Global System for Mobile Communications, A5, A5/2,* LFSR *(Linear Feedback Shift Register*), FPGA.