ABSTRACT

This final project presents an implementation of symmetric cryptography algorithm AES (Advanced Encryption Standard) that use key length of 128 bits which can processes either encryption or decryption in one core (Xilinx XC2300E PQ208-6). The implementation used ECB (Electronic Code Book) operation mode. The implementation design is modeled in VHDL (Very High Speed Integrated Circuit Hardware Language), then simulated using ModelSim SE 6.0 based on KAT (Known Answer Test) from the AES creator. It is also sinthesized and implemented using Xilinx ISE 7.1.03i, then verified on chip using Chipscope Pro 7.1.03i.

The results of implementation show that the AES-128 core is available on maximum frequency 28.771 MHz with throughput 167,395 Mbps on that frequency and the circuit area needed is 35.460 equivalent gates.

Key word: AES-128, ECB, VHDL, Encryption, Decryption, KAT, Throughput, Area.