On Second-Order Nonlinearities of Two Classes of Cubic Boolean Functions

Deep Singh and Maheshanand Bhaintwal

Department of Mathematics,
Indian Institute of Technology Roorkee, Roorkee 247667 India
deepsinghspn@gmail.com,mahesfma@iitr.ernet.in

Abstract. The higher order nonlinearity of a Boolean function is a cryptographic criterion, which plays an important role in the design of secure block ciphers and stream ciphers. In this paper, we obtain lower bounds of second-order nonlinearities of two classes of highly nonlinear cubic Boolean functions of the form $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, for $n = 3r$ and $n = 5r$ by investigating the lower bounds of the first order nonlinearity of their derivatives.

Keywords: Boolean functions, Walsh-Hadamard transform, Nonlinearity, Reed-Muller codes.

1 Introduction

The higher order nonlinearity of a Boolean function is a cryptographic criterion, which plays a role against different kinds of attacks, namely: Best Affine Approximation Attacks [9], Higher-order Approximation Attacks [4] etc., on block ciphers and stream ciphers. In addition, it plays a role in coding theory, since it is related to the covering radii of Reed-Muller codes. The rth-order nonlinearity, where $r \geq 1$, of an n-variable Boolean function f , denoted by $nl_r(f)$, is defined as the minimum Hamming distance of f from all n-variable Boolean functions of degrees at most r. The first order nonlinearity (or simply nonlinearity) $nl(f)$ of a Boolean functions on n variables can be computed by using fast Walsh-Hadamard transform in time $o(n2^n)$. Unlike first order nonlinearity, there is no efficient algorithm to compute second-order nonlinearities for $n > 11$. Second-order nonlinearity is known only for some particular functions. Fourquet and Tavernier [5] provided a nice algorithm which works efficiently for $r = 2$ and $n \leq 11$, and in some cases for $n \leq 13$. However, it is in general a difficult problem to obtain an exact lower bound for second order nonlinearities; few attempts have been made in this direction [2,3,10]. Iwata and Kurosawa [10] have given a construction of Boolean functions whose rth-order nonlinearity is lower bounded by

$$nl_r(f) \geq \begin{cases} 2^{n-r-3}(r+4), & \text{if } r = 0\text{mod}2, \\ 2^{n-r-3}(r+5), & \text{if } r = 1\text{mod}2. \end{cases}$$

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 560–567, 2013.

for $0 \leq r \leq n-3$. They have termed the functions satisfying this bound as rth order bent functions. For odd $n \geq 9$, a tight upper bound of nonlinearities of Boolean functions is not known. Therefore, there is a need to construct Boolean functions with controlled nonlinearity profile. The best known asymptotic upper bound on nl_r, obtained by Carlet and Mesnager [3], is

$$nl_r(f) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{\frac{n}{2}} + O(n^{r-2}).$$

Carlet [2] has developed a recursive approach to compute the lower bounds on rth-order nonlinearities of a function f using the $(r-1)$th-order nonlinearities of the derivatives of the f. Recently, Sun and Wu [15] have obtained a lower bound on second order nonlinearities of a class of cubic Boolean functions of the form $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$, where $n = 4r$ and $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$. For more results on lower bounds on second-order nonlinearities of several classes of Boolean functions we refer to [2,6,7,8,11,14,15].

In this paper, we study the lower bounds of second order nonlinearities of two classes of highly nonlinear cubic Boolean functions of the form $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$ for $n = 3r$ and for $n = 5r$. The bounds obtained in this paper are compared with the bounds obtained by Sun and Wu [15] and those in [2,10] and in Theorem 1 of [6].

The remainder of the paper is organized as follows: Section 2 provide preliminary results. Section 3 covers the main results. In Section 4 we compare our results with the existing results. Section 5 concludes the paper.

2 Preliminaries

Boolean functions on n-variables are mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let $\mathcal{B}_n$ denote the set of all Boolean functions on n-variables. The algebraic normal form of $f \in \mathcal{B}_n$ is $f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a(\prod_{i=1}^n x_i^{a_i})$, where $\mu_a \in \mathbb{F}_2$. The algebraic degree $\deg(f)$ of f is defined as $\max\{wt(a) : \mu_a \neq 0, a \in \mathbb{F}_{2^n}\}$. For any two functions $f, g \in \mathcal{B}_n$, $d(f,g) = |\{x : f(x) \neq g(x), x \in \mathbb{F}_{2^n}\}|$ is said to be the Hamming distance between f and g. The *derivative* of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined by $D_a f(x) = f(x) + f(x+a)$.

The trace function $tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by

$$tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined as

$$W_f(\lambda) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+tr_1^n(\lambda x)}.$$

Let $\mathcal{A}_n$ be the set of all affine functions on n variables. The nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l\in\mathcal{A}_n}\{d(f,l)\}$. The nonlinearity of $f \in \mathcal{B}_n$ in terms of Walsh-Hadamard transform is defined as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda\in\mathbb{F}_{2^n}} |W_f(\lambda)|.$$

By using Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} (W_f(\lambda))^2 = 2^{2n},$$

it can be shown that $max\{|W_f(\lambda)| : \lambda \in \mathbb{F}_{2^n}\} \geq 2^{n/2}$, i.e., $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. For n even, $f \in \mathcal{B}_n$ is called a bent [13] function if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Suppose $f \in \mathcal{B}_n$ is a quadratic function and $B(x, y) = f(0) + f(x) + f(y) + f(x + y)$ is the bilinear form associated with f. The kernel $\mathcal{E}_f$ of $B(x, y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

Lemma 1 ([1], Proposition 1). *Let V be a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $P : V \longrightarrow \mathbb{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of P have the same parity.*

Lemma 2 ([1], Lemma 1). *Let f be any quadratic Boolean function. The kernel $\mathcal{E}_f$ is the subspace of $\mathbb{F}_{2^n}$ consisting of those a such that the derivative $D_a f$ is constant. That is,*

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} : D_a f = \text{ constant }\}.$$

If $f \in \mathcal{B}_n$ be a quadratic Boolean function and $B(x, y)$ be the associated bilinear form, then the Walsh spectrum of f depends only on the dimension of the kernel $\mathcal{E}_f$ of $B(x, y)$ [1,12].

Carlet [2] has obtained the following recursive lower bounds on the nonlinearity profile of Boolean functions.

Proposition 1 ([2], Proposition 2). *Let $f \in \mathcal{B}_n$ and r be a positive integer $(r < n)$, then we have*

$$nl_r(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f).$$

Proposition 2 ([2], Proposition 3). *Let $f \in \mathcal{B}_n$ and r be a positive integer $(r < n)$, then we have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)}.$$

Table 1. Weight distribution of the Walsh spectrum of a quadratic function f

$W_f(\alpha)$	number of α
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

The following corollary is due to Proposition 2.

Corollary 1 ([2], Corollary 2). *Let $f \in \mathcal{B}_n$ and r be a positive integer $(r < n)$. Assume that, for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_{2^n}$. Then*

$$nl_r(f) \geq 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n-1)M2^{m+1} + 2^n}.$$

Carlet [2] further remarked that in general the lower bound obtained in Proposition 2 is better than the bound obtained in Proposition 1.

The following result is used to improve the bounds of the rth-order nonlinearities of a Boolean function and known as McEliece's theorem.

Proposition 3 ([12], Chap. 15, Cor. 13). *The rth-order nonlinearities of $f \in \mathcal{B}_n$ with algebraic degree d is divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$.*

3 Main Results

In this section, we deduce the lower bounds of the second order nonlinearity of two classes of cubic Boolean functions by investigating the lower bounds of the first order nonlinearity of their derivatives.

Theorem 1. *Suppose $f \in \mathcal{B}_n$ such that $f(x) = tr(\lambda x^{2^{2r}+2^{r+1}+1})$ $\forall\ x \in \mathbb{F}_{2^n}$, with $n = 3r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}} + 2^n}.$$

Proof. The derivative of $f(x) = tr(\lambda x^{2^{2r}+2^{r+1}+1})$ with $n = 3r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, with respect to $a \in \mathbb{F}_{2^n} \setminus \{0\}$ is

$$\begin{aligned}
D_a f(x) = f(x) + f(x+a) &= tr\left(\lambda (x+a)^{2^{2r}+2^{r+1}+1}\right) + tr(\lambda x^{2^{2r}+2^{r+1}+1}) \\
&= tr\left(\lambda\left(x^{2^{2r}+2^{r+1}} + x^{2^{2r}}a^{2^{r+1}} + x^{2^{r+1}}a^{2^{2r}} + a^{2^{2r}+2^{r+1}}\right)(x+a)\right. \\
&\qquad \left. + \lambda x^{2^{2r}+2^{r+1}+1}\right) \\
&= tr\left(\lambda\left(x^{2^{2r}+2^{r+1}}a + x^{2^{2r}+1}a^{2^{r+1}} + x^{2^{r+1}+1}a^{2^{2r}}\right)\right) + l(x),
\end{aligned}$$

where $l(x)$ is an affine function. Let $b \in \mathbb{F}_{2^n} \setminus \{0\}$ be such that $a \neq b$, then

$$\begin{aligned}
D_b D_a f(x) &= tr\left(\lambda\left((x+b)^{2^{2r}+2^{r+1}}a + (x+b)^{2^{2r}+1}a^{2^{r+1}} + (x+b)^{2^{r+1}+1}a^{2^{2r}}\right)\right) \\
&\quad + tr\left(\lambda(x^{2^{2r}+2^{r+1}}a + x^{2^{2r}+1}a^{2^{r+1}} + x^{2^{r+1}+1}a^{2^{2r}})\right) + constant \\
&= tr\left(x^{2^{2r}}(\lambda b a^{2^{r+1}} + \lambda a b^{2^{r+1}}) + x^{2^{r+1}}(\lambda b a^{2^{2r}} + \lambda a b^{2^{2r}})\right. \\
&\qquad \left. + x(\lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}})\right) + constant
\end{aligned}$$

$$\begin{aligned}
&= tr\left(x\left((\lambda b a^{2^{r+1}} + \lambda a b^{2^{r+1}})^{2^r} + (\lambda b a^{2^{2r}} + \lambda a b^{2^{2r}})^{2^{2r-1}}\right.\right.\\
&\qquad \left.\left.+(\lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}})\right)\right) + constant\\
&= tr\left(x\left(\lambda^{2^r} b^{2^r} a^{2^{2r+1}} + \lambda^{2^r} a^{2^r} b^{2^{2r+1}} + \lambda^{2^{2r-1}} b^{2^{2r-1}} a^{2^{r-1}}\right.\right.\\
&\quad \left.\left.+\lambda^{2^{2r-1}} a^{2^{2r-1}} b^{2^{r-1}} + \lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}}\right)\right) + constant\\
&= tr\left(x P_{\lambda,a}(b)\right) + constant.
\end{aligned}$$

Clearly, $D_b D_a f(x)$ is constant if and only if $P_{\lambda,a}(b) = 0$. Therefore,

$$\mathcal{E}_{D_a f} = \{b \in \mathbb{F}_{2^n} :\ P_{\lambda,a}(b) = 0\}.$$

The kernel $\mathcal{E}_{D_a f}$ of $D_a f$ is the set of zeroes of $P_{\lambda,a}(b)$, or equivalently the set of zeroes of $(P_{\lambda,a}(b))^{2^{2r+1}}$. Therefore,

$$\begin{aligned}
L_{\lambda,a}(b) = (P_{\lambda,a}(b))^{2^{2r+1}} &= \left(\lambda^{2^r} b^{2^r} a^{2^{2r+1}} + \lambda^{2^r} a^{2^r} b^{2^{2r+1}} + \lambda^{2^{2r-1}} b^{2^{2r-1}} a^{2^{r-1}}\right.\\
&\quad \left.+\lambda^{2^{2r-1}} a^{2^{2r-1}} b^{2^{r-1}} + \lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}}\right)^{2^{2r+1}}\\
&= \lambda^2 a^2 b^{2^{r+2}} + \lambda^{2^{2r+1}} a^4 b^{2^{r+1}} + \lambda^{2^r} a b^{2^r}\\
&\quad +\lambda^{2^{2r+1}} a^{2^{r+1}} b^4 + \lambda^2 b^2 a^{2^{r+2}} + \lambda^{2^r} a^{2^r} b.
\end{aligned}$$

Since $L_{\lambda,a}(b)$ is a linearized polynomial in b of degree at most 2^{r+2}. This implies that the dimension k of $\mathcal{E}_{D_a f}$ is at most $r+2$. Thus, for all $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, Walsh-Hadamard transform is

$$W_{D_a f}(\alpha) = 2^{\frac{n+k}{2}} \leq 2^{\frac{n+r+2}{2}}.$$

Since the nonlinearity of the derivative $D_a f$ of $f \in \mathcal{B}_n$ is

$$nl(D_a f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_{D_a f}(\lambda)|,$$

therefore, we have

$$nl(D_a f) \geq 2^{n-1} - 2^{\frac{n+r}{2}}. \tag{1}$$

Using Proposition 1, we have

$$nl_2(f) \geq \frac{1}{2}\left(2^{n-1} - 2^{\frac{n+r}{2}}\right) = 2^{n-2} - 2^{\frac{n+r-2}{2}}. \tag{2}$$

On comparing 1 and Corollary 1, we get $M = 1, m = \frac{n+r}{2}$. Now, using the result of Corollary 1, we get

$$\begin{aligned}
nl_2(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)M 2^{m+1} + 2^n}\\
&= 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{\frac{n+r+2}{2}} + 2^n}.
\end{aligned} \tag{3}$$

On subtracting the lower bound obtained in (2) from the lower bound obtained in (3) and using $n = 3r$, we get

$$2^{n-1} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}} + 2^n} - \tfrac{1}{2}\left(2^{n-1} - 2^{\frac{n+r}{2}}\right)$$
$$= 2^{n-2} + 2^{\frac{4n-6}{6}} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{4n+6}{6}} + 2^n} > 0.$$

for all values of n. Therefore, the bound given in (3) is better than the lower bound obtained in (2). Thus, we have

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}} + 2^n}. \qquad \square$$

In the following result we provide lower bounds on second order nonlinearities of the function $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$ for all $x \in \mathbb{F}_{2^n}$, where $n = 5r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$.

Theorem 2. *Suppose $f \in \mathcal{B}_n$ such that $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$ $\forall$ $x \in \mathbb{F}_{2^n}$, with $n = 5r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+3r+2}{2}} + 2^n}.$$

Proof. The proof is almost similar to the proof of Theorem 1.

Remark 1. The general lower bounds on second order nonlinearities of Boolean functions due to Carlet [2] and Iwata-Kurosawa [10] are $2^{n-1} - 2^{n-\frac{3}{2}}$ and $2^{n-2} - 2^{n-4}$, respectively. Clearly,

$$(2^{n-2} - 2^{n-4}) - (2^{n-1} - 2^{n-\frac{3}{2}}) = 2^{n-4}(4\sqrt{2} - 5) \geq 0.$$

Hence, the bounds obtained by Iwata-Kurosawa [10] are better than Carlet's general bounds [2]. Now, on subtracting Iwata-Kurosawa's bounds from the bounds obtained in Theorem 2 and using $n = 5r$, we have

$$\left(2^{n-1} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{n+3r+2}{2}} + 2^n}\right) - \left(2^{n-2} - 2^{n-4}\right)$$
$$= 5\ 2^{n-4} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{8n+10}{10}} + 2^n} > 0$$

if and only if $n \geq 12$. Therefore, in Theorem 2 we investigate a class of highly nonlinear cubic Boolean functions whose lower bounds of second order nonlinearities (for all $n \geq 12$) are better than the lower bounds obtained by Iwata-Kurosawa [10].

4 Comparison

In Table 2, we present the numerical comparison between the lower bounds obtained in Theorem 1 with the lower bounds those obtained by Iwata-Kurosawa

Table 2. Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 1 using McEliece's Theorem with the bounds obtained in [2,6,10,15]

n	6	9	12	15	18	21	24
Bounds in Theorem 1	10	128	1328	12288	107904	917504	7.647232×10^6
Bounds due to Iwata-Kurosawa [10]	12	96	764	6144	49152	393216	3.145728×10^6
Bounds in [6, Theorem 1]	10	–	1024	–	84732	–	6.291456×10^6
Bounds due to Sun-Wu [15]	–	–	1318	–	–	–	7.339910×10^6
Carlet's general bounds [2]	10	76	600	4800	38392	307122	2.456968×10^6

Table 3. Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 2 using McEliece's Theorem with the bounds obtained in [2,10]

n	15	20	25	30	35
Bounds in Theorem 2	8192	338944	12582912	441965056	$1.5032385536 \times 10^{10}$
Iwata-Kurosawa's bounds [10]	6144	196608	6291456	201326592	6.442450944×10^9
Carlet's general bounds [2]	4800	153562	4913934	157245850	5.031867186×10^9

[10], Gangopadhyay et al. [6], Sun-Wu [15] and the general bounds obtained by Carlet in [2]. It is clear from Table 2 that for $n \geq 9$, the bounds obtained in Theorem 1 are better than the bounds obtained in [2,10,6,15]. Further, it is observed from remark 1 and Table 3 that the bounds obtained in Theorem 2 are larger than the bounds obtained by Iwata-Kurosawa in [10] and Carlet's general bounds in [2].

5 Conclusion

In this paper, we have obtained the lower bounds on second-order nonlinearities of two classes of highly nonlinear cubic Boolean functions. Here it should be noted that, high first order nonlinearity of a Boolean function does not implies the high second order nonlinearity. For example: bent function $tr(x^{2^i+1})$ possess maximum possible first order nonlinearity but their second order nonlinearity is zero. The results in this paper show that the lower bounds of second order nonlinearity of two classes of Boolean functions are also high. In particular, the lower bounds of second order nonlinearities obtained in Theorem 1 for $n \geq 9$ (when $n = 3r$) are better than the lower bounds obtained in [2,6,10,15]. Further, the lower bounds of second order nonlinearities obtained in Theorem 2 for $n \geq 12$ (when $n = 3r$) are better than those of Iwata-Kurosawa [10]. Since higher order nonlinearity of Boolean functions is useful in providing protection against different kinds of attacks on stream and block ciphers therefore, we expect that the results in this paper may be useful in choosing cryptographically significant Boolean functions.

Acknowledgments. The work of the first author is supported by NBHM (DAE), INDIA.

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.M.: A New Class of Monomial Bent Functions. Finite Fields and Appli. 14, 221–241 (2008)
2. Carlet, C.: Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. IEEE Trans. Inform. Theory 54(3), 1262–1272 (2008)
3. Carlet, C., Mesnager, S.: Improving the Upper Bounds on the Covering Radii of Binary Reed-Muller Codes. IEEE Trans. Inform. Theory 53(1), 162–173 (2007)
4. Courtois, N.T.: Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 182–199. Springer, Heidelberg (2003)
5. Fourquet, R., Tavernier, C.: An Improved List Decoding Algorithm for the Second Order Reed-Muller Codes and its Applications. Designs Codes and Crypto. 49, 323–340 (2008)
6. Gangopadhyay, S., Sarkar, S., Telang, R.: On the Lower Bounds of the Second Order Nonlinearities of Some Boolean Functions. Information Sciences 180, 266–273 (2010)
7. Gangopadhyay, S., Singh, B.K.: On Second-Order Nonlinearities of Some Type Bent Functions, `http://eprint.iacr.org/2010/286.pdf`
8. Gode, R., Gangopadhyay, S.: On Lower Bounds of Second-Order Nonlinearities of Cubic Bent Functions Constructed by Concatenating Gold Functions. Int. J. Comput. Math. 88(15), 3125–3135 (2011)
9. Golić, J.: Fast Low Order Approximation of Cryptographic Functions. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 268–282. Springer, Heidelberg (1996)
10. Iwata, T., Kurosawa, K.: Probabilistic Higher Order Differential Attack and Higher Order Bent Functions. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 62–74. Springer, Heidelberg (1999)
11. Kolokotronis, N., Limniotis, K.: Maiorana-McFarland Functions with High Second Order Nonlinearity, `http://eprint.iacr.org/2011/212.pdf`
12. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
13. Rothaus, O.S.: On "Bent" Functions. Journal of Combinatorial Theory, Series A 20, 300–305 (1976)
14. Sun, G., Wu, C.: The Lower Bounds on the Second-Order Nonlinearity of Three Classes of Boolean Functions with High Nonlinearity. Information Sciences 179(3), 267–278 (2009)
15. Sun, G., Wu, C.: The Lower Bounds on the Second-Order Nonlinearity of a Class of Boolean Functions with High Nonlinearity. Appli. Alg. in Eng. Commu. and Comp. 22, 37–45 (2011)