Serpent Cryptography on Static and Dynamic Reconfigurable Hardware

Issam Damaj (Member IEEE)
Dept. of Electrical and Computer Engineering
Hariri Canadian Academy for Sc. and Tech.
P.O. Box 10 Damour 2010 Shouf, Lebanon
damajiw@hariricanadian.edu.lb

May Itani, and Hassan Diab (Fellow IEEE)
Dept. of Electrical and Computer Engineering
Faculty of Engineering and Architecture
American University of Beirut
P.O. Box 11-0236, Beirut, Lebanon
may11@aub.edu.lb; diab@aub.edu.lb

Abstract

This paper presents parallel reconfigurable hardware implementations of the Serpent (AES Finalist) cryptographic algorithm. Currently, Serpent is well known to be a simple but very strong encryption algorithm. The use of such an algorithm within critical applications, such as banking and military, requires efficient and highly reliable hardware implementation. We will stress the affordability of such requirements by analyzing and evaluating parallel Serpent implementations using static and dynamic reconfigurable systems. The used systems are the MorphoSys dynamically reconfigurable computer and The RC-1000 statically reconfigurable system from Celoxica Ltd with its 2 million gates Xilinx Virtex-E FPGA. In this paper, different designs for the Serpent corresponding to different Degrees of parallelism are presented. Moreover, implementation, realization, and performance analysis and evaluation of the mapped designs are included.