ISSN:0975-9646

Manish Garg / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4251-4256

Higher Order-Nonlinearities on Two Classes of Boolean Functions

Manish Garg

Department of Mathematics
The LNM Institute of Information Technology
Deemed University
Jaipur, Rajasthan-302031, India

***Abstract*— we compute the lower bounds on higher-order nonlinearities of monomial partial-spreads type bent Boolean function $f_\lambda(x)=Tr_1^n(\lambda x^{2^{\frac{n}{2}}-1})$, where $x\in F_{2^n}, \lambda\in F^*_{2^n}$, n is an even positive integer and inverse Boolean function $g_\lambda(x)=Tr_1^n(\lambda x^{2^n-2})$, where $x\in F_{2^n}, \lambda\in F^*_{2^n}$, n is any positive integer. We also show that our lower bounds are better then the Carlet's bounds 2008.**

***Keywords*— Boolean function, Derivatives, Higher-order nonlinearity, Walsh-spectrum**

INTRODUCTION

Suppose F_2 is a prime field consisting two element *0* and *1*. The field F_{2^n} is an extension field over F_2 of degree *n*. F_{2^n} is vector space isomorphic to F_2^n which is an n-dimensional vector space over F_2. Therefore, F_2^n can be viewed as F_{2^n}. Boolean function on n-variable is a mapping from F_2^n to F_2. B_n denotes the collection of all n-variable Boolean functions. The number of one's in $x=(x_1,x_2,...,x_n)\in F_2^n$ is called the Hamming weight and denoted as $wt(x)=\sum_{i=1}^{n} x_i$. Boolean function $f\in B_n$ can be written in the following Algebraic Normal Form

$$f(x)=\bigoplus_{a=(a_1,...,a_n)\in F_2^n}\mu_a\Big(\prod_{i=1}^{n}x_i^{a_i}\Big),$$

where $\mu\in F_2$. The algebraic degree of *f* denoted as *deg(f)*, is the maximum number of one's in the binary expansion of *a* such that $\mu_a\neq 0$. The Hamming distance between two Boolean functions is the number of places where functional value of functions does not match. Boolean function of algebraic degree one or less is said to be affine.

Definition 1: Suppose $f\in B_n$. For every integer $0<r\le n$, the minimum value of the Hamming distance of *f* from all *n* variable Boolean functions of degree at most *r* $(r\ge 1)$ is called the *r*th-order nonlinearity of *f and denoted by* $nl_r(f)$. The sequence of values $nl_r(f)$, *f*or *r* ranging from *1* to *n-1*, is said to be nonlinearity profile of Boolean function *f*.

The nonlinearities of Boolean functions is an important aspect in the security of the stream ciphers as well as block ciphers. In symmetric ciphers, Matsui [24] found the relationship between explicit attack and nonlinearity. The best asymptotic known upper bound [6] on $nl_r(f)$ is given as

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

Kavatiansky and Tavernier [9, 18] proposed an algorithm to compute the second-order nonlinearities by using list decoding algorithms for higher-order Reed-Muller codes. Later it was improved and implemented by Forquet and Tavernier [10]. This algorithm works efficiently for $n\le 11$ and for $n\le 13$ for some particular functions. No efficient algorithm is proposed to compute the *r*th-order $(r>2)$ nonlinearity of Boolean functions. Although, some theoretical results on the lower bound of higher order nonlinearity are known. Garg and Khalyavin [14] have found the higher-order nonlinearities of Kasami function. The third-order nonlinearities for a subclass of Kasami functions was found in [15]. For more results in this direction we refer to [11, 12, 13, 14, 20, 27, 28, 29]. Carlet [4] provides a technique of computing lower bounds of higher-order nonlinearities of Boolean functions recursively. In this paper, we use technique developed by carlet [4] to compute the lower bounds on higher-order nonlinearities of monomial partial-spreads function $f_\lambda(x)=Tr_1^n(\lambda x^{2^{\frac{n}{2}}-1})$, where $x\in F_{2^n}, \lambda\in F^*_{2^n}$, n is an even positive integer and inverse Boolean function $g_\lambda(x)=Tr_1^n(\lambda x^{2^n-2})$, where $x\in F_{2^n}, \lambda\in F^*_{2^n}$, n is any positive integer. We also show that our lower bounds are better than the Carlet's bounds 2008.

PRELIMINARIES

Definition 2: The Walsh transform of $f \in B_n$ at $\lambda \in F_2^n$ is defined as

$$W_f(\lambda) = \sum_{x \in F_2^n} (-1)^{f(x)+\lambda \cdot x}$$

The multiset $[W_f(\lambda) : \lambda \in F_2^n]$ is called the Walsh spectrum of *f*. The nonlinearity in terms of Walsh spectrum is defined as follows

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in F_2^n} |W_f(\lambda)|.$$

Definition 3: The derivative of $f \in B_n$ with respect to $\alpha \in F_{2^n}$ is a Boolean function and defined as

$$D_\alpha(x) = f(x+\alpha) + f(x) \text{ for all } x \in F_{2^n}.$$

Definition 4: Suppose $a_1, a_2, ..., a_l$ is a basis of *l*-dimensional subspace *V* of F_{2^n}. The *l*th derivative of *f* with respect to *V* is a Boolean function defined as

$$D_V f(x) = D_{a_l} D_{a_{l-1}} ... D_{a_1} f(x) \text{ for all } x \in F_{2^n}.$$

The *l*th derivative of f is independent of the choice of the basis of *V*. The trace function is a mapping from F_{2^n} into F_2 and defined as

$$Tr_1^n(u) = u + u^2 + u^{2^2} + ... + u^{2^{n-1}}, \text{ for all } u \in F_{2^n}.$$

For given any $u, v \in F_{2^n}$, $Tr_1^n(uv)$ is called an inner product between *u* and *v*. The general linear group $GL(m, F_2)$ is the collection of all $m \times m$ non-singular matrix with entries either *0* or *1*. In other words, this is the collection of all invertible linear transformations on F_2^n. A positive integer *t* can be represented in its binary expansion as $\sum_{i=0}^{l} t_i 2^i$. We define a partial order denoted by $\preceq$ between any two positive integers as follows: t and t' satisfy $t \preceq t'$ if and only if $t_i \le t_i'$ for all *i*. If $t \preceq t'$ but $t \ne t'$, then it is denoted by $t \prec t'$.

Definition 5: Boolean function $f \in B_n$ is called affine equivalent to $h \in B_n$ iff there exists $M \in GL(n, F_2)$, , $c, \mu \in F_2^n, \theta \in F_2$ such that $h(x) = f(Mx + c) + \mu \cdot x + \theta$ for all $x \in F_{2^n}$, where $\mu \cdot x$ denotes an inner product of μ and x.

Lemma 1. ([1], Propoition1): Suppose *U* is a vector space over a field F_q of characteristic *2* and $R: U \to F_q$ *be a quadratic* form. Then the dimension of *U* and the dimension of the kernel of *R* have the same parity.

The Walsh spectrum of a quadratic Boolean function (algebraic degree at most *2*) is completely characterized by the dimension of the kernel of the bilinear form associated to it. For more description, we refer to [1, 23]. The bilinear form associated with a quadratic Boolean function *f* on *n*-variables is defined as $B(u,v) = f(0) + f(u) + f(v) + f(u+v)$ The kernel [1, 23] of $B(u,v)$ is the subspace of F_{2^n} defined by

$$\varepsilon_f = \{u \in F_{2^n} : B(u,v) = 0, \text{ for all } v \in F_{2^n}\}.$$

Definition 6: ([21], Page 99): A polynomial of the form $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ is called a Linearized polynomial (*q*-polynomial) over F_{q^n} where the coefficients α_i belongs to an extension field F_{q^n} of F_q.

Carlet [4] proved the following useful result.

Proposition 1. ([4], Proposition 2) Suppose *f* is a *n*-variable Boolean function and *r* is a positive integer less than *n*, we have

$$nl_r(f) \ge \frac{1}{2} \max_{a \in F_{2^n}} nl_{r-1}(D_a(f))$$

in terms of higher-order derivatives

$$nl_r(f) \ge \frac{1}{2^i} \max_{a_1, a_2, ..., a_i \in F_{2^n}} nl_{r-1}(D_{a_1} D_{a_2} ... D_{a_i}(f)).$$

Lemma2. [1 23] Let $B(u,v)$ be a bilinear form associated to a quadratic Boolean function $f : F_{2^n} \to F_2$. Then the Walsh spectrum of *f* depends only on the dimension, k, of the kernel, ε_f of $B(u,v)$. The weight distribution of the Walsh spectrum of f is:

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

We denote a condition $[k, c_1, .., c_m]$ such that

1. $\sum_{i=0}^{n} c_i = k$
2. $c_i > 0$ for all $i = i, ..., m.$
3. $c_i \wedge c_j = 0$ for all $1 \le i < j \le m$ where $\wedge$ means bitwise AND operations.

This condition means that non-zero bits from binary representation of *k* are split to *n* non-empty non-intersecting groups.

Lemma 3. [14] For all $t > 0$ and $k > 0$

$$D_{a_1} D_{a_2} \ldots D_{a_t}(x^k) = \sum_{[k,\alpha_o,\alpha_1,\ldots,\alpha_t]} x^{\alpha_0} a_1^{\alpha_1} \ldots a_t^{\alpha_t} + \sum_{\gamma \in v_t} \gamma^k,$$

where V_t is the subspace spanned by $a_1, \ldots, a_t$.

MAIN RESULTS

Theorem1. Let $f_\lambda(x) = Tr_1^n(\lambda x^{2^{\frac{n}{2}-1}})$, where $x \in F_{2^n}, \lambda \in F_{2^n}^*$. Then

$$nl_{(r=(\frac{n}{2}-1))}(f_\lambda(x)) = 2^{\frac{n}{2}}.$$

Proof: Let b be any positive integer. We know that $2^b - 1 = 2^{b-1} + 2^{b-2} + \ldots + 2 + 1$. Therefore there are b ones in the binary form of $(2^b - 1)$. Let $p = 2^{\frac{n}{2}} - 1$. So the algebraic degree of $f_\lambda(x)$ is $\frac{n}{2}$. By Proposition 1, we get

$$nl_{(r=(\frac{n}{2}-1))}(f_\lambda(x)) \geq \frac{1}{2^{(\frac{n}{2}-2)}} \max_{a_1,\ldots,a_{(\frac{n}{2}-2)} \in F_{2^n}} (G(x)),$$

(1.0)

where

$$G(x) = nl(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}}(f_\lambda(x)).$$

By Lemma 3,

$$(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}}(f_\lambda(x)) \geq Tr_1^n(H(x)),$$

Where

$$H(x) = \sum_{\left[p,\alpha_o,\alpha_1,\ldots,\alpha_{(\frac{n}{2}-2)}\right]} x^{\alpha_0} a_1^{\alpha_1} \ldots a_{(\frac{n}{2}-2)}^{\alpha_{(\frac{n}{2}-2)}} + \sum_{\gamma \in v_{(\frac{n}{2}-2)}} \gamma^p,$$

Clearly $p = 2^{\frac{n}{2}} - 1$ has $\frac{n}{2}$ ones in its binary form and each $\alpha_i > 0$ for all i . Therefore each α_i must have at least *1* one in its binary form. Therefore α_0 must have at most *2*ones in binary form. If the above Boolean function is quadratic. Then the nonlinearity of $(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}}(f_\lambda(x))$ is equivalent to the nonlinearity of $h_\lambda(x)$. where $h_\lambda(x)$ can be obtained by omitting constant and all the terms of $wt(\alpha_0) = 1$ in the sum. The bilinear form $B(x, y)$ associated with $h_\lambda(x)$ is given as

$$B(x, y) = h_\lambda(0) + h_\lambda(x) + h_\lambda(y) + h_\lambda(x + y).$$

Then we will have

$$B(x, y) = Tr_1^n\left(\sum_{i=1}^{\frac{n}{2}} y^{\beta_i}\left(\sum_{\left[p,\alpha,\beta_i,\alpha_1,\ldots,\alpha_{(\frac{n}{2}-2)}\right]} \lambda x^{\alpha_0} a_1^{\alpha_1} \ldots a_{(\frac{n}{2}-2)}^{\alpha_{(\frac{n}{2}-2)}}\right)\right),$$

$$B(x, y) = Tr_1^n\left(\sum_{i=1}^{\frac{n}{2}} y^{\beta_i} P_i(x)\right),$$

$$P_i(x) = \left(\sum_{\left[p,\alpha,\beta_i,\alpha_1,\ldots,\alpha_{(\frac{n}{2}-2)}\right]} \lambda x^{\alpha_0} a_1^{\alpha_1} \ldots a_{(\frac{n}{2}-2)}^{\alpha_{(\frac{n}{2}-2)}}\right)$$

Due to the linear property of trace function, it can be written as

$$B(x, y) = \sum_{i=1}^{\frac{n}{2}} Tr_1^n(y^{\beta_i} P_i(x))$$

all $\alpha, \beta_i, \alpha_1, \ldots, \alpha_{(\frac{n}{2}-2)}$ are equal to the some power of *2*. Using properties $x^{2^n} = x$ for all $x \in F_{2^n}$, $Tr_1^n(x) = Tr_1^n(x^2)$ and square each term $\log_2 2^n / \beta_i$ times.

We get

$$B(x, y) = Tr_1^n(y \sum_{i=1}^{\frac{n}{2}} (P_i(x)^{2^n/\beta_i}),$$

$$B(x, y) = Tr_1^n(y(P(x)))$$

where

$$P(x) = \sum_{i=1}^{\frac{n}{2}} (P_i(x)^{2^n/\beta_i}.$$

The kernel of $B(x, y)$ is $\varepsilon_f = \{x \in F_{2^n} : P(x) = 0\}$. The number of elements in the kernel ε_f is equal to the number of zeros of $P(x)$, equivalently, the number of zeros of $P(x)^{2^{\frac{n}{2}-1}}$ which equals to

$$\sum_{i=1}^{\frac{n}{2}}\left(\sum_{\left[p,\alpha,\beta_i,\alpha_1,\ldots,\alpha_{(\frac{n}{2}-2)}\right]} (K(x))\right),$$

where

$$k(x) = \lambda^{\frac{2^{2^{(\frac{n}{2}-1)}}}{\beta_i}} x^{\frac{2^{2^{(\frac{n}{2}-1)}}\alpha}{\beta_i}} a_1^{\frac{2^{2^{(\frac{n}{2}-1)}}\alpha}{\beta_i}} \ldots a_{(\frac{n}{2}-2)}^{\frac{2^{2^{(\frac{n}{2}-1)}}\alpha}{\beta_i}}.$$

This is a linearized polynomial in x. So by Lemma 1, $k \le (n-2)$, since n is even. Therefore, for all $x \in F_{2^n}$, we have

$$W_{(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}})}(f_\lambda(x)) \le 2^{\frac{n+k}{2}}$$

$$W_{(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}})}(f_\lambda(x)) \le 2^{n-1}$$

$$nl_{(D_{a_1} D_{a_2} \ldots D_{a_{(\frac{n}{2}-2)}})}(f_\lambda(x)) \ge 2^{n-1} - 2^{n-2} = 2^{n-2}.$$

Hence by equation 1.0

$$nl_{(r=(\frac{n}{2}-1))}(f_\lambda(x)) = 2^{\frac{n}{2}}.$$

Theorem2. Consider the Boolean function

$$g_\lambda(x) = Tr_1^n(\lambda x^{2^n-2}),$$

where $x \in F_{2^n}$, $\lambda \in F_{2^n}^*$, n is any positive integer. Then

$$nl_{(r=(n-2))}(g_\lambda(x)) \ge 2.$$

Proof: We know that $2^n - 2 = 2^{n-1} + 2^{n-2} + \ldots + 2^2 + 2$. Therefore, $wt(2^n-2) = n-1$. Let $p' = 2^n - 2$. So the algebraic degree of $g_\lambda(x)$ is $n-1$. By Proposition 1, we have

$$nl_{(r=(n-2))}(g_\lambda(x)) \ge \frac{1}{2^{(n-3)}} \max_{a_1,\ldots,a_{(n-3)} \in F_{2^n}} (G_1(x)),$$

where

$$G_1(x) = nl(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}}(g_\lambda(x))).$$

By Lemma 3

$$(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}}(g_\lambda(x)) \ge Tr_1^n(H_1(x)),$$

where

$$H_1(x) = \sum_{[p', \alpha_o, \alpha_1, \ldots, \alpha_{(n-3)}]} x^{\alpha_0} a_1^{\alpha_1} \ldots a_{(n-3)}^{\alpha_{(n-3)}} + \sum_{\gamma \in v_{(n-3)}} \gamma^{p'}.$$

Each α_i must have at least *1* one in its binary form because $p' = 2^n - 2$ has $n-1$ ones in its binary form and each $\alpha_i > 0$ for all i. Therefore α_0 must have at most *2* ones in binary form. If the above Boolean function is quadratic. Then the nonlinearity of $nl(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}}(g_\lambda(x))$ is equivalent to the nonlinearity of $h'_\lambda(x)$ where $h'_\lambda(x)$ can be obtained by omitting constant and all the terms of $wt(\alpha_0) = 1$ in the sum. The bilinear form $B(x,y)$ associated with $h'_\lambda(x)$

$$B(x,y) = h'_\lambda(0) + h'_\lambda(x) + h'_\lambda(y) + h'_\lambda(x+y).$$

Then we get

$$B(x,y) = \sum_{j=1}^{n-1} Tr_1^n(y^{\gamma_j} Q_j(x)),$$

where

$$Q_j(x) = \left(\sum_{[p', \alpha, \gamma_i, \alpha_1, \ldots, \alpha_{(n-3)}]} \lambda x^{\alpha_0} a_1^{\alpha_1} \ldots a_{(n-3)}^{\alpha_{(n-3)}} \right)$$

where all $\alpha, \gamma_j, \alpha_1, \ldots, \alpha_{(n-3)}$ are equal to the some power of *2*. Using properties $x^{2^n} = x$ for all $x \in F_{2^n}$, $Tr_1^n(x) = Tr_1^n(x^2)$ and square each term $\log_2 2^n / \gamma_j$ times. We will have

$$B(x,y) = Tr_1^n(y(Q(x))),$$

where

$$Q(x) = \sum_{j=1}^{n-1} (Q_j(x)^{2^n/\beta_j}.$$

The kernel of $B(x,y)$ is $\varepsilon_g = \{x \in F_{2^n} : Q(x) = 0\}$. The number of elements in the kernel ε_g is equal to the number of zeros of $Q(x)$, equivalently, the number of zeros of $Q(x)^{2^n-1}$. The minimum degree of x in the expression of $Q(x)^{2^n-1}$ is 2. Therefore number of zeros of $Q(x)$ is equal to the number of zeros of $Q(x)^{\frac{1}{2}}$. Let it be denoted by $L'(x)$

$$L'(x) = \sum_{j=1}^{n-1} \left(\sum_{[p', \alpha, \gamma_j, \alpha_1, \ldots, \alpha_{(n-3)}]} (K_1(x)) \right),$$

where

$$k(x) = \lambda^{\left(\frac{2^{(n-1)}}{\gamma_i} - 1\right)} x^{\alpha\left(\frac{2^{(n-1)}}{\gamma_i} - 1\right)} a_1^{\alpha_1\left(\frac{2^{(n-1)}}{\gamma_i} - 1\right)} \ldots a_{(n-3)}^{\alpha_{(n-3)}\left(\frac{2^{(n-1)}}{\gamma_i} - 1\right)}.$$

Clearly, $L'(x)$ is a linearized polynomial in x. The degree of $L'(x)$ will be at most degree 2^{n-1}. Hence by Lemma 1, $k \le (n-2)$, for n is any integer (even or odd). Therefore, for all $x \in F_{2^n}$, we have

$$W_{(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}})}(g_\lambda(x)) \le 2^{\frac{n+k}{2}}$$

$$W_{(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}})}(g_\lambda(x)) \le 2^{n-1}$$

$$nl_{(D_{a_1} D_{a_2} \ldots D_{a_{(n-3)}})}(g_\lambda(x)) \ge 2^{n-1} - 2^{n-2} = 2^{n-2}.$$

Hence by equation 2.0

$$nl_{(r=(n-2))}(g_\lambda(x)) \ge 2.$$

Remark 1. [5, 6] It is to be noted that Boolean function $f_\lambda(x,y) = Tr_1^n(\lambda x y^{2^n-2})$, where $x, y \in F_{2^n}$, $\lambda \in F_{2^n}^*$ and n is an even positive integer is affine equivalent to $f(x,y) = Tr_1^n(xy^{2^n-2})$, for all $\lambda \in F_{2^n}^*$ $x, y \in F_{2^n}$. Similarly Boolean function $g_\lambda(x) = Tr_1^n(\lambda x^{2^n-2})$, where $x \in F_{2^n}$, $\lambda \in F_{2^n}^*$, n is any positive integer is affine equivalent to $g(x) = Tr_1^n(x^{2^n-2})$, for all $\lambda \in F_{2^n}$. Therefore, the lower bounds of nonlinearities of $f_\lambda(x,y)$ and $g_\lambda(x)$ are same as the lower bounds of nonlinearities $f(x,y)$ and $g(x)$ respectively.

COMPARISON

It is proved in [5] that the higher-order nonlinearity of Dillon bent function $f_\lambda(x,y) = Tr_1^n(\lambda x y^{2^n-2})$, where $\lambda \in F_{2^n}^*$ and n is an even positive integer, is

$$nl_r(f_\lambda(x,y)) = 2^{n-1} - l_r.$$

Where

$$l_1 = 2^{\frac{n}{2}-1},$$

$$l_2 = 2^{\frac{3n}{4}},$$

$$l_r = 2^{\frac{n}{2}}\sqrt{l_{r-1}}.$$

It is also proved in [4] that the higher-order nonlinearity of Inverse Boolean Function $g_\lambda(x) = Tr_1^n(\lambda x^{2^n-2})$, where $\lambda \in F_{2^n}^*$, n is any positive integer, is

$$nl_r(g_\lambda(x)) = 2^{n-1} - s_r.$$

Where

$$s_1 = 2^{\frac{n}{2}},$$

$$s_r = \sqrt{(2^n-1)(s_{r-1}+1) + 2^{n-2}}.$$

We give the lower bound of Dillon bent function obtained in [5] and the lower bound monomial partial-spreads function obtained in 1 in Table 1.

r, n	3, 8	4, 10	5, 12	6, 14	7, 16	8, 18	9, 20	10, 22
Lower Bound obtained in [5]	0	0	0	0	0	0	0	0
Lower bound obtained in Theorem 1	16	32	64	128	256	512	1024	2048

Table1. Comparison of the Lower bounds of higher-order nonlinearities .

In the case of inverse Boolean function, the lower bound of $r = (n-2)$ th-order nonlinearity on n-variables obtained by Carlet [4] are trivial (negative) while we find the lower bounds of $r = (n-2)$ th-order nonlinearity on n-variables is 2, where (n = 4, 5, 6, 7, ...). Therefore, it shows that our obtained lower bounds are better than the Carlet's bounds [4, 5].

CONCLUSION

In this paper we compute the lower bounds of higher order nonlinearity of monomial partial-spreads type Boolean function and inverse Boolean Function. In both cases, the lower bounds obtained by Carlet's bounds [4, 5] in both cases are trivial. Our lower bounds obtained in Theorem 1 and Theorem 2 are better then Carlet's bounds.

REFERENCES

[1] A. Canteaut, P. Charpin and G. M. Kyureghyan, “A new class of monomial bent functions,” *Finite Fields and their Applications*. Vol. 14, pp. 221-241, 2008.

[2] C. Carlet, “Boolean Functions for Cryptography and Error Correcting Codes,” *in Boolean Methods and Models. Y. Crama and P. Hammer, Eds.* Cambridge, U.K. : Cambridge Univ. Press [Online]. Avsilsble : //www-rocq.inria.fr/codes/Claude.Carlet/pubs.html 1to be published.

[3] C. Carlet, “Vectorial (Multi-Output) Boolean Functions for Cryptography, in Boolean Methods and Models,” *Y. Crama and P. Hammer, Eds.* Cambridge, U.K. : Cambridge Univ. Press [Online]. Avsilsble : //www-rocq.inria.fr/codes/Claude.Carlet/pubs.htm to be published.

[4] C. Carlet, “Recursive lower bounds on the nonlinearity profile of Boolean functions and their Applications,” *IEEE Trans. Inf. Theory*, 54(3), pp. 1262-1272, 2008.

[5] C. Carlet, “On the nonlinearity profile of the Dillon function,” *http:// eprint.iacr.org/2009/577.pdf.* 2002.

[6] C. Carlet and S. Mesnager, “Improving the upper bounds on the covering radii of binary Reed–Muller codes,” *IEEE Trans. Inf. Theory*, Vol.53, no. 1, pp.162—173, 2007.

[7] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, “Covering Codes,” Amsterdam, The Netherlands: North-Holland, 1997.

[8] N. Courtois, “Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt,” *In Proc. ICISC 2002 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer-Verlag, Vol. 2587, pp. 182-199 , 2002.

[9] I. Dumer, G. Kabatiansky and C. Tavernier, “ List decoding of second order Reed-Muller codes up to the johnson bound with almost linear complexity,” *In: Proceedings of the IEEE International Symposium on Information Theory*, Seattle, WA 2006, pp. 138-142, 2006.

[10] R. Fourquet and C. Tavernier, "An improved list decoding algorithm for the second-order Reed-Muller codes and its applications," *Designs Codes Cryptogr.*," Vol, 49, pp. 323-340, 2008.

[11] S. Gangopadhyay, S. Sarkar and R. Telang, "On the lower bounds of the second-order nonlinearity of some Boolean functions," *Inf. Sci*. 180(2), pp. 266-273 , 2010.

[12] M. Garg,, "Good second-order nonlinearity of a subclass of Kasami function on five, seven and nine variables," *In proceeding of IEEE, International Conference on Communication Systems and Network Technologies* (CSNT-2011), 3rd to 5th June, 2011, SMVDU, Katra, Jammu(India), pp. 624-628, 2011.

[13] M. Garg and S. Gangopadhyay, "A lower bound of the second-order nonlinearities of Boolean bent functions," *Fundamenta Informaticae, European Association for Theoretical Computer Science* (EATCS), Vol. 111(4), pp. 413-422, 2011.

[14] M. Garg, and A. Khalyavin, "Higher order-nonlinearity of Kasami function," *International Journal of Computer Mathematics*, Taylor Francis, Vol. 89, No. 10. pp. 1311-1318, 2012.

[15] R. Gode and S. Gangopadhyay, "Third-order nonlinearities of a subclass of kasami functions," *Cryptography. Commun,* Vol. 2, pp. 69-83, 2010.

[16] J. Golic, "Fast low order approximation of cryptographic functions," *In Proc. EUROCRYPT'96 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer-Verlag, Vol.1070, pp. 268-282, 1996.

[17] T. Iwata and K. Kurosawa, "Probabilistic higher order differential attack and higher-order bent functions," *In Proc. ASIACRYPT'99 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer,-Verlag, Vol.1716, pp. 62-74, 1999.

[18] G. Kabatiansky and C. Tavernier, "List decoding of second order Reed-Muller codes," *In : Proceedings of the Eighteen International Symposium of Communication Theory and Applications*, Ambleside, UK, 2005.

[19] L. R. Knudsen and M. J. B. Robshaw, "Non-linear approximations in linear cryptanalysis. *In Proc. EUROCRYPT'96 (Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, Vol.1070, pp. 224-236, 1996.

[20] X. Li, Y. Hu and J. Gao, "Lower Bounds on the Second Order nonlinearity of Boolean Functions," *Int. J. Found. Comput. Sci*. 22(6), pp. 1331-1349 , 2011.

[21] R. Lidl and H. Niederreiter, "Title of a Book, Introduction to finite fields and their applications," North-Holland, Amsterdam, , 1994.

[22] E. Lucas,"Thorie des functions numriques simplement priodiques," *Amer. J. Math., 1*, pp. 184-240, pp. 289-321 , 1878.

[23] F. J. Macwilliams and N. J. Solane, "Title of a Book, The theory of Error-correcting Codes," Amsterdam: North-holland publishing Company, 1978.

[24] M. Matsui, "Linear cryptanalysis method for DES cipher," *In: Proceeding of the EUROCRYPT'93, LNCS,* Vol. 765, pp. 386-397, 1994.

[25] U. M. Maurer, "New approaches to the design of self-synchronizing stream ciphers," *In Proc. EUROCRYPT'91 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer-Verlag, Vol.547, pp. 458-471, 1991.

[26] W. Millan, "Low order approximation of cipher functions. In Cryptographic Policy and Algorithms," *(Lecture notes in Computer Science.* Berlin, Germany: Springer-Verlag, Vol.1029, pp. 144-155, 1996.

[27] D. Singh, "Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions," *Int. J. of Comput. Sci. Inform. Technol*, Vol. 2(2), pp. 786-791, 2011.

[28] G. Sun and C. Wu, "The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity.," *Information Sciences,* 179 (3), pp. 267-278 , 2009.

[29] G. Sun and C. Wu, "The lower bound on the second-order nonlinearity of a class of Boolean function with high nonlinearity," *Appl. Algebra Engrg. Comm. Comput.* (AAECC), Vol. 22, pp. 37-45, 2011.