INTISARI

Implementasi Algoritme RSA pada Field Programmable Gate Array (FPGA) menggunakan Algoritme Montgomery

Oleh
Esti Kurniasari
13/352643/PA/15685

Sistem keamanan dalam komunikasi data disebut kriptografi. Aplikasi pengamanan data seperti surat elektronik, *e-commerce*, dan *e-passport*. Kriptografi RSA melibatkan operasi perpangkatan yang memerlukan sumber daya yang lebih banyak dibandingkan operasi aritmatika lain pada implementasi perangkat keras. Perangkat keras dapat mengeksekusi instruksi secara efisien, oleh karena itu kriptografi RSA perlu diimplementasikan pada perangkat keras.

Penelitian ini menggunakan algoritme *Montgomery* untuk melakukan operasi perpangkatan dan algoritme *Extended Euclidean* pada proses pembangkitan kunci. Implementasi masing-masing algoritme diawali dengan penentuan operasi dasar yang terlibat dalam RSA seperti operasi modular, perkalian, pembagian, dan pengurangan. Dilanjutkan perancangan modul yang dapat melakukan fungsi tersebut. Modul pada hierarki terendah menjadi komponen dari modul pada hierarki yang lebih tinggi. Sinyal kendali dirancang agar dapat melakukan pengaturan aliran data sehingga sistem dapat melakukan fungsinya sesuai diagram alir algoritme. Pengujian pada penelitian ini meliputi pengujian simulasi, implementasi perangkat keras, frekuensi maksimum, dan lewatan.

Implementasi dirancang dengan menggunakan bahasa deskripsi VHDL dan perangkat lunak Vivado 2017.1. Penelitian ini menggunakan FPGA Nexys 4 Artix 7 seri XC7A100T-1CSG324C sebagai *device target*. Desain *top level* mampu bekerja pada frekuensi maksimum 133,76 MHz dan membutuhkan 17,66 % LUT (11.195 dari 63.400) dan 7,14% IOBs (15 dari 210).

Kata Kunci : kriptografi, RSA, FPGA, enkripsi, dekripsi

ABSTRACT

Implementation of RSA Algorithm on Field Programmable Gate Array (FPGA) using Montgomery Algorithm

By
Esti Kurniasari
13/352643/PA/15685

Security system in data communication called Cryptography. Data security applications such as electronic mail, e-commerce, and e-passports. RSA cryptography involves exponentiation that requires more resources than other arithmetic operations on hardware implementation. Hardware can execute instructions efficiently, therefore RSA cryptography needs to be implemented on hardware.

This research uses the Montgomery algorithm to carry out exponentiation operations and Extended Euclidean algorithms in the key generation. Implementation of each algorithm starts with determining the basic operations involved in RSA such as modular, multiplication, division, and subtraction operations. Continued by designing of modules that can perform these functions. Modules in the lowest hierarchy are component of modules in higher hierarchies. The control signal is designed to be able to adjust the data flow so that the system can perform its functions according to the algorithm flowchart. Testing on this research includes simulation, hardware implementation, maximum frequency, and throughput.

Implementation is designed using the VHDL description language and Vivado 2017.1 software. This study uses Nexys 4 Artix 7 FPGA series XC7A100T-1CSG324C as the target device. The top level design is able to work at a maximum frequency of 133.76 MHz and requires 17.66% LUT (11,195 of 63,400) and 7.14% IOBs (15 of 210).

***Keyword** : cryptography, RSA, FPGA, encryption, decryption*