

Cryptology ePrint Archive: Report 2011/171

On lower bounds on second--order nonlinearities 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 $f(x) = \text{Tr}_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, 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

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: We have revised our paper. We are posting the revised version.

Version: 20110707:071121 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]