Cryptology ePrint Archive: Report 2011/212

Maiorana-McFarland Functions with High Second-Order Nonlinearity

Nicholas Kolokotronis and Konstantinos Limniotis

Abstract: The second-order nonlinearity, and the best quadratic approximations, of Boolean functions are studied in this paper. We prove that cubic functions within the Maiorana-McFarland class achieve very high second order nonlinearity, which is close to an upper bound that was recently proved by Carlet et al., and much higher than the second order nonlinearity obtained by other known constructions. The structure of the cubic Boolean functions considered allows the efficient computation of (a subset of) their best quadratic approximations.

Category / Keywords: secret-key cryptography / boolean functions

Publication Info: An extended version of this work has been submitted to IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible.

Date: received 2 May 2011

Contact author: nkolok at uop gr