

Cryptology ePrint Archive: Report 2011/452

The Good lower bound of Second-order nonlinearity of a class of Boolean function

Manish Garg and Sugata Gangopadhyay

Abstract: In this paper we find the lower bound of second-order nonlinearity of Boolean function $f_{\lambda}(x) = \text{Tr}_{1}^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. It is also demonstrated that the lower bound obtained in this paper is much better than the lower bound obtained by Iwata-Kurosawa [14], and Gangopadhyay et al. (Theorem 1, [12]).

Category / Keywords: Boolean function , Higher-order derivatives, Second-order nonlinearity, Walsh-spectrum

Date: received 18 Aug 2011

Contact author: manishiitr8 at gmail com, manishiitr12@gmail com

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

Version: 20110820:061228 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]