INTISARI

Aritmatika modular terdiri dari penjumlahan modular, pengurangan, perkalian dan perpangkatan. Operasi perkalian modular merupakan operasi yang sangat penting dalam aritmatika modular sehingga diperlukan implementasi pada perangkat keras yang dapat mengeksekusi instruksi secara efisien agar dapat memiliki kinerja yang bagus. Penelitian ini menggunakan algoritma *Add-based Length-scalable Dual-field Modular Multiplication-Addition-Subtraction* (ALDMAS) untuk melakukan operasi perkalian modular dan diimplementasikan pada perangkat keras FPGA. Rancangan terdiri dari modul antarmuka, *data-path* dan kontroler. Pengujian pada penelitian ini meliputi simulasi dan implementasi sistem secara keseluruhan dan modul pengali modular dengan delapan jumlah bit atau lebar data.

Implementasi dirancang menggunakan VHDL dan perangkat lunak Vivado 2018.2. Penelitian ini menggunakan perangkat keras FPGA Xilinx Artix-7 Nexys-4 seri XC7A100T-1CSG324. *Top level design* dengan lebar data 8-bit mampu bekerja pada frekuensi maksimum sebesar 167,169 MHz serta membutuhkan 0,33% LUT (210 dari 63.400), 0,11% FF (145 dari 126.800), dan 6,67% blok IO (14 dari 210). Pengujian dan implementasi modul pengali modular dengan sembilan buah lebar data menunjukkan penggunaan sumber daya perangkat keras berupa LUT, FF, I/O dan DSP semakin besar seiring dengan besarnya lebar data dan titik kritis penggunaan sumber daya terjadi pada saat lebar data 512-bit. Selain itu, analisis pewaktuan pada setiap lebar data menunjukkan bahwa lebar data ≥ 64-bit memiliki nilai yang signifikan dan tetap.

Kata kunci : perkalian modular, FPGA, algoritma ALDMAS

ABSTRACT

Modular arithmetic consists of modular addition, multiplication, substraction, and exponentiation. Since modular multiplication operation is very important operations in modular arithmetic, so implementation on hardware that can execute efficienly to achieve a good performance system. This research uses Add-based Length-scalable Dual-field Modular Multiplication-Addition-Subtraction (ALDMAS) algorithm to perform modular multiplication operations and implemented on the FPGA. The design consists of an interface module, data-path, and controller. Testing in this research includes simulation and hardware implementation of top level design and modular multiplier module with eight data width.

Implementation is designed using the VHDL description language on Vivado 2018.2 software and FPGA Xilinx Artix-7 Nexys-4 series XC7A100T-1CSG324 as hardware. The top level design with 8-bit data width are able to work at maximum frequencies of 167,169 MHz, and requires 0.33% LUT (210 out of 63,400), 0.11% FF (145 out of 126,800), and 6.67% block IO (14 of 210). Testing and implementing a modular multiplier module with eight data widths shows the use of hardware resources like LUT, FF, I/O and DSP block is getting bigger along with the large of data width the critical point of resource usage occurs when the data width is 512-bit. Also, the timing analysis for each data width shows that the data width ≥ 64-bit has a significant and constant value.

Keyword : modular multiplication, FPGA, ALDMAS algorithm