Cryptology ePrint Archive: Report 2011/551

Security Evaluation against Differential Cryptanalysis for Block Cipher Structures

Shengbao Wu and Mingsheng Wang

Abstract: Estimating immunity against differential and linear cryptanalysis is essential in designing secure block ciphers. A practical measure to achieve it is to find the minimal number of active S-boxes, or a lower bound for this minimal number. In this paper, we provide a general algorithm using integer programming, which not only can estimate a good lower bound of the minimal differential active S-boxes for various block cipher structures, but also provides an efficient way to select new structures with good properties against differential cryptanalysis. Experimental results for the Feistel, CAST256, SMS4, CLEFIA and Generalized Feistel structures indicate that bounds obtained by our algorithm are the tightest except for a few rounds of the SMS4 structure. Then, for the first time, bounds of the differential active S-boxes number for the MISTY1, Skipjack, MARS and Four-cell structures are illustrated with the application of our algorithm. Finally, our algorithm is used to find four new structures with good properties against differential cryptanalysis. Security evaluation against liner cryptanalysis can be processed with our algorithm similarly by considering dual structures.

Category / Keywords: block cipher structures, active S-boxes, integer programming, differential cryptanalysis

Date: received 6 Oct 2011, last revised 6 Oct 2011

Contact author: wushengbao at is iscas ac cn;mingsheng_wang@yahoo com cn