Cryptology ePrint Archive: Report 2011/685

Cryptanalysis of Symmetric Block Ciphers Based on the Feistel Network with Non-bijective S-boxes in the Round Function

Roman Oliynykov

Abstract: We consider ciphertext-only attack on symmetric block ciphers based on the Feistel network with secret S-boxes installed as an additional parameter, like in Soviet GOST 28147-89. In case when S-boxes are generated by authorized agency and cannot be verifi ed by enc user of the cipher (e.g., in case of special equipment for encryption), application of non-bijective S-boxes allows significantly decrease decipheri complexity for authorized agency preserving high-level strength for other cryptanalysts.We show that it is necessary to have non-bijective S-box which outputs form non-trivial subgroup and give an example for deciphering complexity with known and secret non-bijective S-boxes for GOS

Category / Keywords: block ciphers, Feistel network, ciphertext-only attack

Date: received 16 Dec 2011, last revised 16 Dec 2011

Contact author: ROliynykov at gmail com