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 $f_{\lambda}(x) = Tr_{1}^{n}(\lambda x^{p})$ 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 \cite{c14}, and Gangopadhyay et al. (Theorem 1, \cite{c12}).

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

Date: received 18 Aug 2011

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