Cryptology ePrint Archive: Report 2011/123

Zero-Correlation Linear Cryptanalysis of Block Ciphers

Andrey Bogdanov and Vincent Rijmen

Abstract: Linear cryptanalysis, along with differential cryptanalysis, is an important tool to evaluate the security of block ciphers.This work introduces a novel extension of linear cryptanalysis -- zero-correlation linear cryptanalysis -- a technique applicable to many block cipher constructions. It is based on linear approximations with a correlation value of exactly zero. For a permutation on n bits, an algorithm of complexity 2^{n-1} is proposed for the exact evaluation of correlation. Non-trivial zero-correlation linear approximations are demonstrated for various block cipher structures including AES, balanced Feistel networks, Skipjack, CLEFIA, and CAST256. Using the zero-correlation linear cryptanalysis, a key-recovery attack is shown on 6 rounds of AES-192 and AES-256 as well as 13 rounds of CLEFIA-256.

Category / Keywords: secret-key cryptography / block cipher, linear cryptanalysis, linear approximation, linear hull, correlation, evaluation of correlation, substitution-permutation network, Feistel cipher, AES, CLEFIA

Publication Info: A version of this paper is submitted to a journal.

Date: received 7 Mar 2011, last revised 25 Oct 2011

Contact author: andrey bogdanov at esat kuleuven be