ABSTRACT

One of important things in data communication is a security system. This system is so important that users feel secured when communicate. High-level security system can be applied for some data deliveries, such as *e-mail*, *e-commerce*, etc. Security system in data communication is well known as cryptography. One of cryptography algorithms used for *credit card* coding is *Rivest-Shamir-Adleman* (*RSA)*.

RSA is an asymetric algorithm which uses different keys in its proccess. They are *public key* and *prívate key. Public key* is used for encryption and *prívate key* is used for decryption. Two main operations consisted in *public key* are modulo multiplication and exponential proccess.

Modulo multiplication rules the *RSA* algorithm. An algorithm which can implement the multiplication is *Montgomery*. *Montgomery* can be applied in hardware because of its efficiency. 512-bit width is minimum value for *RSA* cryptography. The *RSA* construction starts from translating the multiplication algorithm into a computer. The design is drawn by using VHDL dan simulated by using Modelsim SE 6.0. The implementation and synthesizing are proccessed by Xilinx ISE 8.1i. Finally, the result is transfered to a device named FPGA SPARTAN 3 XC3S1000 FT256-4C.

This final project design implementation result by using device target FPGA Spartan 3 XC3S1000 FT256-4C series show *top level entity* capable work on maximum frequency 39,469 MHz and required slices 32% (2485 out of 7680), and also required 7% IOBs (13 out of 173).

Keywords:*Cryptography, RSA, FPGA, Montgomery*