ISSN:0975-9646

Manish Garg / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (2) , 2016, 715-720

The second-order nonlinearity of a class of Boolean functions

Manish Garg

Department of Mathematics
The LNM Institute of Information Technology
Deemed University
Jaipur, Rajasthan-302031, India
manishiitr8@gmail.com

***Abstract*— In this paper we find a lower bound of second-order nonlinearity of Boolean function $f_\lambda(x)=Tr_1^n(\lambda x^p)$, where $p=2^{2r}+2^r+1$, $\lambda\in F_{2^r}^*$, 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 [17] and Gangopadhyay, Sarkar and Telang (Theorem 1, [12]).**

***Keywords*— Boolean function, Second-order nonlinearity, Derivatives**

INTRODUCTION

Let F_2 be the prime field of characteristic *2*. Let F_2^n be an *n*-dimensional vector space over F_2. The finite field F_{2^n} is also an *n*-dimensional vector space over F_2. Let $\{b_1,...,b_n\}$ be a basis of F_{2^n} over F_2. Thus, for any $x\in F_{2^n}$ there exists a vector $\{x_1,...,x_n\}\in F_2^n$ such that $x=x_1b_1+...+x_nb_n$. This establishes a natural F_2-vector space isomorphism between F_{2^n} and F_2^n, both considered as vector spaces over the prime field F_2. We shall frequently identify $x\in F_{2^n}$ with the vector $\{x_1,...,x_n\}\in F_2^n$ assuming a fixed basis $\{b_1,...,b_n\}$. Therefore, F_2^n can be viewed as F_{2^n}. Boolean function on n-variables is a mapping from F_2^n to F_2 (equivalently from F_{2^n} to F_2). The set of all Boolean functions on n-variables is denoted B_n. The Hamming weight number of $x=(x_1,x_2,...,x_n)\in F_2^n$ is defined as $wt(x)=\sum_{i=1}^n x_i$. The Hamming distance between two Boolean functions *f* and *g* is defined as $d(f,g)=\left|\{x\in F_{2^n}: f(x)\neq g(x)\}\right|$, where the cardinality of a set S is denoted by $|s|$. The Algebraic Normal Form (ANF) of a Boolean function $f\in B_n$ is defined as

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

where $\mu_a\in F_2$ for all $a\in F_2^n$. The maximum value of $wt(a)$ such that $\mu_a\neq 0$ is called the algebraic degree of f denoted by $\deg(f)$. The *r*th-order Reed-Muller code $R(r,n)$ of length 2^n and of order *r* is the set of all Boolean functions on *n*-variables with algebraic degree at most *r*.

Definition 1: The nonlinearity of Boolean function $f\in F_2^n$ is defined as the minimum Hamming distance of f from all affine Boolean functions (affine Boolean functions are those Boolean functions whose algebraic degree is at most 1). More over

$$nl(f)=\min\{d_H(f,l)\,|\,l\in A_n\},$$

where A_n is the set of all affine Boolean function on n-variables.

Definition 2: Let $f\in B_n$. For every non-negative integer $0<r\leq n$, the *r*th-order nonlinearity of *f* is the minimum Hamming distance of *f* from all *n*-variable Boolean functions of degree at most *r* $(r\geq 1)$ *and denoted by* $nl_r(f)$. In other words, the *r*th-order nonlinearity of f is equal to the minimum Hamming distance of f from the *r*th-order Reed--Muller code $R(r,n)$ of length 2^n and of order *r*. 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*.

When Boolean functions are used in stream or block ciphers their nonlinearities play an important role with respect to the security of the considered ciphers. The relationship between explicit attack and nonlinearity on symmetric ciphers was found by Matsui [22]. The best known upper bound [5] on $nl_r(f)$ has following asymptotic version

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

There is a lot of research on first-order nonlinearity. Unlike nonlinearity very little is known about higher-order nonlinearity. There are no efficient algorithm to compute the rth-order nonlinearity of Boolean function f for $(r \geq 1)$. However, in [10, 11, 18] list decoding algorithms for higher order Reed-Muller codes are used to compute second-order nonlinearities. Carlet [3] provides a technique of computing lower bounds of higher-order nonlinearities recursively. In the same paper Carlet provides general lower bounds on the nonlinearity profiles of Boolean functions belonging to several important classes including Welch, Kasami and multiplicative inverse functions. Gangopadhyay, Sarkar and Telang [12] have found the second order-nonlinearity of $f_\lambda(x) = Tr_1^n(\lambda x^p)$, where $p = 2^{2r} + 2^r + 1$, $\lambda \in F_{2^n}^*$, and $n = 6r$. Sun and Wu [29], Deep Singh [27] have found the second order-nonlinearity of $f_\lambda(x) = Tr_1^n(\lambda x^p)$, where $p = 2^{2r} + 2^r + 1$, $\lambda \in F_{2^r}^*$, and $n = 4r$ and $n = 3r$ respectively. For more results in this direction we refer to [13-15, 20, 28]

The lower bound of rth-order nonlinearity of Boolean function f from a given algebraic immunity has been studied in [4]. It was improved in [2]. It gives better results than the results obtained by Iwata-Kurosawa [17]. In this paper we use the technique developed by Carlet to find out the lower bound of second-order nonlinearities of Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$, where $p = 2^{2r} + 2^r + 1$, $\lambda \in F_{2^r}^*$, and $n = 5r$. It is also found that the lower bound obtained in this paper is much better than the lower bound obtained by Iwata-Kurosawa [17], and Gangopadhyay, Sarkar and Telang [12].

.

PRELIMINARIES

Definition 3: 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 the Boolean function f. The relation between nonlinearity and Walsh spectrum is given as follows

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

Using Parseval's equality it can be proved that for any positive integer n, their exist a $\lambda \in F_2^n$ such that $W_f(\lambda) = \geq 2^{\frac{n}{2}}$, which implies $nl(f) = 2^{n-1} - 2^{\left(\frac{n}{2}-1\right)}$.

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

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

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

$$D_{V_k} f(x) = D_{a_k} D_{a_{k-1}} ... D_{a_1} f(x) \text{ for all } x \in F_{2^n}.$$

The kth derivative of f is independent of the choice of the basis of V_k.

Remark 1: It is to be noted that the $D_{V_k}(f)$ is independent of the choice of the basis of V_k.

The trace function from $L = F_{2^n}$ into $S = F_{2^c}$ (where $c \mid n$) is defined as

$$Tr_S^L(x) = \sum_{i=0}^{\frac{n}{c}-1} x^{2^{ci}}, \text{ for all } x \in F_{2^n}.$$

If $c = 1$, we called absolute trace function and denoted as $Tr_1^n(x)$ or $Tr(x)$. $Tr_1^n(xy)$ is called an inner product of x and y for any $x, y \in F_{2^n}$. The trace function Tr_S^L satisfies the following properties [21].

1. $Tr_S^L(\alpha x + \beta y) = \alpha Tr_S^L(x) + \beta Tr_S^L(y)$ for all $\alpha, \beta \in S$ and $x, y \in L$.
2. $Tr_S^L(x^s) = Tr_S^L(x)$ for all $x \in L$ and $s = 2^c$.
3. (Transitivity property) Let R be a finite field. Let F be a finite extension of R and L be a finite extension of F, that is $L \supset F \supset R$. Then

$$Tr_R^L(x) = Tr_R^F\left(Tr_F^L(x)\right) \text{ for all } x \in L.$$

2.1 Quadratic Boolean functions

In this subsection, we give some lemmas which are used in this paper.

Let q be a power of *2* and let *V* be an *n*-dimensional vector space over F_q. A function *Q* from *V* to F_q is said to be a quadratic function on *V*, if it satisfies following:

1. $Q(cx)=c^2Q(x)$ for any $c\in F_q$ and $x\in V$,
2. $B(x,y)=Q(x)+Q(y)+Q(x+y)$ is bilinear on *V*.

The kernel [1, 25] of Q is the subspace of V defined by

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

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

Lemma 2. ([1], Lemma1): Let f be a quadratic Boolean function. The kernel of f is the subspace of F_{2^n} having those *b* such that $D_b(f)$ is constant.

$$\varepsilon_f=\{b\in F_{2^n}: D_b(f)\}=Cons\tan t.$$

Lemma 3. [1, 25] If $f:F_{2^n}\to F_2$ is a quadratic Boolean function and $B(x,y)$ is the bilinear form associated to it. Then the Walsh spectrum of *f* depends only on the dimension, k, of the kernel, ε_f of $B(x,y)$. The weight distribution of the Walsh spectrum of f is:

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

Carlet [3] proved the following results.

Proposition 1. ([3], Proposition 2) Let *f* be a *n*-variable Boolean function and *r* be a positive integer less than *n*, we have

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

Corollary 1. ([3], Corollary 2) Let f be an *n*-variable Boolean function and r be a positive integer smaller then n. Assume that, for some non-negative integers M and m, we have

$$nl_{r-1}(D_a f)\ge 2^{n-1}-M2^m \qquad (1)$$

for every non-zero $a\in F_{2^n}$. Then we have

$$nl_r(f)\ge 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)M2^{m+1}+2^n}$$

$$nl_r(f)\approx 2^{n-1}-\frac{1}{2}\sqrt{M}\,2^{\frac{n+m-1}{2}}. \qquad (2)$$

Definition 5: ([21], Page 99): A polynomial of the form

$$L(x)=\sum_{i=0}^{n}\beta_i x^{q^i}$$

with the coefficients β_i in an extension field F_{q^n} of F_q is called a Linearized polynomial (*q*-polynomial) over F_{q^n}.

MAIN RESULTS

Lemma 4. Consider the Boolean function $f_\lambda(x)=Tr_1^n(\lambda x^p)$, where $p=2^{2r}+2^r+1$, $\lambda\in F^*_{2^r}$, and $n=5r$. Then the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either r or $3r$.

Proof: The algebraic degree of Boolean function $f_\lambda(x)$ is 3. The derivative of $f_\lambda(x)$ with respect to $a\in F^*_{2^n}$ is

$$D_a(f_\lambda(x))=f_\lambda(x+a)+f_\lambda(x)$$

$$D_a(f_\lambda(x))=Tr_1^n(\lambda(x+a)^{2^{2r}+2^r+1})+Tr_1^n(\lambda(x)^{2^{2r}+2^r+1})$$

$$D_a(f_\lambda(x))=Tr_1^n(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1}+a^{2^r+1}x^{2^{2r}}+a^{2^{2r}+1}x^{2^r}+a^{2^{2r}+2^r}x+a^{2^{2r}+2^r+1}))$$

The Walsh spectrum of Boolean function $D_a(f_\lambda(x))$ is equal to the Walsh spectrum of the function $G_\lambda(x)$, where $G_\lambda(x)$ is obtained by removing all affine monomials from $D_a(f_\lambda(x))$.

$$G_\lambda(x)=Tr_1^n(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1})).$$

$G_\lambda(x)$ can also be written as

$$G_\lambda(x)=Tr_1^n(\lambda a^{2^r}x^{2^{2r}+1}+(\lambda^{2^{4r}}a^{2^{4r}}+\lambda a^{2^{2r}})x^{2^r+1}).$$

Because $2^{2r}+1$ and 2^r+1 are not lie in the same cyclotomic coset. Therefore, $G_\lambda(x)$ is not equal to zero for $a \in F^*_{2^n}$. Therefore $G_\lambda(x)$ is a quadratic Boolean function. By Lemma 2, 3, the Walsh spectrum of $G_\lambda(x)$ depends on the dimension k of the kernel of $G_\lambda(x)$ which is the subspace of those b such that $D_b(G_\lambda(x))$ is constant. The derivative $D_b(G_\lambda(x))$ is

$$D_b(G_\lambda(x)) = G_\lambda(x+b) + G_\lambda(x)$$

$$\begin{aligned} D_b(G_\lambda(x)) = Tr_1^n(\lambda((ab^{2^r} + a^{2^r}b)x^{2^{2r}} \\ + (ab^{2^{2r}} + a^{2^{2r}}b)x^{2^r}) + (a^{2^r}b^{2^{2^{2r}}} + a^{2^{2r}}b^{2^r})x) \\ + Tr_1^n(\lambda(ab^{2^{2r}+2^r} + a^{2^r}b^{2^{2r}+1} + a^{2^{2r}}b^{2^r+1})). \end{aligned}$$

Since $x, a, b \in F_{2^n}$ and $\lambda \in F^*_{2^r}$. Therefore, $x^{2^n} = x$, $a^{2^n} = a$, $b^{2^n} = b$, $\lambda^{2^r} = \lambda$. We get

$$\begin{aligned} D_b(G_\lambda(x)) = Tr_1^n(\lambda x((a^{2^{3r}} + a^{2^r})b^{2^{4r}} + a^{2^{4r}}b^{2^{3r}} + a^{2^r}b^{2^{2r}})) \\ + (a^{2^{4r}} + a^{2^{2r}})b^{2^r})) + \text{Constant terms.} \end{aligned}$$

Clearly, $D_b(G_\lambda(x))$ is equal to the constant if and only if

$$(a^{2^{3r}} + a^{2^r})b^{2^4} + a^{2^{4r}}b^{2^{3r}} + a^{2^r}b^{2^{2r}} + (a^{2^{4r}} + a^{2^{2r}})b^{2^r} = 0.$$

Or it is equivalent to the following

$$(a^{2^{2r}} + a)b^{2^{3r}} + a^{2^{3r}}b^{2^{2r}} + ab^{2^r} + (a^{2^{3r}} + a^{2^r})b) = 0. \quad (3)$$

It is to be noted that equation 3 is a 2^r-polynomial. Since a polynomial of the form $L(x) = \sum_{i=0}^{n} \beta_i x^{q^i}$ with the coefficients β_i in an extension field F_{q^m} is called *q*-Polynomial over F_{q^m}. Let

$$M(b) = (a^{2^{2r}} + a)b^{2^{3r}} + a^{2^{3r}}b^{2^{2r}} + ab^{2^r} + (a^{2^{3r}} + a^{2^r})b).$$

As a consequence, the dimension of the kernel of $M(x)$ equals to sr, for $s = 0, 1, 2,$ or $3.$

Now quadratic form from F_{q^5} to F_q $(q = 2^r)$

$$N(x) = Tr_E^L(\lambda(ax^{2^{2r}+2^r} + a^{2^r}x^{2^{2r}+1} + a^{2^{2r}}x^{2^r+1})),$$

Where $L = F_{2^{5r}}$ and $E = F_{2^r}$.

The set of roots of $M(x)$ is also the kernel of $N(x)$. Indeed, the kernel of $N(x)$ is the set of those b such that $B(x) = 0$ for all x where $B(x)$ is given as

$$B(x) = N(x) + N(b) + N(x+b)$$

Because $D_b(G_\lambda(x)) = Tr_{F_2}^E(B(x))$, we get

$$B(x) = Tr_E^L(xM(b)).$$

Therefore, the kernel of $N(x)$ is equal to the kernel of $M(x)$. By Lemma 1, the dimension of the kernel of $N(x)$ must have the same parity as 5. Hence this is odd. Therefore, the dimension of the kernel of $N(x)$ is either 1 or 3 which imply that the one of $M(x)$ is either r or $3r$, that is, the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either r or $3r$ (*k = r* or *k= 3r*).

***Theorem* 1**. Consider the Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$, where $p = 2^{2r} + 2^r + 1$, $\lambda \in F^*_{2^r}$, and $n = 5r.$ Then

$$nl_2(f_\lambda(x)) = 2^{n-1} - 2^{\frac{3n+3r-4}{4}}.$$

Proof : From Lemma 4, the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either either r or $3r$ (*k = r* or *k= 3r*). From Corollary 1, nonlinearity of $D_a(f_\lambda(x))$ that is, $nl(D_a(f_\lambda(x)))$ is either $2^{n-1} - \frac{1}{2}2^{\frac{n+r}{2}}$ or $2^{n-1} - \frac{1}{2}2^{\frac{n+3r}{2}}$. Therefore, we have

$$\max_{a \in F_2^n}(nl(D_a(f_\lambda(x)))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+r}{2}}.$$

Therefore, by Proposition 1, we have

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{n+r-4}{4}}. \quad (4)$$

$a \in F^*_{2^n}$, we also have

$$nl(D_a(f_\lambda(x))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+3r}{2}}. \quad (5)$$

We can also improve the lower bound on comparing equation 5 with the equation 1. After comparing, we get

$M=1$ and $m=\dfrac{n+3r-2}{2}$.. Therefore, using the value of M and m in equation 2, we get

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{3n+3r-4}{4}}. \qquad (6)$$

From the above it is clear, the lower bound obtained by equation 6 is better than the lower bound obtained by equation 4 for $r>1$. So, we have

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{3n+3r-4}{4}}.$$

COMPARISON

We compare the lower bound obtained in Theorem 1 with the lower bound obtained by Iwata-Kurosawa [17] and the lower bound obtained by Gangopadhyay, Sarkar and Telang (Theorem 1, [12]) in following Table .

n, r	10, 2	15, 3	20, 4	25, 5	30, 6
Bound obtained in Theorem 1	256	10592	393216	$1.3811 * 10^7$	$4.6976 * 10^8$
Iwata-Kurosawa's bound	192	6144	196608	$6.2914 * 10^6$	$2.0132 * 10^8$
Bound obtained in (Theorem 1, [12])	N/A	N/A	N/A	N/A	$4,4196 * 10^8$

35, 7	40, 8	45, 9	50, 10	55, 11	60,12
$1.5661 * 10^{10}$	$5.1539 * 10^{11}$	$1.6814 * 10^{13}$	$5.4535 * 10^{14}$	$1.7616 * 101^6$	$5.6745 * 10^{17}$
$6.4424 * 10^9$	$2.0615 * 10^{11}$	$6.5970 * 10^{12}$	$2.1110 * 10^{14}$	$6.7553 * 10^{15}$	$2.1617 * 10^{17}$
N/A	N/A	N/A	N/A	N/A	$5.5844 * 10^{17}$

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

It is clear from the above table that our lower bound is much better than lower bounds obtained by Iwata-Kurosawa and Gangopadhyay et al.

CONCLUSION

In this paper, we find a lower bound of second-order nonlinearity of a class of Boolean functions $f_\lambda(x)=Tr_1^n(\lambda x^p)$, where $p=2^{2r}+2^r+1$, $\lambda \in F_{2^r}^*$, and $n=5r$. The algebraic immunity of $f_\lambda(x)$ is at most *3* because the algebraic degree of $f_\lambda(x)$ is *3* $(AI(f) \leq d^0(f)$. Therefore, the lower bound of second-order nonlinearity of $f_\lambda(x)$ can not be obtained from the relation between *r*th-order nonlinearity and the algebraic immunity as given in [2, 4]. The lower bound of second-order nonlinearity of $f_\lambda(x)$ is much better than lower bound obtained in [17] and (Theorem 1, [12]). Carlet [3] has obtained a way of finding out lower bounds of rth-order nonlinearities of Boolean functions. A natural question is whether the bounds obtained by Carlet can be improved for special classes of functions. It is observed that of second-order nonlinearities of cubic functions more refined bounds can be obtained by using the technique developed by Carlet and results related of dimensions of solutions spaces of linearized polynomials which was done by Gangopadhyay et al. [12, 15] and subsequently by several other authors [28, 29]. These bounds are also related to covering radius of second-order Reed-Muller codes. From the cryptographic and coding theoretic perspectives we feel that it is important to consider specific classes of functions and to obtain more information about their second-order nonlinearities. This has motivated our research.

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, "On the higher order-nonlinearities of algebraic immune functions," *Advances in Cryptology-CRYPTO 2006*, LNCS 4117, Springer-Verlag, pp. 584-601, 2006.
[3] 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.
[4] C. Carlet, D. Dalai, K. Gupta and S. Maitra, "Algebraic immunity for cryptographyically significant boolean functions: analysis and construction," *IEEE Trans. Inform. Theory*, 52(7), pp. 3105-3121, 2006.
[5] 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.
[6] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, "Covering Codes," Amsterdam, The Netherlands: North-Holland, 1997.
[7] 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.

[8] C. Ding, G.Xiao and W. Shan, "The stability theory of stream ciphers," *LNCS, Springer,* Heidelberg, Vol. 561, 1991.

[9] H. Dobbertin et al., "Construction of bent functions via Niho power functions," *Journal of Combinatorial Theory*, Series A 113, pp. 779-798, 2006.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[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] N. Kolokotronis, K. Limniotis and N. Kalouptsidis, "Best affine and quadratic approximations of partcular classes of Boolean functions," IEEE Trans. Inform. Theory, Vol. 55, no. 11, pp. 5211-5222, 2009.

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

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

[23] 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.

[24] 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.

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

[26] O. S. Rothaus, "On bent functions," *Journal of Combinatorial Theory*, Series A, 20, pp. 300-305, 1976.

[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.