ABSTRACT

Nowadays, many types of voice communication are still not accompanied with safety. This final project offers a solution for voice messaging security by using Rijndael algorithm. Rijndael algorithm is standard cryptographic algorithm that have been assigned by NIST (*National Institute of Standards and Technology*). Now Rijndael algorithm known as AES (*Advanced Encryption Standard*). AES Rijndael is a block cipher algorithm that using permutation and substitution system (P-Box and S-Box).

In this final project is modeled using VHDL programming language and simulated using Modelsim SE 6.5 then synthesized and implemented using Xilinx ISE 8.1. This final project is using FPGA VIRTEX-4 XC4VLX25 FF668-10 as target device.

The result of modeling and simulating synthesized into hardware using Xilinx Shynthesize Tools. From voice encryption synthesize block can be obtained system resource that required 7% *slice flip-flop*, 7% 4 input LUT, 10 % occupied slice, 100 % related logic slice, 6% IOB, 12% BUFG. Minimum period 4.516 ns (Maximum Frequency: 221.420 MHz). Overall, this research proves that voice encryption using Rijndael algorithm can be implemented on the FPGA. However for decryption block not appropriate with Rijndael Algorithm. For the future the output can be applied for real-time.

Keyword : cryptograph, AES Rijndael, VHDL, FPGA