Jordan University of Science and Technology

AN EFFICIENT FPGA HARDWARE IMPLEMENTATION OF THE THREEFISH TWEAKABLE BLOCK CIPHER

Authors: Hussein R. Al-Zoubi, Anas M. Bataineh, and Osama D. Al-Khaleel

Abstract: Computer security has a significant importance in today?s world. Encryption and decryption of sensitive and important data are required for everyday tasks including electronic, data communications, and internet transactions. A large number of encryption and decryption algorithms have been developed in literature to fulfil the job. Many of these algorithms have been standardized. This paper examines the ThreeFish tweakable block cipher and provides an efficient field programmable gate array hardware implementation of the ThreeFish-256, ThreeFish-512, and ThreeFish-1024 encryption and decryption algorithms. Experimental results are provided and comparisons with the state of the art implementations are made. Experimental results illustrate the efficiency of the proposed implementation.