Improved lower bounds on higher order nonlinearity

Deep Singh & Amit Paul

Department of Mathematics,
Central University of Jammu, Samba, India

Abstract

The higher order nonlinearity of Boolean functions is an important cryptographic criterion concerning the security of cryptosystems. In this article, we compute lower bounds of 2nd order nonlinearity for a class of Boolean function $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ for a general case $n = qs$ with $q > 2$ and s are positive integer. Also, we improved the lower bounds on rth order nonlinearity for monomial partial spreads $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{\frac{n}{2}}-1})$ for all $u \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$ and Kasami Boolean function $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{2r}-2^r+1})$ with $\gcd(r, n) = 1$, where $u \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_{2^n}$.

Subject class [2010]:42C15; 42C30; 42C40.

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 variables. 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 and is important for prevention of affine approximation attacks [1, 13, 14]. The best upper bound on $nl_r(\phi)$ in [6] is asymptotically equivalent to

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

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. Carlet et al. [5] 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 [12, 16, 21, 22] have obtained the lower bounds on the 2nd order nonlinearities for some functions. Furhter, the lower bounds on 3rd order nonlinearities for some classes of functions have obtained in [11, 20].

In this article, we compute lower bounds of 2nd order nonlinearity for a class of Boolean function $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ with $p = 2^{2s} + 2^s + 1$, $\lambda \in \mathbb{F}_{2^s}^*$ for a general case $n = qs$, where $q > 2$ and s are positive integer. Also, we improved the lower bounds on the rth order nonlinearity for monomial partial spreads $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{\frac{n}{2}}-1})$ for all $u \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$ and Kasami Boolean function $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{2r}-2^r+1})$ with $\gcd(r, n) = 1$, where $u \in \mathbb{F}_{2^n},\ \lambda \in \mathbb{F}_{2^n}$.

2 Preliminaries

Let $\mathbb{F}_{2^n}$ be the n degree extension field of $\mathbb{F}_2$. Let $\mathbb{F}_{2^n}^*$ denotes the set of all units of $\mathbb{F}_{2^n}$. 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 $\kappa, h \in \mathcal{B}_n$ is $d(\kappa, h) = |\{\alpha \in \mathbb{F}_{2^n} : \kappa(\alpha) \neq h(\alpha)\}|$. The algebraic normal form of $\phi \in \mathcal{B}_n$ is

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

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 $Tr_t^n(u) = u + u^{2^t} + u^{2^{2t}} + ... + u^{2^{(n-1)t}}$ is called a trace function. For $t = 1$, $Tr_1^n(u) = u + u^2 + u^{2^2} + ... + u^{2^{n-1}}$ 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 $W = \langle v_1, ..., v_m \rangle$ is a t-dimensional subspace in $\mathbb{F}_{2^n}$ then $D_W \phi(u) = D_{v_1} ... D_{v_m} \phi(u)$, for all $u \in \mathbb{F}_{2^n}$ is t-th order derivative of ϕ along W.

The Walsh-Hadamard Transform (WHT) 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 nonlinearity of $\phi \in \mathcal{B}_n$ in terms of WHT is as follows

$$nl(\phi) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_\phi(\alpha)|. \tag{2.1}$$

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* [19] and exists only for n even. In 1976, Rothaus proved that for even n maximum possible nonlinearity of n-variable Boolean functions is $2^{n-1} - 2^{\frac{n}{2}-1}$ [19].

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

1. $Q(mu) = m^2Q(u)\ \forall\ m \in \mathbb{F}_q,\ u \in W$.
2. $B(u, v) = Q(0) + Q(u) + Q(v) + Q(u + v)$ 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 $\mathbb{F}_q$ a field of characteristic 2 and W is a vector space of dimension n over $\mathbb{F}_q$. 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. *[18] If $\phi \in \mathcal{B}_n$ is quadratic, then the WHT of ϕ is only linked with the dimension of 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, Corollary 2] Suppose $r < n$ and $\phi \in \mathcal{B}_n$. Also, suppose for some nonnegative integers L and θ, and for $0 \neq \alpha \in \mathbb{F}_{2^n}$,*

$$nl_{r-1}(D_\alpha\phi) \geq 2^{n-1} - L2^\theta. \tag{2.2}$$

Then

$$\begin{aligned} nl_r(\phi) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)L2^{\theta+1}+2^n} \\ &\approx 2^{n-1} - \sqrt{L}2^{\frac{n+\theta-1}{2}}. \end{aligned} \tag{2.3}$$

Lemma 2.7. *[10] Suppose* $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{\frac{n}{2}}-1})$, *for all* $u \in \mathbb{F}_{2^n}$ *and* $\lambda \in \mathbb{F}_{2^n}^*$. *Then,*

$$nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(\frac{n}{2}-2)}}(\phi_\lambda(u))) \geq 2^{n-1} - 2^{n-2} = 2^{n-2}.$$

Lemma 2.8. *[9] Let* $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{2r}-2^r+1})$ *with* $\gcd(r,n) = 1$, *where* $u \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_{2^n}^*$. *Then*

$$nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(r-1)}}(\phi_\lambda)) \geq \begin{cases} 2^{n-1} - 2^{\frac{n+4r-4}{2}}, & \text{if } n \text{ is even} \\ 2^{n-1} - 2^{\frac{n+4r-5}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

3 Main results

This section presents the lower bounds on rth order nonlinearity of some Boolean functions. Theorem 3.1 below computes the nonlinearity of 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 $n = qs$, where $q > 2$ and s are positive integer.

Theorem 3.1. *Let* $\phi_\lambda(u) = Tr_1^n(\lambda u^p)$ *with* $p = 2^{2s}+2^s+1$, $\lambda \in \mathbb{F}_{2^s}^*$ *and* $n = qs$, $q > 2$ *and* s *are positive integer. Then*

$$\max_{\alpha \in \mathbb{F}_{2^n}} nl(D_\alpha \phi_\lambda(u)) = \begin{cases} 2^{n-1} - 2^{\frac{(q-2)s+n-2}{2}}, & \text{if } q \text{ is even} \\ 2^{n-1} - 2^{\frac{n+s-2}{2}}, & \text{if } q \text{ is odd.} \end{cases}$$

Proof. The derivative of $\phi_\lambda(u)$ 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 removing linear and constant terms $D_\alpha\phi_\lambda(u)$ as

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

or

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

Since $2^{2s}+1$ and 2^s+1 belongs to different cyclotomic cosets. So, $g_\lambda(u) \neq 0$ for any $\alpha \in \mathbb{F}_{2^n}^*$. Also, $g_\lambda(u)$ 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,

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

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

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

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

$$(\alpha^{2^{(q-2)s}}+\alpha^{2^s})\beta^{2^{(q-1)s}}+\alpha^{2^{(q-1)s}}\beta^{2^{(q-2)s}}+\alpha^{2^s}\beta^{2^{2s}}+(\alpha^{2^{(q-1)s}}+\alpha^{2^{2s}})\beta^{2^s}=0.$$

Raising power 2^{-s}, we have

$$(\alpha^{2^{(q-3)s}}+\alpha)\beta^{2^{(q-2)s}}+\alpha^{2^{(q-2)s}}\beta^{2^{(q-3)s}}+\alpha\beta^{2^s}+(\alpha^{2^{(q-2)s}}+\alpha^{2^s})\beta=0 \tag{3.1}$$

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

$$M(\beta)=(\alpha^{2^{(q-3)s}}+\alpha)\beta^{2^{(q-2)s}}+\alpha^{2^{(q-2)s}}\beta^{2^{(q-3)s}}+\alpha\beta^{2^s}+(\alpha^{2^{(q-2)s}}+\alpha^{2^s})\beta.$$

The dimension of kernel of $M(\beta)$ is equal to lr, where $l=0,1,(q-3),(q-2)$
Now, quadratic form from $\mathbb{F}_{p^q}$ to $\mathbb{F}_p\quad(p=2^s)$ 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 $L=\mathbb{F}_{2^{qs}}$ and $E=\mathbb{F}_{2^s}$ The roots of $M(u)$ forms the kernel of $R(u)$. Infact the kernel of $R(u)$ is the set of all those β's where $Q(u)=0\ \forall\ u$ with

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

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

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

Thus, $R(u)$ and $M(u)$ have same kernel. According to Lemma 2.1, if q is even, the dimension k of kernel of $R(u)$ is either 0 or $(q-2)$ which implies that one root of $M(u)$ is either 0 or $(q-2)s$, i.e., the dimension k of kernel of bilinear form of $D_\alpha(\phi_\lambda(u))$ is either 0 or $(q-2)s$.

If q is odd, the dimension k of kernel of $R(u)$ is either 1 or $(q-2)$. Hence one root of $M(u)$ is either s or $(q-2)s$, i.e., the dimension k of kernel of bilinear form of $D_\alpha(\phi_\lambda(u))$ is either s or $(q-2)s$.

By Lemma 2.3 and (2.1), for q = even, the nonlinearity $nl(D_\alpha\phi_\lambda(u))$ is either 0 or $2^{n-1}-2^{\frac{(q-2)s+n-2}{2}}$, and for q = odd, the $nl(D_\alpha\phi_\lambda(u))$ is either $2^{n-1}-2^{\frac{n+s-2}{2}}$ or $2^{n-1}-2^{\frac{(q-2)s+n-2}{2}}$. Therefore, we have

$$\max_{\alpha\in\mathbb{F}_{2^n}} nl(D_\alpha\phi_\lambda(u)) = \begin{cases} 2^{n-1}-2^{\frac{(q-2)s+n-2}{2}}, & \text{if } q \text{ is even} \\ 2^{n-1}-2^{\frac{n+s-2}{2}}, & \text{if } q \text{ is odd.} \end{cases}$$

□

Now, the result below computes 2nd order nonlinearity for the functions discussed in Theorem 3.1.

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 $n = qs$, where $q > 2$ and s are positive integer. Then*

$$nl_2(\phi_\lambda) \geq \begin{cases} 2^{qs-1}-\frac{1}{2}\sqrt{2^{(2q-1)s}+2^{(q+1)s}-2^{qs}}, & \text{if } q \text{ is even} \\ 2^{qs-1}-\frac{1}{2}\sqrt{2^{\frac{(3q+1)s}{2}}-2^{\frac{(q+3)s}{2}}+2^{(q+1)s}}, & \text{if } q \text{ is odd.} \end{cases}$$

Proof.

- For q even, using Lemma 2.5 and Theorem 3.1, we get

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

- For q odd, we have $\max_{\alpha\in\mathbb{F}_{2^n}} nl(D_\alpha(\phi_\lambda(u))) = 2^{n-1}-2^{\frac{n+s-2}{2}}$. By using Lemma 2.5 and Theorem 3.1, we get

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

□

3.1 Improved higher order nonlinearity

The monomial functions of the form $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{\frac{n}{2}}-1})$, where $\lambda \in \mathbb{F}_{2^n}$ are called monomial partial spreads on n variables [7]. For some values of λ these functions becomes PS^- type bent functions. For details we refer to [2, 7]. Suppose $f \in \mathcal{B}_n,\ n = 2t$. Consider a set $\{H_i : i = 1, ..., M\}$ 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). The rth order nonlinearity of these functions is discussed in [10].

Theorem 3.3 below presents improved lower bounds on rth order nonlinearity for monomial partial spreads.

Theorem 3.3. *Let $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{\frac{n}{2}}-1})$, for all $u \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$. Then, we have*

$$nl_{(r=\frac{n}{2}-1)}(\phi_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(\frac{n}{2}-2))2^{n-2}}}}.$$

Proof. From Lemma 2.7, the first order nonlinearity of $D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(\frac{n}{2}-2)}}(\phi_\lambda(u))$ is

$$nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(\frac{n}{2}-2)}}(\phi_\lambda(u))) \geq 2^{n-1} - 2^{n-2} = 2^{n-2}.$$

So by using the Lemma 2.5, we have improved lower bounds on rth order nonlinearity as

$$nl_{(r=(\frac{n}{2}-1))}(\phi_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha_1\in\mathbb{F}_{2^n}}\sqrt{\sum_{\alpha_2\in\mathbb{F}_{2^n}}\cdots\sqrt{2^{2n}-2\sum_{\alpha_{(\frac{n}{2}-2)}\in\mathbb{F}_{2^n}} nl(D_{\alpha_1}\cdots D_{\alpha_{(\frac{n}{2}-2)}}\phi_\lambda(u))}}}$$

$$\geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha_1\in\mathbb{F}_{2^n}}\sqrt{\sum_{\alpha_2\in\mathbb{F}_{2^n}}\cdots\sqrt{2^{2n}-2\sum_{\alpha_{(\frac{n}{2}-2)}\in\mathbb{F}_{2^n}} 2^{n-2}}}}$$

$$= 2^{n-1} - \tfrac{1}{2}\sqrt{2^n - 1\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(\tfrac{n}{2}-2))2^{n-2}}}}.$$

□

The monomial functions of the form $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{2r}-2^r+1})$ for a fixed coefficient $\lambda \in \mathbb{F}_{2^n}$ with $\gcd(r, n) = 1$, $1 \leq r < n$ are called Kasami Boolean functions. The exponent k is known as *Kasami exponent* [15]. For these functions, the bounds on rth order nonlinearity were discussed in [9].

Theorem 3.4 below presents improved lower bounds on rth order nonlinearity for Kasami functions.

Theorem 3.4. *Let* $\phi_\lambda(u) = Tr_1^n(\lambda u^{2^{2r}-2^r+1})$ *such that* $\gcd(r,n)=1$, *where* $u \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_{2^n}$. *Then we have*

$$nl_r(\phi_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(r-1))(2^{n-1}-2^{\frac{n+4r-4}{2}})}}}, & \text{if } n \text{ is even} \\ 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(r-1))(2^{n-1}-2^{\frac{n+4r-5}{2}})}}}, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. From Lemma 2.8, we have

$$nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(r-1)}}(\phi_\lambda)) \geq \begin{cases} 2^{n-1} - 2^{\frac{n+4r-4}{2}}, & \text{if } n \text{ is even} \\ 2^{n-1} - 2^{\frac{n+4r-5}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Now using Lemma 2.5, we get

- For n even

$$nl_r(\phi_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha_1\in\mathbb{F}_{2^n}}\sqrt{\sum_{\alpha_2\in\mathbb{F}_{2^n}}\cdots\sqrt{2^{2n}-2\sum_{\alpha_{(n-3)}\in\mathbb{F}_{2^n}} nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(r-1)}}(\phi_\lambda))}}}$$

$$\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(r-1))(2^{n-1}-2^{\frac{n+4r-4}{2}})}}}.$$

- For n odd

$$nl_r(\phi_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\alpha_1\in\mathbb{F}_{2^n}}\sqrt{\sum_{\alpha_2\in\mathbb{F}_{2^n}}\cdots\sqrt{2^{2n}-2\sum_{\alpha_{(n-3)}\in\mathbb{F}_{2^n}} nl(D_{\alpha_1}D_{\alpha_2}...D_{\alpha_{(r-1)}}(\phi_\lambda))}}}$$

$$\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{(2^n-2)\cdots\sqrt{2^{2n}-2(2^n-(r-1))(2^{n-1}-2^{\frac{n+4r-5}{2}})}}}.$$

□

Tab. 1: Comparison of results in Theorem 3.3 with the results in [4, 10].

r, n	3, 8	4, 10	5, 12	6, 14	7, 16	8, 18	9, 20
Bounds of Theorem 3.3	21	43	87	176	354	709	1418
Carlet's general bounds [4]	-	-	64	128	256	512	1024
Bounds by Garg [10]	16	32	64	128	256	512	1024

Tab. 2: Comparison of results in Theorem 3.4 with the results in [4, 9, 14].

n	19	21	22	23	24	26
Bounds of Theorem 3.4 for r=5	11115	87028	174055	511176	1022352	5338629
Carlet's general bounds [4]	8192	32768	65536	131072	262144	1048576
Bounds by Garg [9]	8192	49152	98304	229376	458752	1966080
Iwata-kurosawa's bounds [14]	20480	81920	163840	327680	655360	2621440

4 Comparison

The comparison of results obtained in Theorem 3.3 and Theorem 3.4 is provided in Table 1 and Table 2. It is observed that the results in Theorem 3.3 are better than those in [4, 10]. Also, the results in Theorem 3.4 are better than those in [4, 9, 14]. Since there is always need of functions having good cryptographic properties. In particular, functions with good higher order nonlinearities are employed to prevent various higher order approximation attacks. Thus, we expect that the results in this article 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.: Differential cryptyanalysis of DES-like cryptosystems, In Advances in cryptography CRYPTO 1990, Lecture Notes in Computer Science, Springer-Verlag, Vol. 537, pp. 2-21, 1991.

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

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

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

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

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

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

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

[9] Garg M and Khalyavin A.: Higher-order nonlinearity of kasami functions, International Journal of Computer Mathematics, 89 (10):1311-1318, 2012.

[10] Garg M and Khalyavin A. Higher order-nonlinearities of two classes of boolean functions. International Journal of Computer Science and Information Technologies, 6 (5):4251-4256, 2015.

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

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

[13] Golić J.: 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, 1996.

[14] Iwata T. and kurosawa K.: 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, 1999.

[15] Kasami T.: The Weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, Information and Control, Vol. 18, pp. 369-394, 1971.

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

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

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

[19] Rothaus O. S.: On bent functions, J. Combi. Theory, Ser. A, Vol. 20, pp.300-305, 1976.

[20] Singh B. K.: On third-order nonlinearity of biquadratic monomial Boolean functions, International Journal of Engineering Mathematics, Vol. 2014, pp. 1-7, 2014.

[21] Singh D.: 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, 2011.

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