INTISARI

IMPLEMENTASI ALGORITME *ADVANCED ENCRYPTION STANDARD* (AES) 128-BIT PADA *FIELD PROGRAMMABLE GATE ARRAY* (FPGA)

Oleh

Muhammad Shofuwan Anwar

18/431931/SV/15902

Ilmu kriptografi memiliki peran penting pada bidang keamanan informasi dan data. Kriptografi sering digunakan sebagai penjaga keamanan data atau informasi, baik informasi yang dikirimkan melalui saluran komunikasi ataupun informasi yang disimpan pada media penyimpanan. Salah satu kriptografi modern yang digunakan sampai saat ini adalah algoritme Rijndael yang ditetapkan sebagai *Advanced Encryption Standard*. Rijndael dipilih karena kemudahan dalam perancangannya dan dalam implementasinya. Tujuan dari penelitian ini adalah melakukan perbandingan implementasi AES pada level perangkat keras dan perangkat lunak, penelitian ini meliputi simulasi dan implementasi enkripsi AES pada perangkat keras FPGA.

Penelitian ini membandingkan data pada FIPS 197 dengan simulasi dan implementasi dari rancangan *engine* AES. Implementasi dari *engine* AES dibagi menjadi dua jenis yaitu pada level perangkat keras dengan melakukan implementasi pada FPGA dan pada level perangkat lunak dengan melakukan implementasi pada prosesor *Zynq*. Implementasi pada level perangkat keras dan perangkat lunak dibandingkan untuk mengetahui perbedaan kecepatan proses.

Implementasi dirancang menggunakan VHDL (*Very High Speed Integrated Circuit Hardware Description Language*) dan perangkat lunak Vivado. Penelitian ini menggunakan perangkat keras FPGA Xilinx Zynq Arty-Z7 dengan seri XC7Z020-1CLG400C. *Top Level Design* mampu bekerja dengan frekuensi maksimum sebesar 110,901 MHz dengan latensi siklus 11 *clock* serta membutuhkan 5,46% LUT (2907 dari 53200), 2,11% FF (2240 dari 106400), 3,13% BUFG (1 dari 32). Pengujian dan implementasi modul enkripsi dengan referensi data FIPS-197 (2001) mampu bekerja dengan baik dan menghasilkan *ciphertext* yang sama.

Kata Kunci : *FPGA, AES, kriptografi, enkripsi, zynq*

ABSTRACT

IMPLEMENTATION OF 128-BIT ADVANCED ENCRYPTION STANDARD ALGORITHM (AES) USING FIELD PROGRAMMABLE GATE ARRAY (FPGA)

By

Muhammad Shofuwan Anwar

18/431931/SV/15902

Cryptography takes an important role in the field of securing information and data. Cryptography frequently used for information and data security to keep them safe. On the other hand, Cryptography is widely used to keep the information in the communication process or data saved in media storage. There is much modern Cryptography art, one of which is the Rijndael algorithm be appointed as Advanced Encryption Standard and was chosen because of the easiest design and implementation process. The goals of this research field are the implementation of the AES algorithm on a hardware level and software level covered by the simulation and the implementation of AES encryption on the FPGA hardware.

Comparing the data between engine AES design with FIPS 197 utilizing simulation and implementation is covered by this research. Implementation of engine AES is divided into two such as hardware level by using FPGA and software level by using Zynq processor. Comparing the processing speed between hardware level and software level also discussed in this research.

VHDL (Very High Speed Integrated Circuit Hardware Description Language) and Vivado software is used to implementing the AES engine design. This research using FPGA Xilinx Zynq Arty-Z7 with the XC7Z020-1CLG400C series as a hardware implementation. Top Level Design can afford maximum frequency at 110,901 MHz with 11 clock latencies and need a 5,46% LUT (2907 from 53200), 2,11% FF (2240 from 106400), 3,13% BUFG (1 from 32). Testing and implementation of encryption modules with reference from FIPS-197 (2001) can work well with the equal ciphertext output.

Keywords : ***FPGA, AES, cryptography, encryption, zynq***