Cryptology ePrint Archive: Report 2013/211

A new criterion for avoiding the propagation of linear relations through an Sbox (Full version)

Christina Boura and Anne Canteaut

Abstract: In several cryptographic primitives, Sboxes of small size are used to provide nonlinearity. After several iterations, all the output bits of the primitive are ideally supposed to depend in a nonlinear way on all of the input variables. However, in some cases, it is possible to find some output bits that depend in an affine way on a small number of input bits if the other input bits are fixed to a well-chosen value. Such situations are for example exploited in cube attacks or in attacks like the one presented by Fuhr against the hash function Hamsi. Here, we define a new property for nonlinear Sboxes, named (v,w)-linearity, which means that 2^w components of an Sbox are affine on all cosets of a v-dimensional subspace. This property is related to the generalization of the so-called Maiorana-McFarland construction for Boolean functions. We show that this concept quantifies the ability of an Sbox to propagate affine relations. As a proof of concept, we exploit this new notion for analyzing and slightly improving Fuhr's attack against Hamsi and we show that its success strongly depends on the (v,w)-linearity of the involved Sbox.

Category / Keywords: secret-key cryptography / Sbox, Boolean function, hash functions, cryptanalysis

Publication Info: Extended version of FSE 2013 paper

Date: received 11 Apr 2013

Contact author: Anne Canteaut at inria fr