INTISARI

AES adalah sebuah algoritma yang paling sering digunakan pada semua perangkat tanpa termasuk perangkat keras. AES diakui sebagai algoritma kriptografi simetri paling aman dalam proses kriptografi pesan dan juga menjadi yang tersulit untuk dipecahkan proses enkripsinya. Penerapannya pada *Field Programmable Gate Array* (FPGA) juga banyak dijadikan kajian karena prosesnya yang kompleks membutuhkan sumber daya yang lebih sehingga banyak yang menerapkan arsitektur terbaru untuk mengoptimalkan penerapannya di FPGA. Penelitian ini berfokus pada optimasi algoritma *Advanced Encryption Standard* (AES) berbasis *Field Programmable Gate Array (FPGA)* dengan menerapkan teknik putaran terbuka dan berbagi sumber daya untuk meningkatkan efisiensi proses kriptografi. Teknik putaran terbuka memungkinkan pengurangan jumlah siklus *clock* dengan memproses beberapa iterasi putaran secara paralel, sementara berbagi sumber daya memanfaatkan perangkat keras secara efisien dengan membagi sumber daya antar modul enkripsi dan dekripsi. Implementasi dilakukan pada FPGA Xilinx Artix-7 100T Nexys-4 menggunakan bahasa pemrograman VHDL dan dirancang melalui perangkat lunak Vivado 2023.2. Sistem ini diuji berdasarkan konsumsi daya, throughput, latensi, dan validasi data sesuai standar AES.

Hasil implementasi mendapatkan latensi sistem sebesar 10 siklus, dengan luaran mencapai 2,13 Gbps. Penggunaan sumber daya mencakup 341 *Look-Up Table* (LUT) dari 63.400 (0,54%), 696 flip-flop dari 126.800 (0,55%), dan 8 dari 210 I/O (3,8%). Konsumsi daya total adalah 0.101 watt, dengan 96% berasal dari konsumsi daya statis dan daya dinamis hanya 4%, terbagi ke *clocks* (47%), sinyal (11%), logika (8%), dan I/O (34%). *Propagation delay* sebesar 6.008 ns (87.034% *routing*, 12.966% logika) memastikan tidak ada pelanggaran pewaktuan, dengan *slack* positif 3.633 nd untuk *setup* dan 0.106 nd untuk *hold timing* serta diperoleh sistem dengan frekuensi maksimum sebesar 165.5 MHz.

Kata kunci : FPGA, AES (*Advanced Encryption Standard*), *Putaran Terbuka*, *Berbagi Sumber Daya*,

ABSTRACT

AES is an algorithm widely utilized across all devices, including hardware. It is recognized as the most secure algorithm in cryptographic message processes and one of the most challenging to break in terms of encryption. Its implementation on Field Programmable Gate Array (FPGA) has been extensively studied due to its complex process, which requires more resources, leading to the adoption of new architectures to optimize its application on FPGA. This study focuses on optimizing the Advanced Encryption Standard (AES) algorithm on FPGA using loop unrolling and resource sharing techniques to enhance the efficiency of cryptographic processes. The loop unrolling technique reduces the number of clock cycles by processing multiple loop iterations in parallel, while resource sharing efficiently utilizes hardware by sharing resources between encryption and decryption modules. The implementation was carried out on an FPGA Xilinx Artix-7 100T Nexys-4 using the VHDL programming language and designed with Vivado 2023.2 software. The system was evaluated based on power consumption, throughput, latency, and data validation in compliance with AES standards.

The implementation results achieved a system latency of 10 cycles with a throughput of 2,13 Gbps. Resource usage included 341 Look-Up Tables (LUT) out of 63,400 (0.54%), 696 Flip-Flops out of 126,800 (0.55%), and 8 out of 210 I/O pins (3.8%). Total power consumption was 0.101 Watts, with 96% attributed to static power and only 4% to dynamic power, distributed among clocks (47%), signals (11%), logic (8%), and I/O (34%). The propagation delay was 6.008 ns (87.034% routing, 12.966% logic), ensuring no timing violations with a positive slack of 3.633 ns for setup and 0.106 ns for hold timing, achieving a maximum frequency of 165.5 MHz.

Keywords: FPGA, AES (Advanced Encryption Standard), Loop Unrolling, Sharing Resource