A case Study of Key-dependent Permutations in Feistel Ciphers

Abstract— **Many attempts have been made to strengthen Feistel based block ciphers. Among the successful proposals is the key-dependent S-box which was implemented in some of the high-profile ciphers. In this paper a key-dependent permutation box is proposed and implemented on DES as a case study. The new modified DES, MDES, was tested against Diehard statistical test, Avalanche test, and performance test. The results showed that in general MDES is more resistible to attacks than DES with negligible overhead. Therefore, it is believed that the proposed key-dependent permutation should be considered as a valuable primitive that can help strengthen the security of Substitution-Permutation Network which is a core design in many Feistel based block ciphers.**

***Index Terms*— Block Cipher, Feistel Structure, DES, Diehard test, Avalanche Effect**