Cryptology ePrint Archive: Report 2011/171

On lower bounds on second--order nonliearities of bent functions obtained by using Niho power functions

Manish Garg and Sugata Gangopadhyay

Abstract: In this paper we find a lower bound of the second-order nonlinearities of Boolean bent functions of the form $f(x) = Tr_{1}^{n}(\alpha_{1}x^{d_{1}} + \alpha_{2}x^{d_{2}})$,where d_1 and d_2 are Niho exponents. A lower bound of the second-order nonlinearities of these Boolean functions can also be obtained by using a result proved by Li, Hu and Gao (eprint.iacr.org/2010 /009.pdf). It is demonstrated that for large values of n the lower bound obtained in this paper are better than the lower bound obtained by Li, Hu and Gao.

Category / Keywords: secret-key cryptography /

Date: received 3 Apr 2011, last revised 7 Jul 2011

Contact author: gsugata at gmail com, manishiitr8@gmail com