Cryptology ePrint Archive: Report 2013/022

Nonlinear cryptanalysis of reduced-round Serpent and metaheuristic search for S-box approximations.

James McLaughlin and John A. Clark

Abstract: We utilise a simulated annealing algorithm to find several nonlinear approximations to various S-boxes which can be used to replace the linear approximations in the outer rounds of existing attacks. We propose three variants of a new nonlinear cryptanalytic algorithm which overcomes the main issues that prevented the use of nonlinear approximations in previous research, and we present the statistical frameworks for calculating the complexity of each version. We present new attacks on 11-round Serpent with better data complexity than any other known-plaintext or chosen-plaintext attack, and with the best overall time complexity for a 256-bit key.

Category / Keywords: secret-key cryptography / Nonlinear cryptanalysis, generalized linear cryptanalysis, metaheuristics, simulated annealing, multidimensional linear cryptanalysis, Serpent

Date: received 13 Jan 2013

Contact author: jmclaugh at cs york ac uk