ABSTRACT

Along with the expanding of information technology, communication media and data flow system have lot varieties than before. This expand makes make communication easier than before. But, this expands also made a new problem in information security.

One kind of information security method is cryptography. With this method, data is ciphered before it's transmitted. One kind of cryptograph algorithm is A5 which used in Global System for Mobile communication (GSM) and divided into A5/1, A5/2, and the new one, A5/3.

In this final Task will be done a design of A5/1 algorithm using VHDL and then implemented to Field Programmable Gate Array (FPGA) Virtex-4 XC4VLX25-10SF363C series. Encrypt and decrypt process done only for one direction. The output is analyzed to get information about avalanche effect, and the output bit frequency from the ciphered information. Design is simulated using Aldec Active-HDL 3.5 software. And the result of implementation is monitored by using LA-2124A logic analyzer.

The results of design analyzing shows that designed system have almost 50% for avalanche effect ,ciphertext bit frequency, and transformation bit frequency. Synthesis report for encryption part shows the system needs 1% of Slices, 0% of Slice Flip Flops, 1% of 4 input LUTS, 3% of bonded IOBs, and 3% of GLCKs of all resource in device with maximum clock frequency is 126,173 MHz. And synthesis report for decryption part shows the system needs 1% of Slices, 0% of Slice Flip Flops, 0% of 4 input LUTS, 2% of bonded IOBs, and 3% of GLCKs of all resource in device with maximum clock frequency is 125,796 MHz.