INTISARI

IMPLEMENTASI *ADVANCED ENCRYPTION STANDARD* (AES) PADA *FIELD PROGRAMMABLE ARRAY* (FPGA) MENGGUNAKAN METODE *CHIPER IN CLB-KEY EXPANSION IN CLB-SERIAL* (CC-KC-S) DAN *PIPELINE*

Oleh:

Ikhsan Loviandri

17/412567/PA/17886

AES (*Advanced Encryption Standard*) adalah lanjutan dari algoritma enkripsi standar DES (*Data Encryption Standard*) yang masa berlakunya dianggap telah usai karena faktor keamanan.

Penelitian sebelumnya yang menggunakan metode *chiper in clb-key expansion in clb-serial* (CC-KC-S) belum dipadukan dengan pipeline, sehingga penelitian ini difokuskan pada implementasi AES yang menggunakan metode *chiper in clb-key expansion in clb-serial* (CC-KC-S) yang menggunakan *pipeline.*

Rancangan sistem AES pada penelitian kali ini menggunakan AES-128 bit. Implementasi dideskripsikan menggunakan bahasa VHDL dan perangkat lunak Vivado 2019.2. Penelitian ini menggunakan perangkat keras FPGA Xilinx Artix-7 seri XC7A100T-1CSG324C pada papan Nexys A7-100T. Rancangan desain tingkat atas menggunakan sumber daya: LUT sebesar 13,01%, FF sebesar 2,30%, BRAM sebesar 7,41%, IO sebesar 1,43%, dan BUFG sebesar 6,25%. Frekuensi maksimum sistem adalah 131,735 MHz dengan *throughput* yang dihasilkan sebesar 259,6 Gbps.

Kata kunci: AES, AES-128 bit, Pippeline, FPGA

ABSTRACT

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) ON FIELD PROGRAMMABLE ARRAY (FPGA) USING CHIPER IN CLB-KEY EXPANSION IN CLB-SERIAL *(CC-KC-S)* METHODE AND PIPELINE

By:

Ikhsan Loviandri

17/412567/PA/17886

AES (Advanced Encryption Standard) is a continuation of DES (Data Encryption Standard) that considered to be obsolete due to security factors.

Previous research using the cipher in clb-key expansion in clb-serial (CC-KC-S) method has not been combined with the pipeline, so this research is focused on the implementation of AES using the cipher in clb-key expansion in clb-serial (CC-serial) method. KC-S) using pipelines.

The design of the AES system in this study uses AES-128 bit. Implementation is described using the VHDL language and using software Vivado 2019.2. This research uses hardware Xilinx Artix-7 series FPGA XC7A100T-1CSG324C on the Nexys A7-100T board. The top-level design uses resources: LUT 13.01%, FF 2.30%, BRAM 7.41%, IO 1.43%, and BUFG 6.25%. Maximum frequency in this system is 131.735 MHz with throughput 259,6 Gbps.

Keywords: AES, AES-128 bit, Pippeline, FPGA