INTISARI

IMPLEMENTASI ALGORITMA SHA-3 PADA *FIELD PROGRAMMABLE LOGIC ARRAY* (FPGA) MENGGUNAKAN DSP48 DAN *PIPELINE*

Oleh:

Andriyana Nugraha Saputra

17/414574/PA/18074

SHA-3 merupakan algoritma kriptografi terbaru yang dirilis oleh NIST sebagai penerus dari SHA-2. Implementasi SHA-3 pada FPGA masih memerlukan sumber daya yang banyak untuk mencapai *throughput* yang tidak signifikan. Penelitian ini difokuskan pada fungsi permutasi SHA-3 yang terdapat operasi logika. Penelitian ini menggunakan DSP48 yang tersedia pada FPGA Xilinx untuk mempercepat proses operasi logika pada algoritma SHA-3 dan delapan tahap *pipeline* untuk memotong waktu *delay* lebih lanjut.

Rancangan sistem algoritma SHA-3 pada penelitian ini terdiri dari modul antarmuka, *data path* dan kontroler. Implementasi dirancang menggunakan VHDL dan perangkat lunak Vivado 2020.2. Penelitian ini menggunakan perangkat keras FPGA Xilinx Artix-7 seri XC7A100T-1CSG324C pada papan Nexys A7-100T. Rancangan *top level design* memanfaatkan sumber daya berupa: LUT sebesar 8,11% (5.140 dari 63.400), LUTRAM sebesar 4,21% (800 dari 19.000), FF sebesar 2,72% (3.444 dari 126.800), BRAM sebesar 16,67% (22,5 dari 135), DSP sebesar 59,17% (142 dari 240), IO sebesar 1,43% (3 dari 210) dan BUFG sebesar 9,38% (3 dari 32). Frekuensi maksimum sistem yaitu 107,979 MHz dan *throughput* yang dihasilkan yaitu 5,183 Gbps untuk SHA3-224, 4,895 Gbps untuk SHA3-256, 3,743 Gbps untuk SHA3-384 dan 2,591 Gbps untuk SHA3-512.

Kata kunci: SHA-3, FPGA, DSP48, *pipeline*

ABSTRACT

IMPLEMENTATION OF SHA-3 ALGORITHM ON FIELD PROGRAMMABLE LOGIC ARRAY (FPGA) USING DSP48 AND PIPELINE

By:

Andriyana Nugraha Saputra

17/414574/PA/18074

SHA-3 is a new cryptographic algorithm released by NIST as a successor to SHA-2. SHA-3 implementation in FPGA still needs many resources to get moderate throughput. This study focus on permutation function in SHA-3 that have logic operations. This study uses DSP48 that is available in Xilinx FPGAs to speed up logic algorithm in SHA-3 algorithm and eight stage pipeline to cut delay time further.

The SHA-3 design in this research consists of an interface module, data path and controller. Implementation is designed using the VHDL on Vivado 2020.2 software and FPGA Xilinx Artix-7 series XC7A100T-1CSG324C in Nexys A7-100T board. The top level design requires 8.11% LUT (5,140 out of 63,400), 4.21% LUTRAM (800 out of 19,000), 2.72% FF (3,444 out of 126,800), 16.67% BRAM (22.5 out of 135), 59.17% DSP (142 out of 240), 1.43% IO (3 out of 210) and 9.38% BUFG (3 out of 32). The maximum frequency in this system is 107.979 MHz and the throughput achieved by this design are 5,183 Gbps for SHA3-224, 4,895 Gbps for SHA3-256, 3,743 Gbps for SHA3-384 and 2,591 Gbps for SHA3-512.

Keywords: SHA-3, FPGA, DSP48, pipeline