ABSTRACT

Nowadays, the development of technology is increasing rapidly. Each of these technological developments also include the dissemination of information. Dissemination of information can be done very easily and quickly. However, the confidentiality of that information becomes a big problem. The information is abused by irresponsible person.

Computer security systems becomes a very important thing to be considered in the confidentiality's issue of such information. Cryptography science is very useful in computer security systems. Of the many cryptography science, one of them is the implementation of cryptography at the IC prototype level.

The research prototype of FPGA based encryption and decryption system using Grain-128 stream cipher algorithm. The inputs in this research is binary form. The method that used in this research is using NFSR (Non-Linear Feedback Shift Register) and LFSR (Linear Feedback Shift Register). Verilog Hardware Description Language (HDL) as programming languange to describe the digital circuit function. The result to be tested in this research is encryption and decryption process analysis, encryption and decryption time process, avalanche effect, clock, and area.

Keywords : Prototype, Cryptography, Grain-128, FPGA