Some Classes of Cubic Monomial Boolean Functions with Good Second-Order Nonlinearities

Ruchi Telang Gode *

Abstract

It is well known that estimating a sharp lower bound on the second-order nonlinearity of a general class of cubic Boolean function is a difficult task. In this paper for a given integer $n \geq 4$, some values of s and t are determined for which cubic monomial Boolean functions of the form $h_\mu(x) = Tr(\mu x^{2^s+2^t+1})$ $(n > s > t \geq 1)$ possess good lower bounds on their second-order nonlinearity. The obtained functions are worth considering for securing symmetric cryptosystems against various quadratic approximation attacks and fast algebraic attacks.

Keywords: *Boolean function; Derivative of Boolean function; Second-order nonlinearity; Linearized polynomial*.

1 Introduction

Let $\mathbb{F}_2 = GF(2)$ be the prime field of characteristic 2. $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. The n degree extension field of $\mathbb{F}_2$ is denoted by $\mathbb{F}_{2^n}$.

Definition 1 *An n-variable Boolean function is the mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ or equivalently from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is said to be a Boolean function on n variables. , $\mathcal{B}_n$ denotes the set of all n-variable Boolean functions, $|\mathcal{B}_n| = 2^{2^n}$.*

A Boolean function $g \in \mathcal{B}_n$ can also be expressed as $g_\mu(x) = Tr_1^n(\mu x^s)$ for $\mu \in \mathbb{F}_{2^n}, s \in \mathbb{N}$, called a monomial Boolean function. Here, s is called the exponent of g and $\deg(g) = wt(s)$, which is the number of digits of s in base 2.

Definition 2 *The Walsh transform of $g \in \mathcal{B}_n$ is an integer valued function $W_g : \mathbb{F}_{2^n} \to [-2^n, 2^n]$ defined as*

$$W_g(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x)+Tr_1^n(\lambda x)}.$$

where $\lambda \in \mathbb{F}_{2^n}$ and $Tr_1^n(\lambda x)$ is the usual inner product of λ and x.

*Department of Mathematics, National Defence Academy Pune, India. Email: telang.ruchi82@gmail.com

Nonlinearity
High nonlinearity is an important combinatorial property of Boolean functions, for cryptographic applications we need functions with high nonlinearity so that they can not be well approximated using the affine ones and thus are optimally resistant to best affine approximation attacks .
Nonlineraity can be expressed in terms of Walsh spectrum as

$$nl(g) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_g(\lambda)|.$$

In case when n is odd the least upper bound of nonlinearity is not known.

Definition 3 *Suppose n is an even integer. A function $g \in \mathcal{B}_n$ is said to be a bent function if and only if it possesses maximum nonlinearity, i.e., $2^{n-1} - 2^{\frac{n}{2}-1}$.*

For a bent function $g \in \mathcal{B}_n$, it is clear that $W_g(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$.
Bent functions were first introduced by Rothaus in 1976 [13]. The rth-order ($r > 1$) nonlinearity of a Boolean function is the generalized concept of nonlinearity or first-order nonlinearity($r = 1$) .

Definition 4 *Suppose g is a Boolean function on n variables. For every integer r, $0 < r \leq n$, the minimum of the Hamming distances of g from all the functions belonging to $RM(r, n)$ is said to be the rth-order nonlinearity of the Boolean functions g. The sequence of values $nl_r(g)$, for r ranging from 1 to $n - 1$, is said to be the nonlinearity profile of g.*

Boolean function plays a prominent role in many fields of mathematics and computer science such as symmetric-key cryptosystems, coding theory etc. The second-order nonlinearity of a Boolean function is a parameter that relates to several known quadratic approximation attacks, fast algebraic and related attacks [8, 9, 12] on stream ciphers and block ciphers. It is also important in coding theory, since the maximal second-order nonlinearity of all Boolean functions on n variables equals the covering radius of the ReedMuller code $RM(2, n)$. Till date there is no work on estimating a sharp lower bound on the second-order nonlinearity of a general class of cubic Boolean function. Also as compare to first-order nonlinearity there is no known efficient algorithm to compute second-order nonlinearities of Boolean functions for large values of n; the most efficient algorithm works upto $n = 13$ for some particular functions only [4]. However Carlet [3] introduced a recursive method for determining the lower bounds of higher order nonlinearity and nonlinearity profile of Boolean functions. Sun and Wu [15] using the recursive techniques of Carlet [3] and multivariate method have obtained lower bounds on the second-order nonlinearities of some functions of form $Tr_1^n(x^d)$. Gode and Gangopadhyay [5] have found a lower bound on the second-order nonlinearities of the function $Tr_1^n(\mu x^{2^{2r}+2^r+1})$ when $\gcd(n, r) = 1$. Gangopadhyay et al [6] have found a lower bound on the second-order nonlinearities of the function $Tr_1^n(\mu x^{2^{2r}+2^r+1})$ for $n = 6r$, Garg and Gangopadhyay [7] for $n = 5r$, Singh [14]for $n = 3r$ and Sun and Wu [16] for $n = 4r$. Motivated by above, this paper is an attempt to search and construct the functions with better lower bounds on their second-order nonlinearities.
In this paper, a good theoretical lower bounds on the second-order nonlinearities of some subclasses of cubic Boolean functions of the form $h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1})$, $n > s > t \geq 1$, s, t

being positive integers is deduced. The technique is an attempt to find values of s and t for which h_μ has high second-order nonlinearity for a given n. Our bounds are applicable for all values of $n \geq 4$ and also give better results for larger values of s. The result thus help to choose Boolean functions that show tradeoffs between second-order nonlinearities and other cryptographic properties of Boolean functions and thus have direct implication in the development of symmetric key cryptosystems. The paper is organized as follows. In Section 2, some concepts and definitions are introduced which will be used throughout this paper. In Section 3 the known recursive lower bounds on higher order nonlinearities of Boolean functions introduced by Carlet [3] is discussed. In Section 4, a generalised theoretical improved lower bounds on the second-order nonlinearity of h_μ for all $n \geq 4$ is deduced. In Section 5, some approach regarding what values of s, t are to be chosen for a fix n to get a better lower bound on the second-order nonlinearity of h_μ is presented. Applying the results of the Section 4 and Section 5 an improved lower bound on many subclasses of h_μ is obtained, further Table 1 and Table 2 give lists of some subclasses with good bounds. In addition, Section 7 calculate the nonlinearity of some cubic functions of the class h_μ which have good bounds on second-order nonlinearity and thus give the nonlinearity profile of some functions from the class h_μ. Comparisons and concluding remarks are given in Section 6 and Section 8 respectively.

2 Preliminary results

Some preliminaries are provided in this Section.

2.1 Walsh Spectrum of quadratic Boolean functions

Suppose $g \in \mathcal{B}_n$ is a quadratic function. The bilinear form associated to g is defined by $B(x, y) = g(0) + g(x) + g(y) + g(x + y)$. The kernel of $B(x, y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

$$\mathcal{E}_g = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

The Walsh spectrum of any quadratic function $g \in \mathcal{B}_n$ is given below:

Lemma 1 ([2]) *If $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $B(x, y)$ is the bilinear form associated to it, then the Walsh Spectrum of g depends only on the dimension, k, of the kernel, $\mathcal{E}_g$, of $B(x, y)$. The weight distribution of the Walsh spectrum of g is:*

$W_g(\lambda)$	*number of* λ
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{g(0)}2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{g(0)}2^{(n-k-2)/2}$

It is a well known result that k and n have the same parity [2].

2.2 Linearised polynomials

Definition 5 ([10]) *Let $q = 2^t$ for some positive integer t. A polynomial of the form*

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

with the coefficients α_i in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is said to be a linearised polynomial over $\mathbb{F}_{q^m}$.

Following are the properties of $L(x)$.

1. The zeroes of $L(x)$ lie in some extension field $\mathbb{F}_{q^w}$ of $\mathbb{F}_{q^m}$, $w \geq m$ where $\mathbb{F}_{q^w}$ is regarded as a vector space over $\mathbb{F}_q$ and the zeroes form a subspace of $\mathbb{F}_{q^w}$.
2. $L(x)$ induces a linear operator on $\mathbb{F}_{q^w}$.
3. Each zero of $L(x)$ has the same multiplicity which is either 1 or a power of q.

Following is a result related to linearised polynomials.

Theorem 1 ([1]) *Let $\mathbb{F}_{2^n}$ be a cyclic extension of $\mathbb{F}_2$ of degree n, and suppose that σ generates the Galois group $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, where $\sigma = 2^p$ for some integer p such that $1 \leq p \leq n$ and $\gcd(p, n) = 1$. Let $c_0, c_1, \ldots, c_n$ be elements of $\mathbb{F}_{2^n}$, not all of them zero. Then the linearised polynomial $f(x)$ defined as*

$$f(x) = c_0 x + c_1 x^{\sigma} + c_2 x^{\sigma^2} + \ldots + c_n x^{\sigma^l}$$

has kernel with dimension at most l in $\mathbb{F}_{2^n}$.

3 Recursive lower bounds of higher-order nonlinearities

The recursive lower bounds of higher-order nonlinearities of Boolean functions, derived by Carlet [3], are dependent on the nonlinearities of their derivatives.

Definition 6 *The derivative of $g \in \mathcal{B}_n$ with respect to $c \in \mathbb{F}_{2^n}$, denoted by $D_c g$, is defined as $D_c g(x) = g(x) + g(x + c)$ for all $x \in \mathbb{F}_{2^n}$.*

The higher-order derivatives are defined as follows.

Definition 7 *Let $a_1, \ldots, a_m \in \mathbb{F}_{2^n}$ and V be the m-dimensional subspace of $\mathbb{F}_{2^n}$ generated by $a_1, \ldots, a_m$, i.e., $V = \langle a_1, \ldots, a_m \rangle$. The mth-order derivative of $g \in \mathcal{B}_n$ with respect to V, denoted by $D_V g$ or $D_{a_1} \ldots D_{a_m} g$, is defined by*

$$D_V g(x) = D_{a_1} \ldots D_{a_m} g(x) \text{ for all } x \in \mathbb{F}_{2^n}.$$

It is well known that the mth-order derivative of g depends only on the choice of the m-dimensional subspace V and is independent of the choice of the basis for V.

Proposition 1 ([3]) *Let g be any n-variable Boolean function and m be a positive integer smaller than n. We have*

$$nl_m(g) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in\mathbb{F}_{2^n}} nl_{r-1}(D_a g)}.$$

Particularly for $r = 2$, we have

$$nl_2(g) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in\mathbb{F}_{2^n}} nl(D_a g)}.$$

This proposition is useful in computing lower bounds of the higher order nonlinearities of Boolean functions.

Proposition 2 ([11], Chapter 15) *The rth-order nonlinearities of an n-variable Boolean function g with algebraic degree d are divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$. Here $\lceil b \rceil$ denotes the ceiling function of b.*

4 Main Result

Consider the general class of n variable cubic monomial Boolean functions of the form $h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1})$, where s, t are positive integers such that $s > t \geq 1$ and $\mu, x \in \mathbb{F}_{2^n}^*$. A lower bound on the second-order nonlinearity of $h_\mu(x)$ is found for all $n \geq 4$.

4.1 Upper bound on the Walsh Transform of $D_c h_\mu$

Theorem 2 *Let $h_\mu \in \mathcal{B}_n$ be given as $h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1})$, here s, t are positive integers such that $s > t \geq 1$ and $\mu, x \in \mathbb{F}_{2^n}^*$. then*

$$W_{D_c h_\mu}(\lambda) \leq \begin{cases} \min(2^{\frac{2n-2u}{2}}, 2^{\frac{n+\frac{2s}{a}}{2}}), & n \text{ and } \frac{2s}{a} \text{ have same parity,} \\ \min(2^{\frac{2n-2u}{2}}, 2^{\frac{n+\frac{2s}{a}-1}{2}}), & n \text{ and } \frac{2s}{a} \text{ have different parity.} \end{cases}$$

Here $a = \max\{d \in \mathbf{N} : d|s, t;\ \gcd(d, n) = 1\}$ and $u = \min(n - s, s - t, t)$.

Proof :First derivative, $D_c h_\mu,$ of h_μ with respect to $c \in \mathbb{F}_{2^n}^*$ given as

$$\begin{aligned} D_c h_\mu(x) &= h_\mu(x + c) + h_\mu(x) = Tr_1^n((x + c)^{2^s+2^t+1}) + Tr_1^n(x^{2^s+2^t+1}) \\ &= Tr_1^n(x^{2^s+2^t}c + x^{2^s+1}c^{2^t} + x^{2^t+1}c^{2^s} + x^{2^s}c^{2^t+1} + x^{2^t}c^{2^s+1} + xc^{2^s+2^t} + c^{2^s+2^t+1}). \end{aligned}$$

The Walsh Hadamard Spectrum of $D_c h_\mu$ is equivalent to the Walsh Hadamard Spectrum of $q(x)$, where $q(x)$ is the quadratic part of $D_c h_\mu$, given as

$$q(x) = Tr_1^n(x^{2^s+2^t}c + x^{2^s+1}c^{2^t} + x^{2^t+1}c^{2^s}).$$

Let $B(x,y)$ be the associated bilinear form corresponding to $q(x)$, which is defined as $B(x,y) = q(x+y) + q(x) + q(y) + q(0)$. The kernel $\mathcal{E}_q$ of $B(x,y)$ is defined as

$$\mathcal{E}_q = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\},$$

and let k denote the dimension of $\mathcal{E}_q$. Now,

$$\begin{aligned}
B(x,y) &= Tr_1^n(x^{2^s+2^t}c + x^{2^s+1}c^{2^t} + x^{2^t+1}c^{2^s}) + Tr(y^{2^s+2^t}c + y^{2^s+1}c^{2^t} + y^{2^t+1}c^{2^s}) \\
&\quad + Tr_1^n((x+y)^{2^s+2^t}c + (x+y)^{2^s+1}c^{2^t} + (x+y)^{2^t+1}c^{2^s}) \\
&= Tr_1^n(((xc^{2^t} + x^{2^t}c)y^{2^s} + (xc^{2^s} + x^{2^s}c)y^{2^t} + (x^{2^s}c^{2^t} + x^{2^t}c^{2^s})y)) \\
&= Tr_1^n((xc^{2^t} + x^{2^t}c)y^{2^s}) + Tr((xc^{2^s} + x^{2^s}c)y^{2^t}) + Tr_1^n((x^{2^s}c^{2^t} + x^{2^t}c^{2^s})y) \\
&= Tr((xc^{2^t} + x^{2^t}c)y^{2^s})^{2^{n-s}} + Tr((xc^{2^s} + x^{2^s}c)y^{2^t})^{2^{n-t}} + Tr_1^n((x^{2^s}c^{2^t} + x^{2^t}c^{2^s})y) \\
&= Tr_1^n((x^{2^{n-s}}c^{2^{n-s+t}} + x^{2^{n-s+t}}c^{2^{n-s}})y^{2^n}) + Tr_1^n((x^{2^{n-t}}c^{2^{n+s-t}} + x^{2^{n+s-t}}c^{2^{n-t}})y^{2^n}) \\
&\quad + Tr_1^n((x^{2^s}c^{2^t} + x^{2^t}c^{2^s})y) \\
&= Tr_1^n(y(x^{2^s}c^{2^t} + x^{2^t}c^{2^s} + x^{2^{s-t}}c^{2^{-t}} + x^{2^{-t}}c^{2^{s-t}} + x^{2^{-s}}c^{2^{t-s}} + x^{2^{t-s}}c^{2^{-s}})) \\
&= Tr_1^n(yP_c(x)).
\end{aligned}$$

Therefore, $\mathcal{E}_h = \{x \in \mathbb{F}_{2^n} : P_c(x) = 0\}$.
For a given n, $a = \max\{d \in \mathbf{N} : d|s,t;\ \gcd(d,n) = 1\}$ and $u = \min(n-s, s-t, t)$ we will show that the maximum degree of $P_c(x)$ is $\min(\frac{2s}{a}, \frac{2s}{a} - 1, n - 2u)$. Consider the following two cases:

Case 1: The size of the kernel $\mathcal{E}_q$ is same as the count of roots of $P_c(x)$, or identically to the count of roots of $(P_c(x))^{2s}$. Put $(P_c(x))^{2s} = \mathcal{Q}_c(x)$. Thus,

$$\begin{aligned}
P_c(x) &= x^{2^s}c^{2^t} + x^{2^t}c^{2^s} + x^{2^{s-t}}c^{2^{-t}} + x^{2^{-t}}c^{2^{s-t}} + x^{2^{t-s}}c^{2^{-s}} + x^{2^{-s}}c^{2^{t-s}} \qquad (1) \\
\mathcal{Q}_c(x) &= (x^{2^s}c^{2^t} + x^{2^t}c^{2^s} + x^{2^{s-t}}c^{2^{-t}} + x^{2^{-t}}c^{2^{s-t}} + x^{2^{t-s}}c^{2^{-s}} + x^{2^{-s}}c^{2^{t-s}})^{2^s}
\end{aligned}$$

Thus

$$\mathcal{Q}_c(x) = x^{2^{2s}}c^{2^{s+t}} + x^{2^{s+t}}c^{2^{2s}} + x^{2^{2s-t}}c^{2^{s-t}} + x^{2^{s-t}}c^{2^{2s-t}} + x^{2^t}c + xc^{2^t}. \qquad (2)$$

Let $a = \max\{d \in \mathbf{N} : d|s,t;\ \gcd(d,n) = 1\}$, then a divides all of $2s, s+t, 2s-t, s-t, t$. Thus

$$\mathcal{Q}_c(x) = x^{(2^a)^{\frac{2s}{a}}}c^{2^{s+t}} + x^{(2^a)^{\frac{s+t}{a}}}c^{2^{2s}} + x^{(2^a)^{\frac{2s-t}{a}}}c^{2^{s-t}} + x^{(2^a)^{\frac{s-t}{a}}}c^{2^{2s-t}} + x^{(2^a)^{\frac{t}{a}}}c + xc^{2^t}.$$

By Theorem 1 it is clear that $Q_c(x)$ is a σ polynomial of degree at most $2^{\frac{2s}{a}}$. Let k_1 be the dimension of kernel of $Q_c(x)$, since k_1 and n have same parity we have

$$k_1 \leq \begin{cases} \frac{2s}{a}, & n \text{ and } \frac{2s}{a} \text{ have same parity,} \\ \frac{2s}{a} - 1, & n \text{ and } \frac{2s}{a} \text{ have different parity.} \end{cases}$$

Next

Case 2: The linearised polynonial $P_c(x)$ as given in Equation (1) can also be written as

$$P_c(x) = x^{2^s}c^{2^t} + x^{2^t}c^{2^s} + x^{2^{s-t}}c^{2^{n-t}} + x^{2^{n-t}}c^{2^{s-t}} + x^{2^{n-(t-s)}}c^{2^{n-s}} + x^{2^{n-s}}c^{2^{n-(t-s)}}$$

It is obvious that $P_c(x)$ is a linearised polynomial of the form $(c_j x^{2^i} + c_j^{2^{n-i}} x^{2^{n-i}})$. Let $u = \min(n-s, s-t, t)$ and $v = \max(n-s, n-s+t, n-t)$. Then $P_c(x)$ can be expressed as $(L(x))^{2^u}$ for some linearised polynomial $L(x)$. Clearly $L(x)$ is a linearised polynomial of degree at most 2^{v-u}, as $v = n-u$ this implies $L(x)$ is a linearised polynomial of degree at most 2^{n-2u}. In this case dimension of the kernel of the bilinear form $B(x,y)$ is at most $n-2u$.

Thus combining the Case 1 and Case 2, we get dimension k of the kernel of the bilinear form $B(x,y)$ less than equal to the minimum of k_1 and $n-2u$, i.e.,

$$k \leq \begin{cases} \min(n-2u, \frac{2s}{a}), & n \text{ and } \frac{2s}{a} \text{ have same parity,} \\ \min(n-2u, \frac{2s}{a}-1), & n \text{ and } \frac{2s}{a} \text{ have different parity.} \end{cases}$$

Thus by Lemma 1,

$$W_{D_c h_\mu}(\lambda) \leq \begin{cases} \min(2^{\frac{2n-2u}{2}}, 2^{\frac{n+\frac{2s}{a}}{2}}), & n \text{ and } \frac{2s}{a} \text{ have same parity,} \\ \min(2^{\frac{2n-2u}{2}}, 2^{\frac{n+\frac{2s}{a}-1}{2}}), & n \text{ and } \frac{2s}{a} \text{ have different parity.} \end{cases}$$

■

4.2 Lower bounds on the Second-Order Nonlinearity of h_μ

Theorem 3 *Suppose $h_\mu \in \mathcal{B}_n$ is defined as*

$$h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1}) \text{ for all } x \in \mathbb{F}_{2^n}.$$

Here $n > s > t \geq 1$ are positive integers and $a = \max\{d \in \mathbf{N} : d|s,t; \gcd(d,n) = 1\}$ and $u = \min(n-s, s-t, t)$. Then for $4 \leq s < n$

1. *If n and $\frac{2s}{a}$ have same parity*

$$nl_2(h_\mu) \geq \max(2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{2n-u} - 2^{n-u}}, 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n}{2}+\frac{s}{a}} - 2^{\frac{n}{2}+\frac{s}{a}}})$$

2. *If n and $\frac{2s}{a}$ have different parity*

$$nl_2(h_\mu) \geq \max(2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{2n-u} - 2^{n-u}}, 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n-1}{2}+\frac{s}{a}} - 2^{\frac{n-1}{2}+\frac{s}{a}}})$$

Proof :The nonlinearity of derivative $D_c h_\mu$ of h_μ is given in terms of Walsh transform $W_{D_c h_\mu}(\lambda)$ as

$$nl(D_c h_\mu) = 2^{n-1} - \frac{1}{2}\max|W_{D_c h_\mu}(\lambda)|$$

for all $c \in \mathbb{F}_{2^n}^*$.

Substituting the bounds of $W_{D_c h_\mu}(\lambda)$ from Theorem 2 in above formula we obtain

$$nl(D_c h_\mu) \geq \begin{cases} \max(2^{n-1} - \frac{1}{2}2^{\frac{2n-2u}{2}}, 2^{n-1} - \frac{1}{2}2^{\frac{n+\frac{2s}{a}}{2}}), & n \text{ and } \frac{2s}{a} \text{ have same parity,} \\ \max(2^{n-1} - \frac{1}{2}2^{\frac{2n-2u}{2}}, 2^{n-1} - \frac{1}{2}2^{\frac{n+\frac{2s}{a}-1}{2}}), & n \text{ and } \frac{2s}{a} \text{ have different parity.} \end{cases}$$

Substituting the bounds of $nl(D_c h_\mu)$ in Proposition 1, the result follows.

■

5 For a given n, search for s and t for which h_μ has better lower bound on its second-order nonlinearity

Fixed n, we consider the problem of determining the values of s and t for which h_μ has high second-order nonlinearity, which in turn boils down to the problem of determination of s and t for which the dimension k of the kernel of bilinear form of the quadratic form $q(x)$ is minimum, this is same as finding an upper bound on the number of roots of the linearised polynomial $\mathcal{Q}_c(x)$ and $P(x)$. In this section we consider the problems related to minimization of $\frac{2s}{a}$ and $n - 2u$.

5.1 Subclasses of h_μ giving good lower bounds under the Case 1 of Theorem 2

Let $n \geq 4$ be a fixed positive integer. Given n, we have to find positive integers $s > t \geq 1$ such that $\frac{2s}{a}$ is minimum where $a = \max\{d \in \mathbf{N} : d|s, t; \gcd(d, n) = 1\}$.

Remark 1 *Let $(s, t, a) = (\bar{s}, \bar{t}, \bar{a})$ be any optimal solution then as $\bar{a}|(\bar{s}, \bar{t})$ this implies $\bar{s} = k_1\bar{a}$, $\bar{t} = k_2\bar{a}$. Since $\bar{s} > \bar{t}$ it follows that $k_1 > k_2 > 1$ and hence $k_1 \geq 2$. Hence $\frac{2\bar{s}}{\bar{a}} = 2k_1 \geq 4$.*

Remark 2 *Since n and the dimension of kernel k has the same parity, Remark 1 implies that in optimal case the upper bound of k is 4 for even n and 3 for odd n. Hence $k \leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$*

So for a given $n \geq 4$ we can find s and t such that $\frac{2s}{a}$ or in turn the dimension k of the kernel of $B(x, y)$ is upper bounded by 4 or 3 as n is even or odd respectively. Table 1 enlist some of the functions from class h_μ which attained these upper bounds of k. Here r is a positive integer. For description an example is provided below.

Table 1: For a given n, some values of s and t for which cubic monomial function of the form $h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1})$ possess high lower bound on its Second-Order Nonlinearity. $m \geq 2$ is a positive integer.

n	s	t	Condition on n	Upper bound on k
$3m$	$2m-2$	$m-1$	$m \neq 3r+1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$3m$	$2m+2$	$m+1$	$m \neq 3r-1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$3m+1$	$2m$	m	-	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$3m+1$	$2m+2$	$m+1$	$m \neq 2r+1$	$\leq \{ 3, \text{ if } n \equiv 1 \mod 2.$
$3m+1$	$2m-2$	$m-1$	$m \neq 4r+1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$3m+2$	$2m$	m	$m \neq 2r$	$\leq \{ 3, \text{ if } n \equiv 1 \mod 2.$
$3m+2$	$2m-2$	$m-1$	$m \neq 5r+1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$3m+2$	$2m+2$	$m+1$	$-$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2. \end{cases}$
$4m$	$2m+2$	$m+1$	$m \neq 2r+1$	$\leq \{ 4, \text{ if } n \equiv 0 \mod 2,$
$5m$	$2m+2$	$m+1$	$m \neq 5r-1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2, \\ 3, \text{ if } n \equiv 1 \mod 2, \end{cases}$
$7m$	$2m+2$	$m+1$	$m \neq 7r-1$	$\leq \begin{cases} 4, \text{ if } n \equiv 0 \mod 2 \\ 3, \text{ if } n \equiv 1 \mod 2 \end{cases}$

Example 1 *If $n = 3m$, with $m > 1$ a positive integer, then choosing $s = 2m+2$ and $t = m+1$ we get $\gcd(3m, m+1) = 3$ or 1, this implies if $3 \nmid m+1$ or $m \neq 3r+1$ for a positive integer r then $\gcd(3m, m+1) = 1$. Thus in this case $k \leq 4$ if n is even and $k \leq 3$ for odd n.*

Remark 3 *Applying Theorem 3 on the functions with n,s and t as enlisted in Table 1, a lower bound on their second-order nonlinearities is obtained as follows:*

1. *If $n \geq 4$ is even*

$$nl_2(h_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n+4}{2}} + 2^{\frac{n+4}{2}}},$$

2. *If $n \geq 4$ is odd*

$$nl_2(h_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n+2}{2}} + 2^{\frac{n+2}{2}}}.$$

Remark 4 *In the same way, for $n = 4m, s = 3m + 3, t = m + 1$ here m is an even positive integer, by Theorem 2 we have $k \leq 6$ and hence $W_{D_c h_\mu}(\lambda) \leq 2^{\frac{n+6}{2}}$. Thus by Theorem 3 $nl_2(h_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n+6}{2}} + 2^{\frac{n+6}{2}}}$. Similarly for a given n, we can choose other appropriate values of s, t and obtain better bounds.*

Corollary 1 *Consider the Boolean function $f_\mu(x) = Tr_1^n(\mu x^{2^{a_1 w}+2^{a_2 w}+1})$ where w and $a_1 > a_2$ are positive integers such that $\gcd(a_1, a_2) = 1$ and $\gcd(w, n) = 1$, we have*

1. *$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n}{2}+a_1} - 2^{\frac{n}{2}+a_1}}$, if n is even.*
2. *$nl_2(f_\mu) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{\frac{3n-1}{2}+a_1} - 2^{\frac{n-1}{2}+a_1}}$, if n is odd.*

Proof :The proof is similar to that of Theorem 2 upto Equation (1). Replacing s with $a_1 w$, t with $a_2 w$ in Equation (1) and then raising the obtained equation to the power 2^{a_1}, we get

$$\begin{aligned}(P_c(x))^{2^{a_1}} &= x^{(2^w)^{2a_1}} c^{2^{a_1 w + a_2 w}} + x^{(2^w)^{a_1+a_2}} c^{2^{2a_1 w}} + x^{(2^w)^{2a_1-a_2}} c^{2^{a_1 w - a_2 w}} \\ &+ x^{(2^w)^{a_1-a_2}} c^{2^{2a_1 w - a_2 w}} + x^{(2^w)^{a_2}} c + x c^{2^{a_2 w}}.\end{aligned}$$

$(P_c(x))^{2^{a_1}}$ is a σ polynomial of degree at most $2a_1$. Thus the dimension of kernel $k \leq 2a_1$ if n is even, else $k \leq 2a_1 - 1$. Thus by Lemma 1

$$W_{D_c f_\mu}(\lambda) \leq \begin{cases} 2^{\frac{n+2a_1}{2}}, & \text{if } n \text{ is even,} \\ 2^{\frac{n+2a_1-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Putting the corresponding values of $nl(D_c f_\mu)$ in Proposition 1, the result follows.

■

5.2 Subclasses of h_μ giving good lower bounds under the Case 2 of Theorem 2

Gode and Gangopadhyay [5] have found a lower bound on the second-order nonlinearities of the function $Tr_1^n(\mu x^{2^{2m}+2^m+1})$ when $\gcd(n, m) = 1$. Gangopadhyay et al [6] have found a lower bound on the second-order nonlinearities of the function $Tr_1^n(\mu x^{2^{2m}+2^m+1})$ for $n = 6m$, Garg and Gangopadhyay [7] for $n = 5m$, Singh [14] for $n = 3m$ and Sun and Wu [16] for $n = 4m$ respectively. In this section we found more subclasses of $Tr_1^n(x^{2^s+2^t+1})$ which have better second-order nonlinearities. Few results are given in Lemma 2 and Table 2 respectively.

Lemma 2 *For a given $n \geq 4$ define function $f : S \to \mathbb{N}$ be defined by $f(n, s, t) = \min\{n - s, s - t, t\}$ where $S = \{(n, s, t) : n > s > t \geq 1\}$. Then range $f = \{1, 2, \ldots, \lfloor \frac{n}{3} \rfloor\}$. Hence $\max f = \lfloor \frac{n}{3} \rfloor$. Some of the choices of n, s and t where f is taking maximum value $\lfloor \frac{n}{3} \rfloor$ is as follows:*

Class 1: $(n, s, t) = (3m + r, 2m + r, m + r)$, *for* $r = 0, 1, 2$

Class 2: $(n,s,t) = (3m+r+1, 2m+r+1, m+r)$, *for* $r = 0,1,2$

Class 3: $(n,s,t) = (3m+r+1, 2m+r, m+r)$, *for* $r = 0,1$

Class 4: $(n,s,t) = (3m+r+1, 2m+r, m)$, *for* $r = 1$

Proof :Let $a_1 = n-s$, $a_2 = s-t$ and $a_3 = t$. Consider $p \in \{1,2,\ldots,\lfloor \frac{n}{3} \rfloor - 1\}$, in this case then $f(2\lfloor \frac{n}{3} \rfloor + p + 2, \lfloor \frac{n}{3} \rfloor + p + 1, p) = min\{\lfloor \frac{n}{3} \rfloor +, \lfloor \frac{n}{3} \rfloor + 1, p\}$ =p. If $p = \lfloor \frac{n}{3} \rfloor$ then suppose that $n \equiv i \pmod 3$. It is easy to see that $f(3\lfloor \frac{n}{3} \rfloor + j, 2\lfloor \frac{n}{3} \rfloor + j, \lfloor \frac{n}{3} \rfloor + j) = \lfloor \frac{n}{3} \rfloor$ for all $j = 0,\ldots,i$. Hence $\{1,2,\ldots,\lfloor \frac{n}{3} \rfloor\} \subseteq range(f)$.
Next, note that if $f(n,s,t) > \lfloor \frac{n}{3} \rfloor$ then $a_i \geq \lfloor \frac{n}{3} \rfloor + 1$ for all i and hence $n = \sum_{i=1}^{3} a_i \geq 3\lfloor \frac{n}{3} \rfloor + 3 > n$ which is illogical. Thus $range(f) = \{1,2,\ldots,\lfloor \frac{n}{3} \rfloor\}$ and so $\max f = \lfloor \frac{n}{3} \rfloor$.
Consider the following classes:

Class 1: Let $(n,s,t) = (3m+r, 2m+r, m+r)$, for $r = 0,1,2$, then $s-t = m$ and and $n-t = m$ so $f(n,s,t) = \min\{n-s, s-t, t\} = \min\{m, m, m+r\} = m = \lfloor \frac{n}{3} \rfloor$

Class 2: Let $(n,s,t) = (3m+r+1, 2m+r+1, m+r)$, for $r = 0,1,2$ then $n-s = m$ and $s-t = m+1$ so $f(n,s,t) = m = \lfloor \frac{n}{3} \rfloor$.

Class 3: Let $(n,s,t) = (3m+r+1, 2m+r, m+r)$, for $r = 0,1$ then $n-s = m+1$ and $s-t = m$ so $f(n,s,t) = m = \lfloor \frac{n}{3} \rfloor$.

Class 4: Let$(n,s,t) = (3m+r+1, 2m+r+1, m+r)$, for $r = 0,1$ then $n-s = m$ and $s-t = m+1$ so $f(n,s,t) = m = \lfloor \frac{n}{3} \rfloor$.

■

Remark 5 *For the 4 classes given in Lemma 2, the dimension of kernel* $k \leq n-2m$ *and hence the second-order nonlineairty of* $Tr_1^n(\mu x^{2^s+2^t+1})$ *is lower bounded by* $2^{n-1} - \frac{1}{2}\sqrt{2^n + 2^{2n-m} - 2^{n-m}}$. *Results for some values of* n , s *and* t *are tabulated in Table 4. In general if* $n = 3r+b$ *where* $b = 0,1,2$*, the dimension* k *of the kernel is upper bounded by* $n - 2\lfloor \frac{n}{3} \rfloor$. k *takes optimal(minimum) value when* $b = 0$.

5.2.1 Some more subclasses of h_μ with good second-order Nonlinearity

Using Lemma 2 more subclasses are found, Table 2 lists some subclasses of functions of the form $Tr_1^n(\mu x^{2^s+2^t+1})$ for various values of $n = im$, here m ad i are positive integers and $3 \leq i \leq 11$ which have good lower bounds on their second-order nonlinearity. This list also includes the functions of the form $Tr_1^n(\mu x^{2^{2m}+2^m+1})$whose lower bounds on the second-order nonlinearities are obtained by Gangopadhyay et al [6] for $n = 6m$, Garg and Gangopadhyay [7] for $n = 5m$, Singh [14]for $n = 3m$ and Sun and Wu [16] for $n = 4m$ respectively.
A description for $n = 5m$, $s = 3m$ and t=m is given in Corllary 2.

Corollary 2 *Consider the function* $h_\mu(x) = Tr_1^{5m}(\mu x^{2^{3m}+2^{2m}+1})$*, then*

$$nl_2(h_\mu) \geq 2^{5m-1} - \frac{1}{2}\sqrt{2^{5m} + 2^{9m} - 2^{4m}}$$

Table 2: For a given n, the lower bound on the second-order nonlinearity of functions of the form $Tr_1^n(\mu x^{2^s+2^t+1})$ for some values of s and t

n	s	t	Upper bound on k by Case 2 of Theorem 2	Lower bound by Theorem 3
$3m$	$2m$	m	m	$2^{3m-1} - \frac{1}{2}\sqrt{2^{5m} + 2^{3m} - 2^{2m}}$
$4m$	$2m, 3m$	m	$2m$	$2^{3m-1} - \frac{1}{2}\sqrt{2^{5m} + 2^{4m} - 2^{3m}}$
$4m$	$3m$	$2m$	$2m$	$2^{3m-1} - \frac{1}{2}\sqrt{2^{5m} + 2^{4m} - 2^{3m}}$
$5m$	$2m, 3m, 4m$	m	$3m$	$2^{5m-1} - \frac{1}{2}\sqrt{2^{9m} + 2^{5m} - 2^{4m}}$
$5m$	$3m, 4m$	$2m$	$3m$	$2^{5m-1} - \frac{1}{2}\sqrt{2^{9m} + 2^{5m} - 2^{4m}}$
$5m$	$4m$	$3m$	$3m$	$2^{5m-1} - \frac{1}{2}\sqrt{2^{9m} + 2^{5m} - 2^{4m}}$
$6m$	$4m$	$2m$	$2m$	$2^{6m-1} - \frac{1}{2}\sqrt{2^{10m} + 2^{6m} - 2^{4m}}$
$7m$	$5m, 4m$	$2m$	$3m$	$2^{7m-1} - \frac{1}{2}\sqrt{2^{12m} + 2^{7m} - 2^{5m}}$
$7m$	$5m$	$3m$	$3m$	$2^{7m-1} - \frac{1}{2}\sqrt{2^{12m} + 2^{7m} - 2^{5m}}$
$8m$	$6m, 5m, 4m$	$2m$	$4m$	$2^{8m-1} - \frac{1}{2}\sqrt{2^{14m} + 2^{8m} - 2^{6m}}$
$8m$	$6m, 5m$	$3m$	$4m$	$2^{8m-1} - \frac{1}{2}\sqrt{2^{14m} + 2^{8m} - 2^{6m}}$
$9m$	$6m$	$3m$	$3m$	$2^{9m-1} - \frac{1}{2}\sqrt{2^{14m} + 2^{9m} - 2^{6m}}$
$10m$	$6m, 7m$	$3m$	$4m$	$2^{10m-1} - \frac{1}{2}\sqrt{2^{17m} + 2^{10m} - 2^{7m}}$
$10m$	$7m$	$4m$	$4m$	$2^{10m-1} - \frac{1}{2}\sqrt{2^{17m} + 2^{10m} - 2^{7m}}$
$11m$	$8m, 7m, 6m$	$3m$	$5m$	$2^{11m-1} - \frac{1}{2}\sqrt{2^{17m} + 2^{11m} - 2^{8m}}$
$11m$	$8m, 7m$	$4m$	$5m$	$2^{11m-1} - \frac{1}{2}\sqrt{2^{17m} + 2^{11m} - 2^{8m}}$

Proof :Putting $s = 3m$ and $t = m$ in Equation (2) we get,

$$\begin{aligned}
\mathcal{Q}_c(x) &= \mu^{2^{3m}} x^{2^{6m}} c^{2^{4m}} + \mu^{2^{3m}} x^{2^{4m}} c^{2^{6m}} + \mu^{2^m} x^{2^{5m}} c^{2^{4m}} \\
&+ \mu^{2^m} x^{2^{2m}} c^{2^{5m}} + \mu x^{2^m} c + \mu x c^{2^m} \\
&= x^{2^m}(\mu^{2^{3m}} c^{2^{4m}} + c\mu) + x^{2^{4m}}(\mu^{2^m} c^{2^m}) + x(\mu^{2^m} c^{2^{4m}} + \mu c^{2^m}) + x^{2^{2m}} \mu^{2^m} c \\
&= (x^{2^m}(\mu^{2^{3m}} c^{2^{4m}} + c\mu) + x^{2^{-m}}(\mu^{2^m} c^{2^m}) + x(\mu^{2^m} c^{2^{4m}} + \mu c^{2^m}) + x^{2^{2m}} \mu^{2^m} c)^{2^m} \\
&= x^{2^{2m}}(\mu^{2^{4m}} c + c^{2^m} \mu^{2^m}) + x(\mu^{2^{2m}} c^{2^{2m}}) + x^{2^m}(\mu^{2^{2m}} c + \mu^{2^m} c^{2^{2m}}) + x^{2^{3m}} \mu^{2^{2m}} c^{2^m}
\end{aligned}$$

Thus $k \leq 3m$. (The technique is similar to the Case 2 of Theorem 2, as here $u = \min(5m - 3m, 3m - m, m) = m$ and hence $k \leq n - 2u = 5m - 2m = 3m$.)
By Lemma 1, we have $W_{D_c g_\mu}(\lambda) \leq 2^{\frac{5m+3m}{2}} = 2^{4m}$ and $nl(D_c(g_\mu)) \geq 2^{5m-1} - 2^{4m-1}$. The result follows by substituting the bound of $nl(D_c(g_\mu))$ in Proposition 1. ■

6 Comparison

To summarize better lower bounds on second-order nonlinearities of h_μ have been obtained for some possible values of s, t where $n \geq 4$ is fixed. Some comparisons with values obtained in [5]

are given in Table 5 and Table 6 respectively. Using Proposition 2 the values of lower bounds in all tables have been rounded up to the nearest multiple of $2^{\lceil \frac{n}{3} \rceil - 1}$.

7 Nonlinearity of some functions with high second-order Nonlinearity

Using SAGE the nonlinearity for some functions from the class h_μ which have good lower bound on their second-order nonlinearity is calculated. Experimental results for some values of $6 \leq n \leq 19$ are given in Table 3. The results show that the nonlinearity of these classes of Boolean functions nonlinearity is also high, apart from their high second-order nonlinearity.

Table 3: The nonlinearity profile of functions of the form $h_1(x) = Tr_1^n(x^{2^s+2^t+1})$ for some values of n, s and t.

n	s	t	h_1	$nl(h_1)$	Lower bound on $nl_2(h_1)$
7	6	3	$Tr_1^7(x^{71})$	56	32
8	6	2	$Tr_1^8(x^{69})$	112	64
8	6	2	$Tr_1^8(x^{69})$	112	64
9	6	3	$Tr_1^9(x^{71})$	224	168
11	6	3	$Tr_1^{11}(x^{71})$	960	768
11	8	4	$Tr_1^8(x^{273})$	960	768
11	4	2	$Tr_1^{11}(x^{21})$	960	768
12	10	5	$Tr_1^{12}(x^{1057})$	1960	1536
13	6	3	$Tr_1^{13}(x^{71})$	4032	3372
14	6	3	$Tr_1^{14}(x^{71})$	7968	6744
15	6	3	$Tr_1^{15}(x^{71})$	16064	14336
16	6	3	$Tr_1^{16}(x^{71})$	32256	28672
17	4	2	$Tr_1^{17}(x^{21})$	64704	59744

8 Conclusion

This paper deals with finding cubic monomial functions of the form $Tr_1^n(\mu x^{2^s+2^t+1})$ which have high lower bounds on their second-order nonlinearities. We give information related to the choice of s and t for which the functions of the given form possess high second-order nonlinearities. Our bounds have improved upon previously known bounds in some cases and are valid for all $n \geq 4$. Results in Section 7 shows that that there are subclasses of h_μ which have good nonlinearity profile. Therefore this search is helpful in locating cryptographically significant Boolean functions that can resist various low order approximation attacks and fast algebraic attacks.

References

[1] B. Csajbk, G. Marino, O. Polverino, F. Zullo, A characterization of linearized polynomials with maximum kernel. Finite Fields Th App, 56, 109-130 (2019).

[2] A. Canteaut, P. Charpin, G. M. Kyureghyan, A new class of monomial bent functions, Finite Fields Th App 14 221-241 (2008).

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

[4] R. Fourquet, C. Tavernier, An improved list decoding algorithm for the second order Reed-Muller codes and its applications, Des. Codes Cryptogr. 49, 323-340(2008).

[5] Ruchi Gode and Sugata Gangopadhyay. On second order nonlinearities of cubic monomial Boolean functions. In: Cryptology ePrint Archive (2009).

[6] S. Gangopadhyay, S. Sarkar, R. Telang, On the lower bounds of the second order nonlinearities of some Boolean functions, Inf. Sci. 180 266-273 (2010).

[7] Manish Garg and Sugata Gangopadhyay. The Good lower bound of Second-order nonlinearity of a class of Boolean function. In: Cryptology ePrint Archive (2011).

[8] J. Golic, Fast low order approximation of cryptographic functions, In: Proceedings of the EUROCRYPT'96, LNCS, 1996, Springer, pp. 268-282 (1996).

[9] L. R. Knudsen, M. J. B. Robshaw, Non-linear approximations in linear cryptanalysis, In: Proceedings of the EUROCRYPT'96, LNCS, 1070, Springer, pp. 224-236 (1996).

[10] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1983.

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

[12] W. Millan, Low order approximation of cipher functions, In: Cryptographic policy and algorithms, LNCS, 1029, pp. 144-155 (1996).

[13] O. S. Rothaus, On bent functions, J. Comb. Theory Ser. A. 20 300-305 (1976).

[14] Deep Singh. Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions. In: Intl J. Comput. Sci. Inform. Technol 2.2 (2011), pp. 786791.

[15] G. Sun, C. Wu, The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity, Inf. Sci. 179 (3) 267-278 (2009).

[16] Guanghong Sun and Chuankun Wu. The lower bound on the second-order nonlinearity of a class of Boolean functions with high nonlinearity. In: Applicable Algebra in Engineering, Com- munication and Computing 22.1 (2011), pp. 3745.

Table 4: The values on the lower bound on the second-order nonlinearity of functions of form $h_\mu(x) = Tr_1^n(\mu x^{2^s+2^t+1})$ for some values of n, s, t (Bound by Case 2 of Theorem 3)

n	s	t	Upper bound on k by Theorem 2	Lower bound on $nl_2(h_\mu)$ by Theorem 3
4	$3, 2$	1	2	4
4	3	2	2	4
5	$2, 3, 4$	1	3	6
6	4	2	2	16
7	$4, 5$	2	3	32
7	5	3	3	32
8	$4, 5, 6$	2	4	64
8	$5, 6$	3	4	64
9	6	3	3	168
10	7	4	4	332
10	$6, 7$	3	4	332
11	$7, 8$	5	5	662
11	7	5	5	662
12	8	4	4	1536
13	$8, 9$	4	5	3072
13	9	5	5	3072
14	$8, 9, 10$	4	6	6144
14	$9, 10$	5	6	6144
14	10	6	6	6144
15	10	5	5	13488
16	$10, 11$	5	6	26976
17	$10, 11, 12$	5	7	57344
18	12	6	6	114688
19	13	6	7	238972
20	$12, 13, 14$	6	8	477946

Table 5: Comparison of the values of the improved lower bounds for some values of n, s and t as given in Lemma 2 with bound of [5]

n	s	t	Upper bound on k	Lower bound of Theorem 3	[5]
7	4	2	3	32	-
7	6	2	5	19	-
8	4	2	4	64	38
8	6	3	4	64	-
9	6	4	5	128	-
9	6	2	5	168	-
10	6	3	4	332	332
11	4	2	3	768	768
11	6	3	3	768	768
11	6	2	5	662	-
11	8	4	3	768	768
12	10	5	4	1536	1536
13	6	2	5	3072	1200
13	6	3	3	3372	3372
13	12	4	5	3072	-
13	10	5	3	3372	3372
13	15	5	5	3372	3372
14	6	3	4	6744	6744
14	10	5	4	6744	6744
15	6	2	3	13488	8192
15	8	4	3	14336	14366
15	14	7	3	14336	14366
16	6	3	4	28672	28672
16	10	5	4	28672	28672
16	14	7	3	28672	28672
17	6	2	5	57344	42366
17	6	3	3	59744	59744
17	8	6	7	53951	19196
17	10	5	3	59744	59744
17	12	4	5	57344	-
18	14	7	4	119488	119488
19	4	2	3	245760	245760
19	6	2	5	238974	196608
19	10	5	3	245760	245760
19	12	3	7	229376	-
19	16	4	7	229376	-
20	6	3	4	491520	491520
20	18	6	4	477948	-

Table 6: Comparison of the values of the lower bound on the second-order nonlinearity of functions of form $Tr_1^n(\mu x^{2^s+2^t+1})$ for some values of n, s, t. Given by Theorem 3 with others

n	s	t	Theorem 3	[14]	[16]	[7]	[6]	[5]
4	2	1	4	-	4	-	-	4
5	2	1	6	-	-	6	-	6
6	2	1	8	-	-	-	10	8
6	4	2	16	16	-	-		-
7	4, 5	2	32	-	-	-	-	-
8	5	2	64	-	-	-		-
8	4	2	64	-	64	-	-	38
9	6	3	168	168		-	-	-
10	4	2	256	-	-	256	-	150
10	7	3, 4	332	-	-	-	-	-
11	7, 8	5	662	-	-	-	-	-
12	4	2	1024	-	-	-	1024	1024
12	6	3	1324	-	1324	-	-	-
12	8	4	1536	1536		-	-	-
13	8, 9	4	3072	-	-	-		-
14	10	4	6144	-	-	-		-
15	6	3	10592	-		10592	-	4799
15	10	5	13488	13488	-	-		-
16	10, 11	5	26976	-	-	-		-
16	8	4	24576	-	24576	-		-
17	10, 11, 12	-	57344		-	-		-
18	13	6	107902	-	-	-		-
18	12	6	114688	114688		-	-	-
19	13	6	238972	-	-	-	-	-
20	13, 14	6	477946	-	-	-	-	-
20	8	4	393216	-	-	393216	-	262144
20	10	5	431606	-	431606	-	-	-