International Journal of Computational and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 2 (2017), pp. 195-205

http://www.ripublication.com/ijcam.htm

Higher order nonlinearity of some cryptographic functions

Deep Singh[1] **and Amit Paul**
Department of Mathematics,
Central University of Jammu, Samba, India.

Abstract

The security of various cryptosystems is strongly related to the higher order nonlinearity of cryptographic functions. This paper investigates some cryptographic functions with good 2nd and 4th order nonlinearities. Firstly, we tighten the lower bounds on 2nd order nonlinearity for the function $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ and $n = 7s$. Further, we give lower bounds for 4th order nonlinearity of 10-variable partial spreads: $\phi(u) = Tr_1^{10}(\lambda u^{2^{\frac{10}{2}}-1})$, $\lambda \in \mathbb{F}_{2^{10}}^*$.

AMS subject classification:
Keywords: Boolean functions, higher-order nonlinearity, trace functions, Kasami functions, Walsh-Hadamard transform.

1. Introduction

Boolean functions are considered to be the building blocks in the design of several symmetric key cryptosystems. Let $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function on n-unknowns. The rth order nonlinearity $nl_r(\phi)$, $0 < r \leq n$ of ϕ is the minimum Hamming distance of ϕ from the functions of degree $\leq r$ (when $r = 1$, it becomes $nl(\phi)$, the first order nonlinearity). The collection of different values of $nl_r(\phi)$ for $1 \leq r \leq n-1$ is nonlinearity profile for ϕ. The rth order nonlinearity $nl_r(\phi)$ is a natural generalization of first order nonlinearity of ϕ which is important for prevention of affine approximation attacks [1, 12, 13]. The best upper bound on $nl_r(\phi)$ in [6] is asymptotically equivalent to

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

[1] corresponding author

For rth order nonlinearity ($r > 1$) of Boolean functions, we do not have an algorithm unlike the first order nonlinearity. The best algorithm presented in [8] for the case $r = 2$ for $n \leq 11$ and up to $n = 13$ for some functions. Cryptographer feels that there is a need to obtain theoretical bounds of higher order nonlinearities of Boolean functions which are satisfied for all values of n. The *rth order bent* functions with lower bound $2^{n-r-3}(r+5)$ are presented in [13]. Carlet et al. [5] in 2006 derived the lower bounds on rth order nonlinearities of Boolean functions by means of algebraic immunity, the bounds were further improved by Carlet [3].

In [4], Carlet presented recursive approach for rth order nonlinearity. He obtained lower bounds of nonlinearity profiles for the Kasami functions, Welch functions, inverse functions. Using the Carlet's recursive approach various authors [11, 14, 18, 20] have obtained the bounds on the second order nonlinearities of some functions.

In this article, we deduce lower bounds on 2nd order nonlinearity of functions $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ and $n = 7s$. Further, we obtain lower bounds on 4th order nonlinearity of 10-variable monomial partial spreads: $\phi(u) = Tr_1^{10}(\lambda u^{2^{\frac{10}{2}}-1})$, $\lambda \in \mathbb{F}_{2^{10}}^*$.

2. Preliminaries

Let $\mathbb{F}_{2^n}$ be the n degree extension field of $\mathbb{F}_2$. The set of all units of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. A function $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called n-variable Boolean function. Suppose $\mathcal{B}_n$ is the collection of all Boolean functions such that cardinality $|\mathcal{B}_n| = 2^{2^n}$.

The support of $\phi \in \mathcal{B}_n$ is defined as $supp(\phi) = \{u \in \mathbb{F}_2^n : \phi(u) = 1\}$. The Hamming weight of $\phi \in \mathcal{B}_n$ is defined as $wt(\phi) = |supp(\phi)|$. The Hamming distance between two Boolean function $h, \kappa \in \mathcal{B}_n$ is $d(h, \kappa) = |\{\alpha \in \mathbb{F}_{2^n} : h(\alpha) \neq \kappa(\alpha)\}|$. The algebraic normal form of $\phi \in \mathcal{B}_n$ is

$$\phi(u_1, u_2, \ldots, u_n) = \sum_{J \subseteq \{1,2,\ldots,n\}} \alpha_J \left(\prod_{j \in J} u_j \right),$$

where $\alpha_J \in \mathbb{F}_2$ and the terms $\prod_{j \in J} u_j$ are monomials. The maximum degree of the monomial with nonzero coefficient is algebraic degree of ϕ.

For any subfield $\mathbb{F}_{2^t}$ of $\mathbb{F}_{2^n}$ (obviously $t|n$), the function the function $Tr_t^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^t}$ defined by $Tr_t^n(u) = u + u^{2^t} + u^{2^{2t}} + \cdots + u^{2^{(n-1)t}}$ is called a trace function. For $t = 1$, $Tr_1^n(u) = u + u^2 + u^{2^2} + \cdots + u^{2^{n-1}}$ is absolute trace function.

The *derivative* of $\phi \in \mathcal{B}_n$ along $\alpha \in \mathbb{F}_{2^n}$ is given by $D_\alpha \phi(u) = \phi(u) + \phi(u + \alpha)$ for all $u \in \mathbb{F}_{2^n}$. If $W = \langle v_1, \ldots, v_m \rangle$ is a t-dimensional subspace in $\mathbb{F}_{2^n}$ then $D_W \phi(u) = D_{v_1} \cdots D_{v_m} \phi(u)$, for all $u \in \mathbb{F}_{2^n}$ is t-th order derivative of ϕ along W.

The Walsh Hadamard Transform of $\phi \in \mathcal{B}_n$ is defined as

$$W_\phi(\alpha) = \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\phi(u) + Tr_1^n(\alpha u)}, \quad \alpha \in \mathbb{F}_{2^n}$$

The sequence of Walsh coefficients of ϕ is Walsh Hadamard spectrum (WHS) of ϕ. The minimum Hamming distance of $\phi \in \mathcal{B}_n$ from affine functions is nonlinearity of ϕ given as

$$nl(\phi) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_\phi(\alpha)|.$$

Parseval's identity $\sum_{\alpha \in \mathbb{F}_{2^n}} W_\phi^2(\alpha) = 2^{2n}$, implies that $nl(\phi) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. The function with maximum possible nonlinearity is called *bent function* [17] and exists only for n-even. Rothaus [17] in 1976 proved that for even n maximum possible nonlinearity of n-variable Boolean functions is $2^{n-1} - 2^{\frac{n}{2}-1}$.

Let W be a vector space of dimension n over $\mathbb{F}_q$, a field of characteristic 2. A map $Q : W \to \mathbb{F}_q$ is a quadratic form on W if

1. $Q(mu) = m^2 Q(u) \; \forall \; m \in \mathbb{F}_q, u \in W$.
2. $B(u, v) = Q(u) + Q(v) + Q(0) + Q(u + v)$ is bilinear on W.

The kernel of $B(u, v)$ denoted by $\mathcal{E}_Q$ is the subspace of W and is defined as

$$\mathcal{E}_Q = \{u \in W : B(u, v) = 0 \; \forall \; v \in W\}.$$

Lemma 2.1. [2] Suppose W be a vector space of dimension n over $\mathbb{F}_q$, a field of characteristic 2. For a quadratic form Q on W, the dimension of both W and kernel of $B(u, v)$ possess same parity.

Lemma 2.2. [2] Suppose $\phi \in \mathcal{B}_n$ is quadratic. The kernel $\mathcal{E}_\phi$ is

$$\mathcal{E}_\phi = \{u \in \mathbb{F}_{2^n} : D_\alpha \phi = constant\}.$$

Lemma 2.3. [16] If $\phi \in \mathcal{B}_n$ is quadratic, then the WHT of ϕ is only linked with the kernel of ϕ.

Lemma 2.4. [4] Suppose $r < n$ and $\phi \in \mathcal{B}_n$, then

$$nl_r(\phi) \geq \frac{1}{2} \max_{\alpha \in \mathbb{F}_{2^n}} nl_{r-1}(D_\alpha \phi).$$

Lemma 2.5. [4] Suppose $r < n$ and $\phi \in \mathcal{B}_n$, then

$$nl_r(\phi) \geq 2^{n-1} - \frac{1}{2} \sqrt{2^{2n} - 2 \sum_{\alpha \in \mathbb{F}_{2^n}} nl_{r-1}(D_\alpha \phi)}.$$

In terms of higher-order derivative, for every positive integer $\ell < r$.

$$nl_r(\phi) \geq 2^{n-1} - \frac{1}{2} \sqrt{\sum_{\alpha_1 \in \mathbb{F}_{2^n}} \sqrt{\sum_{\alpha_2 \in \mathbb{F}_{2^n}} \cdots \sqrt{2^{2n} - 2 \sum_{\alpha_\ell \in \mathbb{F}_{2^n}} nl_{r-\ell}(D_{\alpha_1} \cdots D_{\alpha_\ell} \phi)}}}.$$

Lemma 2.6. **[4]** Suppose $r < n$ and $\phi \in \mathcal{B}_n$. Also suppose for some nonnegative integers L and θ, and for $0 \neq \alpha \in \mathbb{F}_{2^n}$, we have

$$nl_{r-1}(D_\alpha \phi) \geq 2^{n-1} - L2^\theta. \tag{2.1}$$

Then

$$\begin{aligned} nl_r(\phi) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)L2^{\theta+1} + 2^n} \\ &\approx 2^{n-1} - \sqrt{L}2^{\frac{n+\theta-1}{2}}. \end{aligned} \tag{2.2}$$

3. Main results

This section presents lower bounds on higher order nonlinearities of some cryptographic functions. First, we provide bounds on 2nd order nonlinearities, further, in Subsection 3.1, we discuss 4th order nonlinearities.

Theorem 3.1. Let $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $n = 7s$, $\lambda \in \mathbb{F}_{2^s}^*$. Then dimension of kernel of bilinear form of $D_\alpha(\phi_\lambda(u))$ is either s or $5s$.

Proof. The derivative $D_\alpha(\phi_\lambda(u))$ with respect to $\alpha \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_\alpha\phi_\lambda(u) &= \phi_\lambda(u+\alpha) + \phi_\lambda(u) \\ &= Tr_1^n(\lambda(u+\alpha)^{2^{2s}+2^s+1}) + Tr_1^n(\lambda u^{2^{2s}+2^s+1}) \\ &= Tr_1^n(\lambda(\alpha u^{2^{2s}+2^s} + \alpha^{2^s}u^{2^{2s}+1} + \alpha^{2^{2s}}u^{2^s+1} + \alpha^{2^s+1}u^{2^{2s}} \\ &\quad +\alpha^{2^{2s}+1}u^{2^s} + \alpha^{2^{2s}+2^s}u + \alpha^{2^{2s}+2^s+1})) \end{aligned}$$

quadratic. The WHS of $D_\alpha\phi_\lambda(u)$ is equivalent to that of $g_\lambda(u)$, where $g_\lambda(u)$ is obtained by eliminating linear and constant terms in $D_\alpha\phi_\lambda(u)$ as

$$g_\lambda(u) = Tr_1^n(\lambda(\alpha u^{2^{2s}+2^s} + \alpha^{2^s}u^{2^{2s}+1} + \alpha^{2^{2s}}u^{2^s+1})),$$

$g_\lambda(u)$ can also be written as

$$g_\lambda(u) = Tr_1^n(\lambda\alpha^{2^s}u^{2^{2s}+1} + (\lambda^{2^{6s}}\alpha^{2^{6s}} + \lambda\alpha^{2^{2s}})u^{2^s+1}).$$

Since $2^{2s}+1$ and 2^s+1 do not belongs to same cyclotomic coset. So, $g_\lambda(u) \neq 0$ for any $\alpha \in \mathbb{F}_{2^n}^*$. Since $g_\lambda(u)$ is a quadratic function. In the view of Lemma 2.2 and 2.3, we collect all those β's for which $D_\beta(g_\lambda(u))$ is constant.

Now,

$$\begin{aligned} D_\beta(g_\lambda(u)) &= g_\lambda(u+\beta) + g_\lambda(u) \\ &= Tr_1^n(\lambda(\alpha(u+\beta)^{2^{2s}+2^s} + \alpha^{2^s}(u+\beta)^{2^{2s}+1} + \alpha^{2^{2s}}(u+\beta)^{2^s+1})) \\ &\quad +Tr_1^n(\lambda(\alpha u^{2^{2s}+2^s} + \alpha^{2^s}u^{2^{2s}+1} + \alpha^{2^{2s}}u^{2^s+1})) \\ &= Tr_1^n(\lambda((\alpha\beta^{2^s} + \alpha^{2^s}\beta)u^{2^{2s}} + (\alpha\beta^{2^{2s}} + \alpha^{2^{2s}}\beta)u^{2^s} \\ &\quad +(\alpha^{2^s}\beta^{2^{2s}} + \alpha^{2^{2s}}\beta^{2^s})u)) \\ &\quad +Tr_1^n(\lambda(\alpha\beta^{2^{2s}+2^s} + \alpha^{2^s}\beta^{2^{2s}+1} + \alpha^{2^{2s}\beta^{2^s+1}})). \end{aligned}$$

Since $u, \alpha, \beta \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^s}^*$. Using $u^{2^n} = u, \alpha^{2^n} = \alpha, \beta^{2^n} = \beta, \lambda^{2^n} = \lambda$, we get

$$\begin{aligned} D_\beta(g_\lambda(u)) &= Tr_1^n(\lambda u((\alpha^{2^{5s}} + \alpha^{2^s})\beta^{2^{6s}} + \alpha^{2^{6s}}\beta^{2^{5s}} + \alpha^{2^s}\beta^{2^{2s}} + (\alpha^{2^{6s}} + \alpha^{2^{2s}})\beta^{2^s})) \\ &\quad + Tr_1^n(\lambda(\alpha\beta^{2^{2s}+2^s} + \alpha^{2^s}\beta^{2^{2s}+1} + \alpha^{2^{2s}\beta^{2^s+1}})). \end{aligned}$$

Clearly, $D_\beta(g_\lambda(u))$ is equal to the constant if and only if

$$(\alpha^{2^{5s}} + \alpha^{2^s})\beta^{2^{6s}} + \alpha^{2^{6s}}\beta^{2^{5s}} + \alpha^{2^s}\beta^{2^{2s}} + (\alpha^{2^{6s}} + \alpha^{2^{2s}})\beta^{2^s} = 0.$$

Raising power 2^{-s}th, we have

$$(\alpha^{2^{4s}} + \alpha)\beta^{2^{5s}} + \alpha^{2^{5s}}\beta^{2^{4s}} + \alpha\beta^{2^s} + (\alpha^{2^{5s}} + \alpha^{2^s})\beta = 0, \tag{3.1}$$

which is a 2^s-polynomial. The polynomial $L(u) = \sum_{i=0}^{n} a_i x^{q^i}$ with $a_i \in \mathbb{F}_{q^m},\ m > 1$ is q polynomial over $\mathbb{F}_{q^m}$. Let

$$M(\beta) = (\alpha^{2^{4s}} + \alpha)\beta^{2^{5s}} + \alpha^{2^{5s}}\beta^{2^{4s}} + \alpha\beta^{2^s} + (\alpha^{2^{5s}} + \alpha^{2^s})\beta.$$

The dimension of kernel of $M(\beta)$ is $lr, l = 0, 1, 4, 5$.

Now, quadratic form from $\mathbb{F}_{q^5}$ to $\mathbb{F}_q \quad (q = 2^s)$ is

$$R(u) = Tr_E^L(\lambda(\alpha u^{2^{2s}+2^s} + \alpha^{2^s} u^{2^{2s}+1} + \alpha^{2^{2s}u^{2^s+1}})),$$

where $L = \mathbb{F}_{2^{7s}}$ and $E = \mathbb{F}_{2^s}$ The roots of $M(u)$ forms kernel of $R(u)$. In fact, kernel of $R(u)$ is the collection of β's where $B(u) = 0\ \forall\ u$ with

$$B(u) = R(u) + R(\beta) + R(u + \beta).$$

Since $D_b(G_\lambda(x)) = Tr_{\mathbb{F}_2}^E(B(u))$, we get

$$B(u) = Tr_E^L(u(M(\beta))).$$

Thus, $R(u)$ and $M(u)$ have same kernel. According to Lemma 2.1, $R(u)$ has dimension of its kernel either 1 or 5 which implies either s or $5s$ is one of the root of $M(u)$. Hence the dimension of the kernel of bilinear form of $D_\alpha(\phi_\lambda(u))$ is either s or $5s$. ■

Theorem 3.2. Let $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ and $n = 7s$. Then

$$nl_2(\phi_\lambda(u)) \geq 2^{7s-1} - 2^{2s-1}\sqrt{2^s(2^{6s} + 2^{3s} - 1)}.$$

Proof. From Theorem 3.1, dimension k of kernel of bilinear of $D_a(\phi_\lambda(u))$ is either s or $5s$. The nonlinearity of $D_\alpha(\phi_\lambda(u))$ i.e., $nl(D_\alpha(\phi_\lambda(u)))$ is either $2^{n-1} - \frac{1}{2}2^{\frac{n+s}{2}}$ or $2^{n-1} - \frac{1}{2}2^{\frac{n+5s}{2}}$. Therefore, we have

$$\max_{\alpha \in \mathbb{F}_{2^n}} nl(D_\alpha(\phi_\lambda(u))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+s}{2}}.$$

Now, Lemma 2.5 implies that

$$\begin{aligned} nl_2(\phi_\lambda(u)) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{\alpha\in\mathbb{F}_{2^n}} nl(D_\alpha\phi_\lambda(u))} \\ &= 2^{7s-1} - \frac{1}{2}\sqrt{2^{14s} - 2(2^{7s} - 2^s)(2^{7s-1} - 2^{4s-1})} \\ &= 2^{7s-1} - 2^{2s-1}\sqrt{2^s(2^{6s} + 2^{3s} - 1)}. \end{aligned}$$

Hence the result. ■

Now with the help of Lemma 2.6, we improve the above results in the following theorem.

Theorem 3.3. Let $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ and $n = 7s$. Then

$$nl_2(\phi_\lambda(u)) \geq 2^{7s-1} - 2^{\frac{22s-4}{4}}.$$

Proof. From Theorem 3.2, we have

$$\max_{\alpha\in\mathbb{F}_{2^n}} nl(D_\alpha(\phi_\lambda(u))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+s}{2}}.$$

On comparing the above equation with equation (2.1), we get $L = 1$ and $\theta = \dfrac{n+s-2}{2}$. Thus, by (2.2), we obtain

$$\begin{aligned} nl_2(\phi_\lambda(u)) &\geq 2^{n-1} - 2^{\frac{3n+s-4}{4}} \\ &= 2^{7s-1} - 2^{\frac{22s-4}{4}}. \end{aligned}$$

■

3.1. Lower bounds of 4th-order nonlinearity for monomial partial spread on 10-variables

The monomial functions of the form $f_\lambda(x) = Tr_1^n(\lambda x^{2^{\frac{n}{2}}-1})$, where $\lambda \in \mathbb{F}_{2^n}$ are called monomial partial spreads on n-variables. For some values of λ these functions becomes PS^- type bent functions. For details we may refer to [2, 7]. Dillon [7] has introduced an important class of Boolean functions called partial spreads. Suppose $f \in \mathcal{B}_n$, $n = 2t$. Consider a set $\{H_i : i = 1, \ldots, M\}$ of subspaces of $\mathbb{F}_{2^n}$ of dimension t, with $H_i \cap H_j = \{0\}$, when $i \neq j$. The function f with

$$supp(f) = \cup_{i=0}^{M} H_i$$

is called a partial spreads (PS).

In the following theorem, we obtain lower bound for 4th order nonlinearity of monomial partial spreads on 10-variables: $\phi(u) = Tr_1^{10}(\lambda u^{2^{\frac{10}{2}}-1}) = Tr_1^n(\lambda u^{31})$.

Theorem 3.4. Let $\phi(u) = Tr_1^{10}(\lambda u^{2^{\frac{10}{2}}-1})$, for all $u \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$. Then, we have

$$nl_4(\phi_\lambda) \geq 43.$$

Proof. The derivative $D_\alpha\phi_\lambda$ of ϕ_λ along $\alpha \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_\alpha\phi_\lambda(u) &= \phi_\lambda(u+\alpha)+\phi_\lambda(u) \\ &= Tr_1^n(\lambda(u+\alpha)^{2^4+2^3+2^2+2+1}) + Tr_1^n(\lambda u^{2^4+2^3+2^2+2+1}) \\ &= Tr_1^n(\lambda(\alpha u^{2^4+2^3+2^2+2} + \alpha^{2^4}u^{2^3+2^2+2+1} + \alpha^{2^3}u^{2^4+2^2+2+1} + \alpha^{2^2}u^{2^4+2^3+2+1} \\ &\quad +\alpha^2 u^{2^4+2^3+2^2+1})) + c(u), \end{aligned}$$

where $c(u)$ is cubic function. The second derivative $D_\beta D_\alpha\phi_\lambda$ of ϕ_λ along $\beta \in \mathbb{F}_{2^n}^*$ ($\alpha \neq \beta$) is

$$\begin{aligned} D_\beta D_\alpha\phi_\lambda(u) &= \phi_\lambda(u+\alpha+\beta)+\phi_\lambda(u+\alpha)+\phi_\lambda(u+\beta)+\phi_\lambda(u) \\ &= Tr_1^n[\lambda((\alpha\beta^2+\beta\alpha^2)u^{2^4+2^3+2^2} + (\alpha\beta^{2^4}+\beta\alpha^{2^4})u^{2^3+2^2+2} \\ &\quad +(\alpha\beta^{2^3}+\beta\alpha^{2^3})u^{2^3+2^2+2} + (\alpha\beta^{2^2}+\beta\alpha^{2^2})u^{2^4+2^3+2} \\ &\quad +(\alpha^{2^2}\beta^2+\alpha^2\beta^{2^2})u^{2^4+2^3+1} + (\alpha^{2^3}\beta^2+\alpha^2\beta^{2^3})u^{2^4+2^2+1} \\ &\quad +(\alpha^{2^3}\beta^{2^2}+\alpha^{2^2}\beta^{2^3})u^{2^4+2+1} + (\alpha^{2^4}\beta^2+\alpha^2\beta^{2^4})u^{2^3+2^2+1} \\ &\quad +(\alpha^{2^4}\beta^{2^k}+\alpha^{2^k}\beta^{2^4})u^{2^3+2+1} + (\alpha^{2^4}\beta^{2^3}+\alpha^{2^3}\beta^{2^4})u^{2^2+2+1})] + q(u), \end{aligned}$$

where $q(u)$ is a quadratic function. The third derivative $D_\gamma(D_\beta D_\alpha\phi_\lambda)$ of ϕ_λ along $\gamma \in \mathbb{F}_{2^n}^*$ ($\alpha \neq \gamma,\ \beta \neq \gamma$) is

$$\begin{aligned} &D_\gamma(D_\beta D_\alpha\phi_\lambda(u)) \\ &= \phi_\lambda(u+\beta+\alpha+\gamma)+\phi_\lambda(u+\beta+\alpha)+\phi_\lambda(u+\alpha+\gamma)+\phi_\lambda(u+\alpha) \\ &\quad +\phi_\lambda(u+\beta+\gamma)+\phi_\lambda(u+\beta)+\phi_\lambda(u+\gamma)+\phi_\lambda(u) \\ &= Tr_1^n[\lambda((\alpha\beta^2\gamma^{2^2}+\beta\alpha^2\gamma^{2^2}+\alpha\beta^{2^2}\gamma^2+\beta\alpha^{2^2}\gamma^2+\alpha^{2^2}\beta^2\gamma+\alpha^2\beta^{2^2}\gamma)u^{2^4+2^3} \\ &\quad +(\alpha\beta^{2^4}\gamma^{2^3}+\beta\alpha^2\gamma^{2^3}+\alpha\beta^{2^3}\gamma^{2^4}+\beta\alpha^{2^3}\gamma^2+\alpha^{2^3}\beta^2\gamma+\alpha^2\beta^{2^3}\gamma)u^{2^4+2^2} \\ &\quad +(\alpha\beta^{2^3}\gamma^{2^2}+\alpha^{2^3}\beta\gamma^{2^2}+\alpha\beta^{2^2}\gamma^{2^3}+\alpha^{2^2}\beta\gamma^{2^3}+\alpha^{2^3}\beta^{2^2}\gamma+\alpha^{2^2}\beta^{2^3}\gamma)u^{2^4+2} \\ &\quad +(\alpha\beta^2\gamma^{2^4}+\alpha^2\beta\gamma^{2^4}+\alpha\beta^{2^4}\gamma^2+\alpha^{2^4}\beta\gamma^2+\alpha^{2^4}\beta^2\gamma+\alpha^2\beta^{2^4}\gamma)u^{2^3+2^2} \\ &\quad +(\alpha\beta^{2^2}\gamma^{2^4}+\alpha^{2^2}\beta\gamma^{2^4}+\alpha\beta^{2^4}\gamma^{2^2}+\alpha^{2^4}\beta\gamma^{2^2}+\alpha^{2^4}\beta^{2^2}\gamma+\alpha^{2^2}\beta^{2^4}\gamma)u^{2^3+2} \\ &\quad +(\alpha\beta^{2^4}\gamma^{2^3}+\alpha^{2^4}\beta\gamma^{2^3}+\alpha\beta^{2^3}\gamma^{2^4}+\alpha^{2^3}\beta\gamma^{2^4}+\alpha^{2^4}\beta^{2^3}\gamma+\alpha^{2^3}\beta^{2^4}\gamma)u^{2^2+2} \\ &\quad +(\alpha^{2^2}\beta^2\gamma^{2^3}+\alpha^2\beta^{2^2}\gamma^{2^3}+\alpha^{2^3}\beta^2\gamma^{2^2}+\alpha^2\beta^{2^3}\gamma^{2^2}+\alpha^{2^3}\beta^{2^2}\gamma^2 \\ &\quad +\alpha^{2^2}\beta^{2^3}\gamma^2)u^{2^4+1} + (\alpha^{2^2}\beta^2\gamma^{2^4}+\alpha^2\beta^{2^2}\gamma^{2^4}+\alpha^{2^4}\beta^2\gamma^{2^2}+\alpha^2\beta^{2^4}\gamma^{2^2} \\ &\quad +\alpha^{2^4}\beta^{2^2}\gamma^2+\alpha^{2^2}\beta^{2^4}\gamma^2)u^{2^3+1} + (\alpha^{2^3}\beta^2\gamma^{2^4}+\alpha^2\beta^{2^3}\gamma^{2^4}+\alpha^{2^4}\beta^2\gamma^{2^3} \\ &\quad +\alpha^2\beta^{2^4}\gamma^{2^3}+\alpha^{2^4}\beta^{2^3}\gamma^2+\alpha^{2^3}\beta^{2^4}\gamma^2)u^{2^2+1} + (\alpha^{2^3}\beta^{2^2}\gamma^{2^4}+\alpha^{2^2}\beta^{2^3}\gamma^{2^4} \\ &\quad +\alpha^{2^4}\beta^{2^2}\gamma^{2^3}+\alpha^{2^2}\beta^{2^4}\gamma^{2^3}+\alpha^{2^4}\beta^{2^3}\gamma^{2^2}+\alpha^{2^3}\beta^{2^4}\gamma^{2^2})u^{2+1})] + l(u). \end{aligned}$$

Since $D_\gamma(D_\beta D_\alpha \phi_\lambda(u))$ is quadratic. The WHS of $D_\gamma(D_\beta D_\alpha \phi_\lambda)$ is equivalent to the WHS of $h_\lambda(u)$ with

$$\begin{aligned}
h_\lambda(u) = Tr_1^n[\lambda((&\alpha\beta^2\gamma^{2^2} + \beta\alpha^2\gamma^{2^2} + \alpha\beta^{2^2}\gamma^2 + \beta\alpha^{2^2}\gamma^2 + \alpha^{2^2}\beta^2\gamma + \alpha^2\beta^{2^2}\gamma)u^{2^4+2^3} \\
&+(\alpha\beta^2\gamma^{2^3} + \beta\alpha^2\gamma^{2^3} + \alpha\beta^{2^3}\gamma^2 + \beta\alpha^{2^3}\gamma^2 + \alpha^{2^3}\beta^2\gamma + \alpha^2\beta^{2^3}\gamma)u^{2^4+2^2} \\
&+(\alpha\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta\gamma^{2^2} + \alpha\beta^{2^2}\gamma^{2^3} + \alpha^{2^2}\beta\gamma^{2^3} + \alpha^{2^3}\beta^{2^2}\gamma + \alpha^{2^2}\beta^{2^3}\gamma)u^{2^4+2} \\
&+(\alpha\beta^2\gamma^{2^4} + \alpha^2\beta\gamma^{2^4} + \alpha\beta^{2^4}\gamma^2 + \alpha^{2^4}\beta\gamma^2 + \alpha^{2^4}\beta^2\gamma + \alpha^2\beta^{2^4}\gamma)u^{2^3+2^2} \\
&+(\alpha\beta^{2^2}\gamma^{2^4} + \alpha^{2^2}\beta\gamma^{2^4} + \alpha\beta^{2^4}\gamma^{2^2} + \alpha^{2^4}\beta\gamma^{2^2} + \alpha^{2^4}\beta^{2^2}\gamma + \alpha^{2^2}\beta^{2^4}\gamma)u^{2^3+2} \\
&+(\alpha\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta\gamma^{2^3} + \alpha\beta^{2^3}\gamma^{2^4} + \alpha^{2^3}\beta\gamma^{2^4} + \alpha^{2^4}\beta^{2^3}\gamma + \alpha^{2^3}\beta^{2^4}\gamma)u^{2^2+2} \\
&+(\alpha^{2^2}\beta^2\gamma^{2^3} + \alpha^2\beta^{2^2}\gamma^{2^3} + \alpha^{2^3}\beta^2\gamma^{2^2} + \alpha^2\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta^{2^2}\gamma^2 + \alpha^{2^2}\beta^{2^3}\gamma^2)u^{2^4+1} \\
&+(\alpha^{2^2}\beta^2\gamma^{2^4} + \alpha^2\beta^{2^2}\gamma^{2^4} + \alpha^{2^4}\beta^2\gamma^{2^2} + \alpha^2\beta^{2^4}\gamma^{2^2} + \alpha^{2^4}\beta^{2^2}\gamma^2 + \alpha^{2^2}\beta^{2^4}\gamma^2)u^{2^3+1} \\
&+(\alpha^{2^3}\beta^2\gamma^{2^4} + \alpha^2\beta^{2^3}\gamma^{2^4} + \alpha^{2^4}\beta^2\gamma^{2^3} + \alpha^2\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta^{2^3}\gamma^2 + \alpha^{2^3}\beta^{2^4}\gamma^2)u^{2^2+1} \\
&+(\alpha^{2^3}\beta^{2^2}\gamma^{2^4} + \alpha^{2^2}\beta^{2^3}\gamma^{2^4} + \alpha^{2^4}\beta^{2^2}\gamma^{2^3} + \alpha^{2^2}\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta^{2^4}\gamma^{2^2})u^{2^2+1})].
\end{aligned}$$

Let $\mathcal{E}_{h_\lambda} = \{u \in \mathbb{F}_(2^n) : B(u, y) = 0 \text{ with } y \in \mathbb{F}_{2^n}\}$, where $B(u, y)$ is the bilinear form of h_λ is given by

$$\begin{aligned}
B(u, y) &= h_\lambda(0) + h_\lambda(u) + h_\lambda(u) + h_\lambda(u + y) \\
B(u, y) &= Tr_1^n[\lambda(y^{2^4}\{R_1u^{2^3} + R_2u^{2^2} + R_3u^2 + R_7u\} + y^{2^3}\{R_1u^{2^4} + R_4u^{2^2} \\
&\quad + R_5u^2 + R_8u\} + y^{2^2}\{R_2u^{2^4} + R_4u^{2^3} + R_6u^2 + R_9u\} + y^2\{R_3u^{2^4} \\
&\quad + R_5u^{2^3} + R_6u^{2^2} + R_{10}u\} + y\{R_7u^{2^4} + R_8u^{2^3} + R_9u^{2^2} + R_{10}u^2\})] \\
&= Tr_1^n(yP(u)),
\end{aligned}$$

where

$$\begin{aligned}
R_1 &= \alpha\beta^2\gamma^{2^2} + \beta\alpha^2\gamma^{2^2} + \alpha\beta^{2^2\gamma^2} + \beta\alpha^{2^2}\gamma^2 + \alpha^{2^2}\beta^2\gamma + \alpha^2\beta^{2^2}\gamma \\
R_2 &= \alpha\beta^2\gamma^{2^3} + \beta\alpha^2\gamma^{2^3} + \alpha\beta^{2^3}\gamma^2 + \beta\alpha^{2^3}\gamma^2 + \alpha^{2^3}\beta^2\gamma + \alpha^2\beta^{2^3}\gamma \\
R_3 &= \alpha\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta\gamma^{2^2} + \alpha\beta^{2^2}\gamma^{2^3} + \alpha^{2^2}\beta\gamma^{2^3} + \alpha^{2^3}\beta^{2^2}\gamma + \alpha^{2^2}\beta^{2^3}\gamma \\
R_4 &= \alpha\beta^2\gamma^{2^4} + \alpha^2\beta\gamma^{2^4} + \alpha\beta^{2^4}\gamma^2 + \alpha^{2^4}\beta\gamma^2 + \alpha^{2^4}\beta^2\gamma + \alpha^2\beta^{2^4}\gamma \\
R_5 &= \alpha\beta^{2^2}\gamma^{2^4} + \alpha^{2^2}\beta\gamma^{2^4} + \alpha\beta^{2^4}\gamma^{2^2} + \alpha^{2^4}\beta\gamma^{2^2} + \alpha^{2^4}\beta^{2^2}\gamma + \alpha^{2^2}\beta^{2^4}\gamma \\
R_6 &= \alpha\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta\gamma^{2^3} + \alpha\beta^{2^3}\gamma^{2^4} + \alpha^{2^3}\beta\gamma^{2^4} + \alpha^{2^4}\beta^{2^3}\gamma + \alpha^{2^3}\beta^{2^4}\gamma \\
R_7 &= \alpha^{2^2}\beta^2\gamma^{2^3} + \alpha^2\beta^{2^2}\gamma^{2^3} + \alpha^{2^3}\beta^2\gamma^{2^2} + \alpha^2\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta^{2^2}\gamma^2 + \alpha^{2^2}\beta^{2^3}\gamma^2 \\
R_8 &= \alpha^{2^2}\beta^2\gamma^{2^4} + \alpha^2\beta^{2^2}\gamma^{2^4} + \alpha^{2^4}\beta^2\gamma^{2^2} + \alpha^2\beta^{2^4}\gamma^{2^2} + \alpha^{2^4}\beta^{2^2}\gamma^2 + \alpha^{2^2}\beta^{2^4}\gamma^2 \\
R_9 &= \alpha^{2^3}\beta^2\gamma^{2^4} + \alpha^2\beta^{2^3}\gamma^{2^4} + \alpha^{2^4}\beta^2\gamma^{2^3} + \alpha^2\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta^{2^3}\gamma^2 + \alpha^{2^3}\beta^{2^4}\gamma^2 \\
R_{10} &= \alpha^{2^3}\beta^{2^2}\gamma^{2^4} + \alpha^{2^2}\beta^{2^3}\gamma^{2^4} + \alpha^{2^4}\beta^{2^2}\gamma^{2^3} + \alpha^{2^2}\beta^{2^4}\gamma^{2^3} + \alpha^{2^4}\beta^{2^3}\gamma^{2^2} + \alpha^{2^3}\beta^{2^4}\gamma^{2^2}
\end{aligned}$$

and

$$\begin{aligned}
P(u) &= (\lambda R_1u^{2^3} + \lambda R_2u^{2^2} + \lambda R_3u^2 + \lambda R_7u)^{2^{n-4}} \\
&\quad +(\lambda R_1u^{2^4} + \lambda R_4u^{2^2} + \lambda R_5u^2 + \lambda R_8u)^{2^{n-3}} \\
&\quad +(\lambda R_2u^{2^4} + \lambda R_4u^{2^3} + \lambda R_6u^2 + \lambda R_9u)^{2^{n-2}} \\
&\quad +(\lambda R_3u^{2^4} + \lambda R_5u^{2^3} + \lambda R_6u^{2^2} + \lambda R_{10}u)^{2^{n-1}} \\
&\quad +(\lambda R_7u^{2^4} + \lambda R_8u^{2^3} + \lambda R_9u^{2^2} + R_{10}u^2).
\end{aligned}$$

$$\begin{aligned}\text{Let } L_\lambda(u) &= (P(u))^{2^4} \\ &= \lambda(R_1x^{2^3}+R_2x^{2^2}+R_3x^2+R_7x)+\lambda^2[R_1^2x^{2^5}+R_4^2x^{2^3}+R_5^2x^{2^2}+R_8^2x^2] \\ &\quad +\lambda^{2^2}[R_2^{2^2}x^{2^6}+R_4^{2^2}x^{2^5}+R_6^{2^2}x^{2^3}+R_9^{2^2}x^{2^2}]+\lambda^{2^3}[R_3^{2^3}x^{2^7}+R_5^{2^3}x^{2^6}+R_6^{2^3}x^{2^5} \\ &\quad +R_{10}^{2^3}x^{2^3}]+\lambda^{2^4}[R_7^{2^4}x^{2^8}+R_8^{2^7}x^{2^7}+R_9^{2^7}x^{2^6}+R_{10}^{2^7}x^{2^5}].\end{aligned} \tag{3.2}$$

$L_{(\lambda)}(u)$ is a linearized polynomial in u. The degree of $L_{(\lambda)}(u)$ is at most 2^8, this implies that $k \leq 6$. The Walsh transform of $D_\gamma(D_\beta D_\alpha \phi_\lambda)$ at $\lambda \in \mathbb{F}_{2^{10}}$ is

$$W_{D_\gamma(D_\beta D_\alpha\phi_\lambda)}(\lambda) = 2^{\frac{10+k}{2}} \leq 2^{\frac{10+8}{2}}.$$

Therefore, the nonlinearity of $D_\beta D_\alpha \phi_\lambda$ is

$$\begin{aligned} nl(D_\gamma(D_\beta D_\alpha\phi_\lambda)) &= 2^9 - \frac{1}{2}\max_{\lambda\in\mathbb{F}_{2^{10}}}|W_{D_\gamma(D_\beta D_\alpha\phi_\lambda)}(\lambda)| \\ &\geq 2^9 - \frac{1}{2}2^{\frac{10+8}{2}} \\ &= 256.\end{aligned}$$

From Lemma 2.4, we conclude that the 4th order nonlinearity of ϕ_λ is

$$\begin{aligned} nl_4(\phi_\lambda) &\geq \frac{1}{2^3}\max_{\alpha,\beta,\gamma\in\mathbb{F}_{2^n}} nl(D_\alpha(D_\beta D_\alpha\phi_\lambda)) \\ &\geq \frac{1}{2^3}256.\end{aligned}$$

Hence,

$$nl_4(\phi_\lambda) \geq 32. \tag{3.3}$$

Also, $nl(D_\gamma(D_\beta D_\alpha\phi_\lambda)) \geq 256$, for all $\alpha, \beta, \gamma \in \mathbb{F}_{2^{10}}^*(\alpha \neq \beta \neq \gamma)$. So there is a scope to improve the bound obtained in (3.3). Lemma 2.5 implies that

$$\begin{aligned} nl_4(\phi_\lambda) &\geq 2^{10-1} - \frac{1}{2}\sqrt{\sum_{\gamma\in\mathbb{F}_{2^{10}}}\sqrt{\sum_{\beta\in\mathbb{F}_{2^{10}}}\sqrt{2^{20}-2\sum_{\alpha\in\mathbb{F}_{2^{10}}} nl(D_\beta D_\alpha\phi_\lambda)}}} \\ &= 2^9 - \frac{1}{2}\sqrt{(2^{10}-1)\sqrt{(2^{10}-2)\sqrt{2^{20}-2\cdot(2^{10}-3).256}}} \\ &= 2^9 - \frac{1}{2}\sqrt{880665.9046} \\ &= 43.\end{aligned}$$

■

4. Conclusion

The comparison of the results obtained in Theorem 3.3 with the results given by Iwata-kurosawa [13], Singh [18] and general bounds i.e., $nl_2(\phi) \geq 2^{n-3}$ [4] is provided in Table 1. It is observed that the results given by us in Theorem 3.3 are better than those given in [4, 13, 18].

Table 1: Comparison of results in Theorem 3.3 with the results obtained in [4, 13, 18] for $n = 7s$

n,s	14,2	21,3	28,4	35,5	42,6
Bounds in Theorem 3.3	7168	1002235	13.21×10^7	1708.49×10^7	2194.72×10^9
Bounds by Singh [18]	–	955894	–	–	21.81×10^9
Bounds by Iwata-kurosawa [13]	3072	393216	5.03×10^5	6.44×10^7	8.24×10^9
General bounds by Carlet [4]	2048	262144	3.35×10^5	4.29×10^7	5.49×10^9

Since there is always need of functions having good cryptographic properties, in particular, functions with good higher order nonlinearities are employed to prevent higher order approximation attacks. Therefore, we expect that the results in this paper will help in selecting good cryptographic functions.

Acknowledgement

The second author thanks to UGC, India for providing financial support through "Rajiv Gandhi National Fellowship".

References

[1] Biham, E., and Shamir, A., 1991, "Differential cryptyanalysis of DES-like cryptosystems," In Advances in cryptography CRYPTO 1990, Lecture Notes in Computer Science, Springer-Verlag, Vol. 537, pp. 2–21.

[2] Canteaut, A., Charpin, P., and Kyureghyan, G., 2008, "A new class of monomial bent functions," Finite Fields and Their Applications, Vol. 14, pp. 221–241.

[3] Carlet, C., 2006 "On the higher order nonlinearities of algebraic immune functions," In CRYPTO 2006, Lecture Notes in Computer Science, Springer-Verlag, Vol. 4117, pp. 584–601.

[4] Carlet, C., 2008, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," IEEE Trans. Inform. Theory, Vol. 54 (3), pp. 1262–1272.

[5] Carlet, C., Dalai, D. K., Gupta, K. C., and Maitra, S., 2006, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and Construction," IEEE Trans. Inform. Theory, Vol. 52 (7), pp. 3105–3121.

[6] Caret, C., and Mesnager, S., 2007, "Improving the upper bounds on the covering radii of binary Reed-Muller codes," IEEE Trans. Inform Theory, Vol. 53 (1), pp. 162–173.

[7] Dillon, J. F., 1974 Elementary Hadamard Difference sets, PhD Thesis, University of Maryland.

[8] Fourquet, R. and Tavernier, C., 2008, "An improved list decoding algorithm for the second order ReedMuller codes and its applications," Des. Codes Cryptogr., Vol. 49, pp. 323–340.

[9] Gode, R., and Gangopadhyay, S., "On second order nonlinearities of cubic monomial Boolean functions," In cryptography ePrint Archive, http://ePrint.iacr.org/2009/502.pdf.

[10] Gode R. and Gangopadhyay S., 2010, "Third-order nonlinearities of a subclass of Kasami functions," Cryptography and Communications - Discrete Structures, Boolean functions and Sequences, Vol. 2, pp. 69–83.

[11] Gode, R. and Gangopadhyay, S., 2010, "On higher-order nonlinearity of monomial partial-spreads type Boolean functions," Journal of Combinatorics, Information and System Sciences, Vol. 35, pp. 341–360.

[12] Golić, J., 1996, " Fast low order approximation of cryptographic functions," In proceedings of the EUROCRYPT 1996, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1070, pp. 268–282.

[13] Iwata, T., and kurosawa, K., 1999, "Probabilistic higher order differential attack and higher order bent functions," In Proceedings of the ASIACRYPT 1999, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1716, pp. 62–74.

[14] Li, X., Hu, Y. and Gao, J., 2011, "Lower bounds on the second-order nonlinearity of Boolean functions," Int'l. Journal of Found. of Computer Science, Vol. 22 (6), pp. 1331–1349.

[15] Lidl, R. and Niederreiter, H., 1994, Introduction to Finite Fields and Their Applications, Cambridge University Press.

[16] MacWilliams, F. J., and Sloane, N. J. A., 1977, The Theory of Error Correcting Codes, North-Holland, Amsterdam.

[17] Rothaus, O. S., 1976, "On bent functions," J. Combi. Theory, Ser. A, Vol. 20, pp. 300–305.

[18] Singh, D., 2011, "Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions," International Journal of Computer Science and Information Technologies, Vol. 2(2), pp. 786–791.

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

[20] Sun, G. and Wu C., 2011, "The lower bound on the second order nonlinearity of a class of Boolean functions with high nonlinearity, AAECC, Vol. 22(1), pp. 37–45.