Optimized Hardware Implementation of Enhanced TRIPLE-DES using Cluster LUT and Pipelining on SPARTEN FPGA

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 164
Number 4

Year of Publication: 2017

Authors:
Amany Sarhan, Marwa Fayez, Noha Hussen

10.5120/ijca2017913608

Abstract

Due to the rapid use of Internet technology, a need for security mechanisms has appeared to protect the information. Cryptography is one of the most effective techniques used to protect and secure information. Triple Data encryption standard is a cryptography system that provides security in the commercial enterprise. A lot of research has been made over DES and Triple DES algorithms to enhance their performance. In this paper, an Enhanced Triple-DES Algorithm based on Cluster LUT (Look Up Table) and Pipelining (ETDCP) is proposed, as a modification of the Triple DES. ETDCP algorithm uses Cluster LUT in hardware implementation and uses the large embedded memories available in the SPARTAN-E FPGA as hardware designed to obtain the minimum utilized resource. Using cluster LUT diminishes the consumption power by reducing the number of registers and slice/area, which decreases the number of logic utilizations used for Spartan Xilinx FPGA. In addition, ETDCP uses pipelining techniques which will increase the processing rate. The experimental results are based on simulated and synthesized (Xilinx Spartan–E) using ModelSim 6.5 and VHDL code. The results show high throughput/area FPGA implementation. The simulation result also proves that the proposed
FPGA implementation of ETDCP algorithm has better speed performance compared to previous implementations of cryptographic algorithms.

References


Index Terms
Computer Science Security

Keywords
Cryptography, DES, FPGA, Spartan-E, Custer LUT, Pipelining.