ISSN:0975-9646

Second Order Nonlinearities of Some Classes of Cubic Boolean Functions Based on Secondary Constructions

Deep Singh
Department of Mathematics,
Indian Institute of Technology Roorkee
Roorkee 247 667, India.

***Abstract*- The higher order nonlinearity of a Boolean function is a cryptographic criterion, which play a role against attacks on stream and block ciphers. Also it play a role in coding theory, since it is related to the covering radii of Reed-Muller codes. In this paper, we study the lower bounds of second-order nonlinearities of a class of cubic Boolean functions of the form $tr_1^n(\lambda x^{2^{2r}+2^r+1})$ with $n = 3r$ and $\lambda \in F'_{2^r}$ and some classes of cubic Boolean functions based on secondary construction. Whose lower bounds on second order nonlinearities improved upon previous existing general results.**

***Index Terms*-Cryptography, derivative of Boolean functions, second-order nonlinearity, partial spreads.**

I. INTRODUCTION

Boolean functions play an important role in cryptography. The Boolean functions used in streams ciphers must have high order nonlinearity profile. Any function from F_{2^n} to F_2 is called a Boolean function on *n*-variables, where $F_2 = \{0, 1\}$ be the prime field of characteristic 2 and F_{2^n} is extension field of degree n over F_2. The set of all n-variable Boolean functions is denoted by B_n. The Algebraic Normal Form (ANF) of the Boolean function is given as

$$f(x) = \bigoplus_{a \in F_2^n} \mu_a x^a$$

Where $x^a = \prod_{i=1}^{n} x_i^{a_i}$ is a monomial and $\mu_a \in F_2$. The algebraic degree of *f*, denoted by deg (*f*) and is the maximum degree of monomial for which $\mu_a \neq 0$. The Hamming distance, $d(f, g)$ between $f, g \in B_n$ is the size of set $\{x \in F_{2^n}: f \oplus g \neq 0\}$.

The trace function $f: F_{2^n} \rightarrow F_2$ is defined by $tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. For given any $x, y \in F_{2^n}, tr_1^n(xy)$ is an inner product of x and y. Let A_n is the set of all affine Boolean functions on n- variables. Nonlinearity of $f \in B_n$ is defined as $nl(f) = min_{l \in A}\{d(f, l)\}$. The Walsh transform of $f \in B_n$ at $\lambda \in F_{2^n}$ is defined as:

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

The multiset $\{W_f(\lambda): \lambda \in F_{2^n}\}$ is said to be the Walsh spectrum of f. Following is the relationship between nonlinearity and Walsh spectrum of $f \in B_n$ is

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

By Parseval's identity

$$\sum_{\lambda \in F_{2^n}} W_f(\lambda)^2 = 2^{2n}$$

It can be shown that $|W_f(\lambda)| \geq 2^{n/2}$, which implies that

$$nl(f) \leq 2^{n-1} - 2^{n/2-1}$$

Definition 1: Suppose n is an even integer. A function $f \in B_n$ is said to be a bent function if and only if $nl(f) \leq 2^{n-1} - 2^{n/2-1}$ (i.e., $W_f(\lambda) = \{2^{n/2}, -2^{n/2}\}$ for all $\lambda \in F_{2^n}$.

Bent functions first time introduced by Rothous [10]. For odd $n \geq 9$ the tight upper bound of nonlinearities of Boolean functions B_n is not known**.**

Definition 2: The derivative of $f \in B_n$ with respect to $a \in F_{2^n}$ denoted by $D_a f(x)$ is defined as

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

The higher order derivatives are defined as follows.

Definition 3: Let V be a r-dimensional subspace of F_{2^n} generated by $a_1, a_2, ...a_r$, i.e. $V = < a_1, a_2, ...a_r >$. The r-th order derivative of $f \in B_n$ with respect to *V*, denoted by $D_V(f)$ or $D_{a_1}, D_{a_2}, \dots, D_{a_r} f(x)$ is defined by $D_V f(x) = D_{a_1}, D_{a_2}, \dots, D_{a_r} f(x)$ for all$x \in F_{2^n}$. .

It is noted that the r-th order derivative of f depends only on the choice of the r-dimensional subspace V and independent of the choice of the basis of *V*.

Definition 4: Let $f \in B_n$ for every non-negative integer *r* smaller than *n*, we denote by $nl_r(f)$ the r-th order nonlinearity of f**,** which is the minimum Hamming distance of f from all n variable Boolean functions of algebraic degree at most r**.**

The set of all Boolean function of *n* variables of degree at most r is said to be the Reed-Muller code$RM(r, n)$, of length 2^n and of order r**.** The sequence of values *n* $nl_r(f)$, for n ranging from 1 to $n-1$**,** is said to be the nonlinearity profile of f The first order nonlinearity of a Boolean function on *n* variables can be computed by using fast Walsh transform in time *o(n2*^{n}*).* Unlike first-order nonlinearity there is no efficient algorithm to compute second-order nonlinearities for $n > 11$. Most efficient algorithm due to Fourquet and Tavernier [6] works for $n \le 11$ and up to $n = 13$ for some special functions. Thus, identifying classes containing Boolean functions with "good" nonlinearity profile is an important problem. There is no efficient algorithm to compute rth-order(for $r \ge 2$) nonlinearity of a Boolean function. Carlet [3, 4] for the first time did the systematic study of higher order nonlinearity and nonlinearity profile of Boolean functions. He 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*. He also obtained of the lower bounds of the second-order nonlinearities of several classes of functions, Welch function and the inverse function being among of them. We also refer to results due to Carlet-Mesnager [5] and Sun-Wu [12]. The best known asymptotic upper bound on $nl_r(f)$ is obtained by Carlet and Mesnager [5], which is

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

In [5] Carlet efficiently lower bounded the nonlinearity profile of Dillon type bent functions. Using Carlet's approach Gangopadhyay, Sarkar and Telang [7], Gode and Gangopadhyay [8], Sun and Wu [12] obtained the lower bounds of the second-order nonlinearities of several classes of Boolean functions. In this paper, we consider a class of cubic Boolean functions of the form $tr_1^n(\lambda\, x^{2^{2r}+2^r+1})$ with $n = 3r$ and $\lambda \in F'_{2^r}$. A lower bound of second-order nonlinearities of these functions is obtained and compared with the lower bounds of second-order nonlinearities obtained for functions belonging to some other classes of functions which are recently studied.

II. PRELIMINARIES

A. *Quadratic Boolean function*

Suppose $f \in B_n$ is a quadratic function. The binary form associated with f is defined by

$$B(x, y) = f(0) + f(x) + f(y) + f(x + y).$$

The kernel of $B(x, y)$ is subspace of F_{2^n} defined by

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

Lemma 1. ([1], Proposition 1): 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], Lemma 1): Let f be any quadratic Boolean function. The kernel, ε_f is the subspace of F_{2^n} consisting of those $a \in F_{2^n}$ such that the derivative $D_a f(x)$ is constant. That is,

$$\varepsilon_f = \{x \in F_{2^n} : D_a f = constant\}.$$

If f is a quadratic Boolean function and $B(x, y)$ is the quadratic form associated with it, then the Walsh Spectrum of f depends only on the dimension, k, of the kernel of $B(x, y)$ [1, 9]. The weight distribution of the Walsh spectrum of *f* is:

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

B. *Recursive lower Bounds of Higher-Order Nonlinearities*

Following are some results proved by Carlet [4].

Proposition 1. ([4], Proposition 2): Let $f \in B_n$ and r be a positive integer smaller than *n* then 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,

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

For every non-negative integer $i < r$.
In particular, for r = 2,

$$nl_2(f) \geq \frac{1}{2} \max_{a \in F_{2^n}} nl(D_a f)$$

Proposition 2. ([4], Proposition 3): Let $f \in B_n$ and r be a positive integer smaller than , then we have

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

Corollary 1. [[4], Corollary 2]: Let $f \in B_n$ and r be a positive integer smaller than n**.** Assume that, for some non-negative integers $M$and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in F_{2^n}$. Then

$$\begin{aligned} nl_r(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{\frac{n+m-1}{2}}} \\ &\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}} \end{aligned}$$

Carlet remarked that in general, the lower bound given by the Proposition 2 is potentially stronger than that given in Proposition 1 [4].

In this paper, we study the lower bounds of second-order nonlinearities of a class of cubic Boolean functions of the form $tr_1^n\left(\lambda\, x^{2^{2r}+2^r+1}\right)$ with $n = 3r$ and $\lambda \in F'_{2^r}$ and some classes of cubic Boolean functions based on secondary construction. Whose lower bounds on second order nonlinearities improved upon some previous existing general results. The derivative of any cubic Boolean function has algebraic degree at most 2 and the Walsh spectrum of a quadratic Boolean function [1] is completely characterized by the dimension of the kernel of the bilinear form associated with it.

III. SECOND ORDER NONLINEARITY OF A CLASS OF CUBIC BOOLEAN FUNCTIONS OF THE PARTICULAR TYPE

Theorem 1. Suppose $f \in B_n$ such that $f(x) = tr_1^n\left(\lambda\, x^{2^{2r}+2^r+1}\right) \forall\, x \in F_{2^n}$, with $n = 3r$ and $\lambda \in F'_{2^r}$. Then

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

Proof: *f(x)* =$tr_1^n(\lambda\, x^{2^{2r}+2^r+1})$ with $n = 3r$ and $\lambda \in F'_{2^r}$, the first order derivative f w. r. t. $a \neq 0,\ a \in F_{2^n}$ is

$$D_a f(x) = tr_1^n\left(\lambda\,(x + a)^{2^{2r}+2^r+1}\right) + tr_1^n\left(\lambda\, x^{2^{2r}+2^r+1}\right)$$

$$= tr_1^n\left(\lambda\left(a\, x^{2^{2r}+2^r}\, a^{2^r}\, x^{2^{2r}+1} + a^{2^{2r}} x^{2^r+1}\right)\right) + l(x)$$

Where $l(x)$ is an affine Boolean function. Let $b \in F_{2^n}$ such that $a \neq b$, then

$$\begin{aligned} D_b\, D_a f(x) = tr_1^n(a\lambda\big((x+b)^{2^{2r}+2^r} + x^{2^{2r}+2^r}\big) \\ + a^{2^r}\lambda\big((x+b)^{2^{2r}+1} + x^{2^{2r}+1}\big) \\ + a^{2^{2r}}\lambda\big((x+b)^{2^r+1} + x^{2^r+1}\big)\,) \end{aligned}$$

$$\begin{aligned} = tr_1^n(a\lambda\big(b^{2^r}x^{2^{2r}} + b^{2^{2r}}x^{2^r} + b^{2^{2r}+2^r}\big) \\ + a^{2^r}\lambda\big(bx^{2^{2r}} + b^{2^{2r}}x + b^{2^{2r}+1}\big) \\ + a^{2^{2r}}\lambda\big(bx^{2^{2r}} + b^{2^r}x + b^{2^r+1}\big)) \end{aligned}$$

$$= tr_1^n\big(x^{2^{2r}}\lambda\big(ab^{2^r} + a^{2^r}b\big) + x^{2^r}\lambda\big(ab^{2^{2r}} + a^{2^{2r}}b\big) + x\lambda(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r})\big) + constatns$$

$$\begin{aligned} = tr_1^n(x\Big(\lambda^{2^{n-2r}}\big(ab^{2^r} + a^{2^r}b\big)^{2^{n-2r}} \\ + \lambda^{2^{n-r}}\big(ab^{2^{2r}} + a^{2^{2r}}b\big)^{2^{n-r}} \\ + \lambda\,(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}))\Big) + constant \end{aligned}$$

$D_b\, D_a f$ is constant if and only if

$$\begin{aligned} \lambda^{2^{n-2r}}\big(ab^{2^r} + a^{2^r}b\big)^{2^{n-2r}} + \lambda^{2^{n-r}}\big(ab^{2^{2r}} + a^{2^{2r}}b\big)^{2^{n-r}} \\ + \lambda\left(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}\right) = 0 \end{aligned}$$

Since $\lambda \in F'_{2^r}$ and $n = 3r$, therefore,

$$\begin{aligned} \lambda\Big(\big(ab^{2^r} + a^{2^r}b\big)^{2^{n-2r}} + \big(ab^{2^{2r}} + a^{2^{2r}}b\big)^{2^{n-r}} \\ + \big(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}\big)\Big) = 0 \end{aligned}$$

$$\begin{aligned} i.e., \quad \Big(\big(ab^{2^r} + a^{2^r}b\big)^{2^{n-2r}} + \big(ab^{2^{2r}} + a^{2^{2r}}b\big)^{2^{n-r}} \\ + \big(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}\big)\Big)^{2^{2r}} = 0 \end{aligned}$$

$$\begin{aligned} i.e., \quad ab^{2^r} + a^{2^r}b + a^{2^r}b^{2^{3r}} + a^{2^{3r}}b^{2^r} + a^{2^{3r}}b^{2^{4r}} \\ + a^{2^{4r}}b^{2^{3r}} = 0. \end{aligned}$$

Using $x^{2^n} = x\ and\ n = 3r$, we have

$$ab^{2^r} + a^{2^r}b = 0$$

$$(b/a)^{2^r-1}=1, \qquad for\ \ b\neq 0$$
$$b\ \in aF'_{2^r}.$$

Thus, for any non zero $a\in F_{2^n}$, number of ways in which b can be chosen so that $D_b\,D_af$ is constant are 2^r (including the case $b=0$). Hence by Lemma 2 we have, the dimension, k of the kernel associated with $D_a\,f$ is r i.e., $k=r$. Thus the Walsh transform of $D_a\,f$ at any point $\alpha\in F_{2^n}$ is

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

Therefore nonlinearity of $D_a\,f$ is

$$nl(D_a\,f)=2^{n-1}-2^{\frac{n+r-2}{2}} \qquad (1)$$

Using Proposition 1 we have

$$nl_2(f)\geq 2^{n-2}-2^{\frac{n+r-4}{2}}$$

Therefore we have a scope to get the better bounds using Corollary 1. Comparing (1) and Corollary 1, we have $M=1,\ m=\frac{n+r-2}{2}$, then by Corollary 1,

$$nl_2(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r-2}{2}+1}+2^n}$$
$$\approx 2^{n-1}-2^{\frac{n+\frac{n+r-2}{2}-1}{2}}$$
$$\approx 2^{n-1}-2^{\frac{3n+r-4}{4}} \qquad (2)$$

IV. SECOND ORDER NONLINEARITIES OF A SOME CLASSES OF CUBIC BOOLEAN FUNCTIONS BASED ON SECONDARY CONSTRUCTION

Lemma 3: Let $g_\lambda(x,y)=(1+y)tr_1^t\big(\lambda(x^d+x)\big)+ytr_1^t(\lambda x^d)$, $\lambda\in F'_{2^t}$ be a Boolean function defined on $F_{2^n},\ n=t+1$ then the dimension of the kernel of the bilinear form associated to $D_{(a,b)}g_\lambda$ is $k+1$ where k is the dimension of the kernel of the bilinear form associated to $D_af_{\lambda,}\ f_\lambda(x)=tr_1^t(\lambda x^d)$, here $x\in F_{2^t,}\ y\in F_2$ and f_λ be a cubic Boolean function.

Proof: The function g_λ can be written as $g_\lambda(x,y)=tr_1^t\big(\lambda(x+xy)\big)+tr_1^t(\lambda x^d)$. Consider a 2-dimensional subspace V generated by two vectors (a,b) and (c,d). The second order derivative of g at V is as follows:

$$D_Vg_\lambda(x,y)=D_{(c,d)}D_{(a,b)}g_\lambda(x,y)$$
$$=\text{constant}+D_Vf_\lambda(x) \qquad (3)$$

Clearly $D_{(a,b)}g_\lambda(x,y)$ is quadratic hence by Lemma 2 the kernel,

$$\varepsilon_{D_{(a,b)}g_\lambda}=\{(c,d)\in\ F_{2^t}\times\ F_2:D_{(c,d)}D_{(a,b)}g_\lambda=constant\}$$
$$=\{(c,d)\in\ F_{2^t}\times\ F_2:D_{(c,d)}D_{(a,b)}f_\lambda=constant\} \ (4)$$

Also it is given that the kernel, $\varepsilon_{D_cf_\lambda}$ is of dimension $k.$ Thus in (4) c has 2^k distinct values. Corresponding to each value of c,d can be chosen in 2 ways. Therefore, the total number of ways in which (c,d) can be chosen so that $D_{(c,d)}D_{(a,b)}g_\lambda$ is constant is $2^k.2=2^{k+1}$. Hence $\varepsilon_{D_{(a,b)}g_\lambda}$ contains exactly 2^{k+1} elements.

Theorem 2: Let n is even and $n=t+1$ and l be integer such that $l=\frac{t+1}{2}$ or $=\frac{t-1}{2}$, define a function g defined on F_{2^n} as $g(x,y)=(1+y)tr_1^t\left(x^{2^l+3}+x\right)+ytr_1^t\left(x^{2^l+3}\right)$, then second order nonlinearity of g is given by

$$nl_2(g)=\ 2^{n-1}-\frac{1}{2}\sqrt{2^{n+1}+2^{\frac{3n+4}{2}}-2^{\frac{n+6}{2}}}$$

Proof: $g(x,y)=(1+y)tr_1^t\left(x^{2^l+3}+x\right)+ytr_1^t\left(x^{2^l+3}\right)$
Comparing this equation to Lemma 3, when $\lambda=1$ we get $f(x)=tr_1^t(x^{2^l+3})$, it is given in [3] that the dimension ,k, of the kernel, ε_{D_af}, is ≤3 i.e., $k\leq 3$ for all a∈ F'_{2^t}. Hence by Lemma 3, the dimension, $k(a,b)$, of the kernel, $\varepsilon_{D_{(a,b)}g}$ is ≤4 i.e., $k(a,b)\leq 4$, for all (a, b)∈ $F_{2^t}\times F_2\big((a,b)\neq(0,b)\big)$. Hence the Walsh transform for all $(\lambda,\mu)\in F_{2^t}\times F_2$ is:

$$W_{D_{(a,b)}g}(\lambda,\mu)\leq 2^{\frac{n+k(a,b)}{2}}$$

Thus the nonlinearity of $D_{(a,b)}g$ is:

$$nl_1\big(D_{(a,b)}g\big)=2^{n-1}-\frac{1}{2}max_{(\lambda,\mu)\in F_{2^t}\times F_2}|W_{D_{(a,b)}g}(\lambda,\mu)|$$
$$\geq 2^{n-1}-\frac{1}{2}2^{\frac{n+k(a,b)}{2}}$$
$$\geq 2^{n-1}-2^{\frac{n+2}{2}}$$

By using Proposition 2 we get:

$$nl_2(g)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2(2^n-2)(2^{n-1}-2^{\frac{n+2}{2}})}$$
$$\approx 2^{n-1}-\frac{1}{2}\sqrt{2^{n+1}+2^{\frac{3n+4}{2}}-2^{\frac{n+6}{2}}}.$$

Theorem 3: Suppose $g_\lambda(x,y)=ytr_1^6\big(\lambda\,x^{2^3-1}\big)+(1+y)tr_1^6\left(\lambda\big(x^{2^3-1}+x\big)\right)$, then second order nonlinearity of the function g_λ defined on 7-variable is:

$$nl_2(g_\lambda)=24$$

Proof: Clearly g_λ is cubic function. It is proved in [11] that the dimension of the kernel $\varepsilon_{D_{(a=1)}f_\lambda}$ is 2 where $f_\lambda(x,y)=tr_1^6(\lambda(x^{2^3-1}))$. By lemma 3 we get that the dimension, $k(a,b)$, of the kernel, $\varepsilon_{D_{(a,b)}g_\lambda}$is 3, i.e., $k(1,b)=3$. Hence the Walsh transform for all $(\lambda,\mu)\in F_{2^t}\times F_2$ is :

$$W_{D_{(1,b)}g_\lambda}(\lambda,\mu)=2^{\frac{n+k(1,b)}{2}}$$

i.e., $$W_{D_{(1,b)}g_\lambda}(\lambda,\mu)=2^{\frac{7+3}{2}}=2^5$$

Thus the nonlinearity of $D_{(1,b)}g_\lambda$ is:

$$nl_1\left(D_{(1,b)}g_\lambda\right) = 2^{n-1} - \tfrac{1}{2}max_{(\lambda,\mu)\in F_{2^t}\times F_2}|W_{D_{(1,b)}f}(\lambda,\mu)|$$
$$= 2^6 - 2^{5-1} = 48$$

By using Proposition 1 we get:

$$nl_2(g_\lambda) \geq 24.$$

Theorem 4: Let $g(x,y) = ytr_1^6\left(x^{2^3-1}\right) + (1+y)tr_1^6\left(x^{2^3-1} + x\right)$, then second order nonlinearity of the function g defined on 7-variables is:

$$nl_2(g) \geq 28$$

Proof: Clearly g is cubic function. It is proved in [11] that the dimension of the kernel ε_{D_af} is 2 at 49 points and 4 at 14 points in F_{2^6}, where $f_\lambda(x,y) = tr_1^6\left(x^{2^3-1}\right)$. Hence by Lemma 5, the dimension, $k(a,b)$, of the kernel, $\varepsilon_{D_{(a,b)}g}$ is 3 at 98 points and 5 at 28 points in F_{2^7}. Therefore,

$$nl\left(D_{(a,b)}g\right) = \begin{cases} 2^6 - 2^{\frac{7+3}{2}-1} = 48, & if\ k = 3, \\ 2^6 - 2^{\frac{7+5}{2}-1} = 32, & if\ k = 5. \end{cases}$$

By using Proposition 2 we get:

$$nl_2(g) \geq 2^6 - \frac{1}{2}\sqrt{2^{14} - 2\sum_{(a,b)\in F_{2^6}\times F_2} nl_1(D_{(a,b)}g_\lambda)}$$
$$= 2^6 - \tfrac{1}{2}\sqrt{16384 - 2(98.48 + 28.32)}$$
$$= 64 - \tfrac{1}{2}\sqrt{5184} = 28.$$

Theorem 5: Define Boolean function $g_\lambda : F_{2^n} \to F_2$ as follows $g_\lambda(x,y) = (1+y)(f(x)+x) + yf(x)$, where $f_\lambda(x) = (\lambda(x^{2^{2l}+2^l+1}))$, $\lambda \in F_{2^t}$ and l is a positive integer such that $gcd(t,1) = 1$ then for $t > 4$, second order nonlinearity of g_λ is:

$$nl_2(g_\lambda) \geq \begin{cases} 2^{n-1} - \tfrac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+5}{2}} - 2^{\frac{n+7}{2}}}, & if\ \ n \equiv 1\ mod\ 2, \\ 2^{n-1} - \tfrac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}}}, & if\ n \equiv 0\ mod\ 2. \end{cases}$$

Proof: Here the function $f_\lambda(x) = tr_1^t(\lambda(x^{2^{2l}+2^l+1}))$ is cubic, let the dimension of the kernel ε_{D_af} associated with $D_af_\lambda(x)$ is $k(a)$. It is proved in [8] that for all nonzero $a \in F_{2^t}$ is $k(a) \leq 4$ if t is even else $k(a) \leq 3$. Hence Lemma 5 gives us for all $a \in F'_{2^t}$, the dimension, $k(a,b)$, of the kernel, $\varepsilon_{D_{(a,b)}g_\lambda}$ is ≤ 5 i.e., $k(a,b) \leq 5$ if t is even else $k(a,b) \leq 4$. Thus for $(\mu,\ \eta) \in F_{2^t} \times F_2$

$$W_{D_{(a,b)}g_\lambda}(\mu,\ \eta) = 2^{\frac{n+k(a,b)}{2}}$$

i.e., $$W_{D_{(a,b)}g_\lambda}(\mu,\ \eta) \leq \begin{cases} 2^{\frac{n+4}{2}}, & if\ n\equiv 0\ mod\ 2 \\ 2^{\frac{n+5}{2}}, & if\ n\equiv 1\ mod\ 2 \end{cases}$$

Therefore nonlinearity of $D_{(a,b)}g_\lambda$ for all $(a,b) \in F_{2^t} \times F_2$ except $a = 0$ and $a = b$.

$$nl(D_{(a,b)}g_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}2^{\frac{n+4}{2}}, & if\ n \equiv 0\ mod\ 2 \\ 2^{n-1} - \frac{1}{2}2^{\frac{n+5}{2}}, & if\ n \equiv 1\ mod\ 2 \end{cases}$$

- For n even, Proposition 2 gives

$$nl_2(g_\lambda) \geq 2^{n-1} - \tfrac{1}{2}\sqrt{2^{2n} - 2(2^n - 2)(2^{n-1} - 2^{\frac{n+2}{2}})}$$

i.e., $$nl_2(g_\lambda) \geq 2^{n-1} - \tfrac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}})}$$

- For n odd, Proposition 2 gives

$$nl_2(g_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^n - 2)(2^{n-1} - 2^{\frac{n+3}{2}})}$$
$$\geq 2^{n-1} - \tfrac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+5}{2}} - 2^{\frac{n+7}{2}})}.$$

V. COMPARISONS:

In Table 1, (2 and 3) we give the numerical comparison between the bound obtained in Theorem 1(Theorem 3 and 5) and the general bound obtained by Carlet [4] and some other known bounds. it is clear that for $n \in \{3, 6, 9\}$ the bounds obtained by Theorem 1 are very close to maximum known bounds. Also the bounds on second order nonlinearities obtained in Theorem 3 and 5 are more efficient.

TABLE 1
COMPARISON OF THE VALUES OF LOWER BOUNDS OF SECOND ORDER NONLINEARITIES WITH SOME OTHER KNOWN BOUNDS

n, r with n=3r	**Lower bounds obtained in Theorem 1**	**Gode et al. [8] bounds**	**Carlet's General bounds [4]**	***Hmax [6]**
3, 1	2	--	2	1
6, 2	16	10	10	18
9, 3	166	128	75	196
12, 4	1536	1024	600	1760
15, 5	13488	10592	4799	--
18, 6	114688	85732	38391	--

*Hmax used for maximum known Hamming distance.

TABLE 2
COMPARISON OF THE VALUES OF LOWER BOUNDS OF SECOND ORDER NONLINEARITIES OBTAINED BY THEOREM 3 AND 5 (FOR ODD *n*) WITH SOME OTHER KNOWN BOUNDS

n	**Lower bounds obtained in Theorem 3 and 5**	**Gode et al. [8] bounds**	**Carlet's General bounds [4]**	***Hmax [6]**
6	10	10	10	18
8	64	64	38	84
10	331	331	150	400
12	1536	1536	600	1760

TABLE 3
COMPARISON OF THE VALUES OF LOWER BOUNDS OF SECOND ORDER NONLINEARITIES OBTAINED BY THEOREM 5(FOR EVEN *n*) WITH SOME OTHER KNOWN BOUNDS

n	**Lower bounds obtained in Theorem 3 and 5**	**Carlet's General bounds [4]**	***Hmax[6]**
7	19	19	40
9	128	75	196
11	661	300	848
13	3071	1200	---

VI. CONCLUSIONS

In this paper we presented several classes of cubic Boolean functions which shows good behaviour with respect to second order nonlinearities and obtained efficient lower bounds on the second order nonlinearities of the class of cubic Boolean functions. The functions which are used in cipher systems are required to have good nonlinearity profile.

ACKNOWLEDGMENT

The author would like to thank ‘‘NBHM (DAE)", India, for providing financial support. The author also wishes to thank to Mr. B. K. Singh for his helpful suggestions.

REFERENCES

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

[2] C. Carlet, “The complexity of Boolean functions from cryptographic view point,” *Proc. Dagstuhl Seminar Complexity of Boolean Functions*, 2006, pp. 15.

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

[4] C. Carlet and S. Mesnager, “Improving the upper bounds on the covering radii of binary Reed-Muller codes,” *IEEE Trans. Inform. Theory*, vol. 53 (1), 2007, pp. 162-173.

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

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

[7] S. Gangopadhyay, S. Sarkar and R. Telang, “On the lower bounds of the second-order nonlinearities of some Boolean functions”, *Information Sciences,* 180, 2010, pp.266-273.

[8] R. Gode, S. Gangopadhyay, “On second order nonlinearities of cubic monomial Boolean functions,”
Available: http://eprint.iacr.org/2009/502.pdf.

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

[10] 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), 2009, pp. 267-278.

[11] R. Telang and S. Gangopadhyay, On higher-order nonlinearity of monomial partial-spreads type Boolean functions, IMST 2009 - FIM XVIII, Jaypee University of Information Technology, Waknaghat, Solan, H.P., India. August 2-4, 2009.