Additive autocorrelation of some classes of cubic semi-bent Boolean functions

Deep Singh[⋆]and Maheshanand Bhaintwal

Department of Mathematics,
Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
{deepsinghspn,mbhaintwal}@gmail.com

Abstract. In this paper, we investigate the relation between the autocorrelation of a cubic Boolean function $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$ and the kernel of the bilinear form associated with $D_a f$, the derivative of f at a. Further, we apply this technique to obtain the tight upper bounds of absolute indicator and sum-of-squares indicator for avalanche characteristics of various classes of highly nonlinear non-bent cubic Boolean functions.

Key words: Semi-bent Boolean functions, Additive autocorrelation, Welch functions

1 Introduction

Let $\mathbb{F}_2^n$ be the vector space n-tuples over the $\mathbb{F}_2$, the prime field of characteristic 2. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on n variables. $\mathcal{B}_n$ denotes the set of all such functions. The Boolean functions used in cryptosystems should possess certain desirable cryptographic criteria such as high nonlinearity profile, resiliency, low additive autocorrelations and low crosscorrelations etc. Resiliency ensures the system is not prone to correlation attacks [18, 20] while high nonlinearity offers protection against linear approximation attacks [15, 16]. Another criterion studied in many recent papers, is low additive autocorrelation [9, 13] which ensures that the output of the Boolean function is complemented with probability close to $1/2$ when any number of input bits are complemented. As a result, it provides protection against differential-like cryptanalysis [1]. In [21], it has been discussed that this is a more practical criterion than the propagation criterion of order k, which, in the case of high nonlinearity may cause linear structures to occur.

Zhang and Zheng [21] introduced two indicators related to global avalanche characteristics (GAC) called the absolute indicator (or additive autocorrelation) $\triangle_f$ and sum-of-square indicator σ_f of autocorrelation function of a Boolean function. Zhou et al. [22] proposed the absolute indicator $\triangle_{f,g}$ and sum-of-square indicator $\sigma_{f,g}$ of crosscorrelation function between two Boolean functions

[⋆] Research supported by NBHM (DAE), INDIA.

and obtained lower and upper bounds for them. Determining the autocorrelation $\triangle_f(a),\ a \in \mathbb{F}_{2^n}$ and the additive autocorrelation $\triangle_f$ of any $f \in \mathcal{B}_n$ are of great interest in cryptography and codding theory [9]. In addition, autocorrelation function in another form also have applications in physics [10, 11]. Although autocorrelation is is an important indicator for a Boolean function, it is a difficult task to determine all the autocorrelation coefficients because the computation of the Hamming weights of the derivatives of the function at each point is a difficult problem.

In this paper we investigate the relation between the autocorrelation of a cubic function $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$ and the kernel of the bilinear form associated with $D_a f$, the derivative of f at a. Further, we apply this technique to obtain the upper bounds of absolute indicators (i.e., additive autocorrelation) and sum-of-squares avalanche characteristics for various classes of highly nonlinear non-bent cubic Boolean functions.

Remainder of paper is organized as follows. Section 2 provides several known results. In section 3 we compute the autocorrelation of quadratic Boolean functions for an even n. In section 4 we establish a relation between the autocorrelation of a cubic Boolean function and the kernel of the bilinear form associated with the derivative of f.

2 Priliminaries

The set $\mathbb{F}_2^n$ of all n-tuples of elements of $\mathbb{F}_2$ is isomorphic to $\mathbb{F}_{2^n}$ as $\mathbb{F}_2$-vector spaces. Thus, a Boolean function can also be thought of as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The addition in both $\mathbb{Z}$ and $\mathbb{F}_{2^n}$ is denoted by '+', whereas '$\oplus$' denotes the addition in $\mathbb{F}_2^n$. The Hamming weight of any element $\mathbf{x} \in \mathbb{F}_2^n$, $w_H(\mathbf{x}) := \sum_{i=1}^n x_i$, where the sum is over $\mathbb{Z}$. The trace function $tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as follows:

$$tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}},\ \text{for all } x \in \mathbb{F}_{2^n}.$$

The functions $(x, y) \mapsto tr_1^n(xy)$ and $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y} = \oplus_{i=1}^n x_i\, y_i$ are both inner products on $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, respectively. The algebraic normal form (ANF) of a Boolean function, $f \in \mathcal{B}_n$ is

$$f(x_1, x_2, \ldots, x_n) = \sum_{\mathbf{a}=(a_1,a_2,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \prod_{i=1}^n x_i^{a_i},\ \text{where } \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The algebraic degree of f, $\deg(f) := \max\{w_H(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0, \mathbf{a} \in \mathbb{F}_2^n\}$. For any $f, g \in \mathcal{B}_n$, the Hamming distance between f and g is $d(f, g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|$.

The derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as

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

Suppose $a, b \in \mathbb{F}_{2^n}$ are $\mathbb{F}_2$-linearly independent and generate a two-dimensional subspace V in $\mathbb{F}_{2^n}$. The function

$$D_V f(x) = D_a D_b f(x) = f(x) + f(x + a) + f(x + b) + f(x + a + b) \text{ for all } x \in \mathbb{F}_{2^n}$$

is said to be the *second-derivative* of f with respect to the subspace V. It can be checked that $D_V f$ is independent of the choice of the basis of V. This notion can further be generalized. For more details we refer to [5].

The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$ is defined as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+tr_1^n(ax)}.$$

The nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l \in \mathcal{A}_n}\{d(f,l)\}$, where $\mathcal{A}_n$ be the set of all affine functions in $\mathcal{B}_n$. The nonlinearity of $f \in \mathcal{B}_n$ in terms of Walsh-Hadamard transform is defined as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} |W_f(a)|.$$

By Parseval's identity,

$$\sum_{a \in \mathbb{F}_{2^n}} W_f(a)^2 = 2^{2n},$$

it can be shown that $\max_{a \in \mathbb{F}_{2^n}} |W_f(a)| \geq 2^{n/2}$, which implies that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. The functions achieving this bounds are called *bent* [17]. These functions exist only for even integers.

The sum

$$C_{f,g}(a) = \sum_{x \in \mathbb{F}_{2^n}} \xi^{f(x)+g(x+a)},$$

is called the cross-correlation of $f, g \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$. In particular for $f = g$, the sum $C_{f,f}(a) = C_f(a)$ is called the autocorrelation of f at $a \in \mathbb{F}_{2^n}$.

The additive autocorrelation or the absolute indicator [21] of the autocorrelation function of $f \in \mathcal{B}_n$ is defined as

$$\triangle_f = \max_{a \in \mathbb{F}_{2^n} \setminus \{0\}} |\triangle_f(a)|.$$

and the sum-of-squares indicator [21] of the autocorrelation function of f is defined as

$$\sigma_f = \sum_{a \in \mathbb{F}_{2^n}} |\triangle_f(a)|^2.$$

The smaller are the values of $\triangle_f$ and σ_f, the better is the GAC of a Boolean function. Like many other characteristics of a function including nonlinearity, algebraic degree etc., the two indicators for the GAC are invariant under nonsingular linear transformations on the input coordinates. We have $\triangle_f = 0$ if and only if f is bent, and $\triangle_f = 2^n$ if and only if f has nonzero linear structure. Moreover, $0 \leq \triangle_f \leq 2^n$ and $2^{2n} \leq \sigma_f \leq 2^{3n}$. If f is cubic non-bent function on $\mathbb{F}_{2^n}$ then $\triangle_f \geq 2^{\frac{n+1}{2}}$ [21].

2.1 Quadratic Boolean functions

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

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

Lemma 1 ([3], Proposition 1). *Let V be a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $Q : V \longrightarrow \mathbb{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Lemma 2 ([3], Lemma 1). *Let f be any quadratic Boolean function. The kernel $\mathcal{E}_f$ is the subspace of $\mathbb{F}_{2^n}$ consisting of those a such that the derivative D_af is constant. That is,*

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} : D_af = \text{ constant } \}.$$

If $f \in \mathcal{B}_n$ be a quadratic Boolean function and $B(x,y)$ be the associated bilinear form, then the Walsh spectrum of f depends only on the dimension of the kernel $\mathcal{E}_f$ of $B(x,y)$ [3, 14]. The weight distribution of the Walsh spectrum of f is provided in Table 1.

Table 1. Weight distribution of the Walsh spectrum of a quadratic function f

$W_f(a)$	number of a
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)}2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)}2^{(n-k-2)/2}$

3 Additive autocorrelation and sum-of-squares indicators

Gong and Khoo [9] introduced the concept of dual function of a Boolean function and investigated the autocorrelation of the functions having 3-valued Walsh-Hadamard spectrum. The dual of $f \in \mathcal{B}_n$ is defined as follows

Definition 1. *The dual of $f \in \mathcal{B}_n$ is a function $\tilde{f} \in \mathcal{B}_n$ defined by*

$$\tilde{f}(x) = \begin{cases} 1 & \text{if } W_f(x) \neq 0, \\ 0 & \text{if } W_f(x) = 0. \end{cases}$$

By Parseval's identity it is observed that if the Walsh-Hadamard spectrum of f is 3-valued, i.e., for any $a \in \mathbb{F}_{2^n}$ $W_f(a) \in \{0, \pm 2^i\}$, then the weight of its dual $\tilde{f}$ is $2^{2(n-i)}$. A function $f \in \mathcal{B}_n$ is *semi-bent* if for any $a \in \mathbb{F}_{2^n}$ (i) $W_f(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for odd n, and (ii) $W_f(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for even n. The following result is due to Gong and Khoo [9]

Lemma 3. *[9] Let $f \in \mathcal{B}_n$ such that $W_f(a) \in \{0, \pm 2^i\}$ for all $a \in \mathbb{F}_{2^n}$. Then*

$$C_f(a) = -2^{2i-(n+1)} W_{\tilde{f}}(a), \text{ for all } a \in \mathbb{F}_{2^n} \setminus \{0\}.$$

In particular, if $f \in \mathcal{B}_n$ is semi-bent Boolean function, then for any $a \neq 0$

$$C_f(a) = \begin{cases} -W_{\tilde{f}}(a) & \text{if } n \equiv 1 \mod 2, \\ -2W_{\tilde{f}}(a) & \text{if } n \equiv 0 \mod 2. \end{cases}$$

Thus the autocorrelation spectrum of a semi-bent Boolean function f depends on the Walsh-Hadamard spectrum of its dual $\tilde{f}$. It is shown in [9, Theorem 2] that if $f \in \mathcal{B}_n$ (for odd n) is a balanced preferred (semi-bent) function and $\tilde{f} \in \mathcal{B}_n$ is preferred, then $\triangle_f = 2^{\frac{n+1}{2}}$ and $C_f(a) = 0$ for $2^{n-1} - 1$ $a's$. That is, f has optimal additive autocorrelation. Now, if $f \in \mathcal{B}_n$ (for n even) be semi-bent, then the Hamming weight of $\tilde{f}$, the dual of f is 2^{n-2}, and the Hamming weight of f, $w_H(f) \in \{2^{n-1}, 2^{n-1} \pm 2^{\frac{n}{2}}\}$. Therefore, by Lemma 3 and [9, Proposition 3], we have the following

Proposition 1. *Let n be an even positive integer and $f \in \mathcal{B}_n$ be a semi-bent function. Then dual $\tilde{f}$ of f will never be bent, or semi bent. In particular, the function f will never achieve the optimal value of additive autocorrelation, and the sum of square indicators, σ_f, is at most $5 \cdot 2^{2n}$.*

Remark 1. It follows from Lemma 3 that if n is an odd positive integer and $f \in \mathcal{B}_n$ is semi-bent, then the sum of square indicators, σ_f, of f is at most 2^{2n+1}.

Theorem 1. *Let n be a positive integer and $M = \{x \in \mathbb{F}_{2^n} : x^{2^{2i}} + x = 0\}$. Then the autocorrelation of a quadratic Boolean function, $f(x) = tr_1^n(x^{2^i+1})$ is given as*

$$|C_f(a)| = \begin{cases} 2^n & \text{if } a \in M, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $a \in \mathbb{F}_{2^n}$. Then we have,

$$\begin{aligned} C_f(a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{2^i+1}) + tr_1^n((x+a)^{2^i+1})} \\ &= (-1)^{tr_1^n(a^{2^i+1})} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x^{2^i}a + a^{2^i}x)} \\ &= (-1)^{tr_1^n(a^{2^i+1})} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x(a^{2^i} + a^{2^{n-i}}))} = (-1)^{tr_1^n(a^{2^i+1})} 2^n \phi_M(a), \end{aligned}$$

where ϕ_M is the indicator function of M. Therefore,

$$|C_f(a)| = \begin{cases} 2^n & \text{if } a \in M, \\ 0 & \text{otherwise.} \end{cases}$$

□

4 Upper bounds of additive autocorrelation and sum-of-squares indicators for cubic functions

Zhou et al. [22], provided the following relation between the $(r-1)$th order nonlinearity of the derivative of $f \in \mathcal{B}_n$ and two indicators $\triangle_{f,g}$ and $\sigma_{f,g}$.

Proposition 2. *[22, Theorem 8] If $f, g \in \mathcal{B}_n$ and $\deg(g) \leq r$, then*

(i) $\triangle_{f,g} \leq \sqrt{2^{2n} - 2\sum_{b\in\mathbb{F}_{2^n}} nl_{r-1}D_{f(x)}(b)}$, *and*
(ii) $\sigma_{f,g} \leq 2^{3n} - 2^{n+1}\sum_{b\in\mathbb{F}_{2^n}} nl_{r-1}D_{f(x)}(b)$.

In particular, using these relations for $f = g$, we get $\triangle_f \leq 2^n$ and $\sigma_f \leq 2^{3n}$, which are well known and are worst upper bounds. Thus, we have no new information about the two indicators $\triangle_f$ and σ_f.
In the following lemma, for a cubic Boolean function $f \in \mathcal{B}_n$, we establish a relation between absolute indicator $\triangle_f$ and the kernel of the bilinear form associated with D_af, the derivative of f at $a \in \mathbb{F}_{2^n}$.

Lemma 4. *Let $f \in \mathcal{B}_n$ be a cubic Boolean function then the autocorrelation of f at $a \in \mathbb{F}_{2^n}$ is*

$$|C_f(a)|^2 = 2^n \sum_{b\in\mathcal{E}_{D_af}} (-1)^{\epsilon_{a,b}}, \tag{1}$$

where $\mathcal{E}_{D_af}$ is the kernel of D_af and $\epsilon_{a,b}$ is given by

$$\mathcal{E}_{D_af} = \{b \in \mathbb{F}_{2^n} : D_bD_af(x) = \epsilon_{a,b}(constant)\}.$$

Also, we have

$$|C_f(a)|^2 \leq 2^n|\mathcal{E}_{D_af}|. \tag{2}$$

Proof. We have

$$C_f(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{D_af(x)}$$

Therefore,

$$
\begin{aligned}
|C_f(a)|^2 &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{D_af(x)}(-1)^{D_af(y)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} \sum_{y=x+b\in\mathbb{F}_{2^n}} (-1)^{D_af(x)}(-1)^{D_af(y)} \\
&= \sum_{b\in\mathbb{F}_{2^n}} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{D_af(x)+D_af(x+b)} \\
&= \sum_{b\in\mathbb{F}_{2^n}} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{D_bD_af(x)} \qquad (3)
\end{aligned}
$$

Since f is a cubic function therefore, D_af, the first derivative of f, at each $a \in \mathbb{F}_{2^n}$ is at most quadratic. The weight distribution of quadratic and affine functions is well known [14, Chap. 15]. The kernel, $\mathcal{E}_{D_af}$, of bilinear form associated with D_af is

$$\mathcal{E}_{D_af} = \{b \in \mathbb{F}_{2^n} : D_bD_af(x) = \epsilon_{a,b}\}. \qquad (4)$$

Moreover, $D_bD_af(x)$ is at most affine. This implies that $D_bD_af(x)$ is either constant or balanced. Therefore, by Eq. (4), $D_bD_af(x)$ is balanced if $b \notin \mathcal{E}_{D_af}$ otherwise $D_bD_af(x)$ is constant. Using this result in (3), we have

$$
\begin{aligned}
|C_f(a)|^2 &= \sum_{b\in\mathcal{E}_{D_af}} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\epsilon_{a,b}} + \sum_{b\notin\mathcal{E}_{D_af}} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{D_bD_af(x)} \\
&= 2^n \sum_{b\in\mathcal{E}_{D_af}} (-1)^{\epsilon_{a,b}}.
\end{aligned}
$$

Therefore, we have

$$|C_f(a)|^2 \leq 2^n|\mathcal{E}_{D_af}|.$$

□

4.1 Upper bounds for Welch and Modified Welch functions

A vectorial function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F(x) = x^d$ is called a *power function*. The vectorial Welch function $F_{welch} : x \in \mathbb{F}_{2^n} \to x^{2^\ell+3} \in \mathbb{F}_{2^n}$ is defined by $x \to x^{2^\ell+3}$, where ℓ is a positive integer such that $n = 2\ell + 1$, ℓ. The Welch functions are almost perfect nonlinear functions, i.e., they are maximally nonlinear [2]. Let $f_\lambda(x) = tr_1^n(\lambda x^{2^\ell+3})$ is a Welch Boolean function. The crosscorrelatiom spectrum betwwen any two Welch functions is 3-valued, $\{-1, -1 \pm 2^{\ell+1}\}$ [7]. The vectorial Welch function is a permutation. Therefore, all Boolean functions $tr_1^n(\lambda x^{2^\ell+3})$, $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, are affine equivalent to each other [4] and hence autocorrelation spectrum of these functions are same. We shall therefore study the additive autocorrelation and sum-of-squares of avalanche characteristics of $tr_1^n(x^{2^\ell+3})$. The second-order nonlinearities of these functions are extremely good [4]. Carlet [4, Lemma 1] proved that the dimension $k(a)$ of the kernel $\mathcal{E}_{D_af}$ is at most 3 for any $a \in \mathbb{F}_{2^n} \setminus \{0\}$. Thus, by Remark 1 and Lemma 4, we have the following

Theorem 2. *Let n, ℓ be positive integers such that $\ell = \frac{n-1}{2}$ and let $f(x) = tr_1^n(x^{2^\ell+3})$. Then $\triangle_f \leq 2^{\frac{n+3}{2}}$ and $\sigma_f \leq 2^{2n+1}$.*

Remark 2. It is to be noted that $2^{2n} \leq \sigma_f \leq 2^{3n}$. Also, for an odd positive integer n, the optimal value of $\triangle_f$ is $2^{\frac{n+1}{2}}$ [9, Theorem 2] and the worst value is 2^n. Hence by Theorem 2, we observe that for the Welch functions, the additive autocorrelation and the sum-of-squares indicator of avalanche characteristics both are extremely good.

Carlet [4, Eq. (3)] has established that the lower bound on second-order nonlinearity of modified Welch functions is better than that of the Welch functions. This bound is improved in the same paper [4, pp. 1269]. In the following theorem we obtain the upper bounds for additive autocorrelation and sum-of-squares indicator of avalanche characteristics for these functions.

Theorem 3. *Let n, ℓ be positive integers such that $\ell = \frac{n+1}{2}$ and let $f(x) = tr_1^n(x^{2^\ell+3})$. Then (i) $\triangle_f \leq 2^{\frac{n+3}{2}}$, and (ii) $\sigma_f \leq 2^{2n+2} + 2^{2n+1}$ if $\gcd(n,3) = 1$ otherwise $\sigma_f \leq 2^{2n+2} + 2^{2n+1} + 7\sqrt{6} \cdot 2^{\frac{3n}{2}-1}$.*

Proof. From [4, pp 1269] the dimension $k(a)$ of the kernel $\mathcal{E}_{D_af}$ is at most 3 for any $a \in \mathbb{F}_{2^n} \setminus \{0\}$. Moreover, $N(a)$, the number of a's for which $k(a) = 1$ is 2^{n-1}, i.e., $N(a) = 2^{n-1}$ if $\gcd(n,3) = 1$ otherwise $N(a) \geq 2^{n-1} - 2^{\frac{n}{2}-1}\sqrt{6}$. Applying these results in Lemma 4, we have the theorem.

Remark 3. We observe that the additive autocorrelation and the sum-of-squares indicator of avalanche characteristics of modified Welch functions are efficiently very low. It is to be noted that while the lower bound on second-order nonlinearity of modified Welch functions is better than that of the Welch functions, the bound for σ_f is very high in comparison to Welch functions.

4.2 Upper bounds for two classes of semi-bent functions

In this section, we deduce the upper bounds of additive autocorrelation and sum-of-squares indicators of two well known classes [6] of cubic semi-bent Boolean functions (functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$) of the form $f(x) = tr_1^n(x^d)$, for all $x \in \mathbb{F}_2^n$, where (i) $d = 2^{r+1} + 3$ and $n = 2r$, and (ii) $d = 2^{2r} + 2^{r+1} + 1$, $n = 2r$, and r is odd. Sun and Wu [19] have demonstrated that the lower bounds of second-order nonlinearities of these functions are extremely good. In particular, for $n = 8$, these functions achieve the maximum possible second-order nonlinearity ($nl_2(f) = 84$) [19, Section 4]. The bounds of additive autocorrelation and sum-of-squares indicator of these classes are given in the following

Theorem 4. *Let $f \in \mathcal{B}_n$ be cubic Boolean function of the form $f(x) = tr(x^d)$, where*

(*i*) $d = 2^{r+1} + 3$ *and* $n = 2r$, *or*
(*ii*) $d = 2^{2r} + 2^{r+1} + 1$, $n = 2r$, *and* r *is odd.*

Then $\triangle_f \leq 2^{\frac{3n+4}{4}}$ *and* $\sigma_f \leq 5 \cdot 2^{2n}$.

Proof. It is shown by Sun and Wu [19, Lemma 2 and Lemma 3] that the dimension $k(a)$ of the kernel $\mathcal{E}_{D_a f}$ in either case satisfies the following relation

$$k(a) = \begin{cases} 2 & \text{if } a \notin \mathbb{F}_{2^r}, \\ r+2 & \text{if } a \in \mathbb{F}_{2^r}. \end{cases} \tag{5}$$

Using Lemma 4, we have

$$|C_f(a)|^2 \leq \begin{cases} 2^{n+2} & \text{if } a \notin \mathbb{F}_{2^r}, \\ 2^{n+r+2} & \text{if } a \in \mathbb{F}_{2^r}. \end{cases}$$

Therefore,

$$\triangle_f = \max_{a \in \mathbb{F}_{2^n} \setminus \{0\}} |C_f(a)| \leq 2^{\frac{3n+4}{4}}$$

In either case f is semi-bent. The second part then follows from Proposition 1. □

4.3 Upper bounds for cubic functions with exponent $d = 2^{2r} + 2^r + 1$ with $\gcd(r, n) = 1$

Gode and Gangopadhyay [8] have obtained some lower bounds on second-order nonlinearity for a more general classes of cubic functions. They have proved that the dimension of the kernel for the cubic functions of the form $tr_1^n(\alpha x^{2^{2r}+2^r+1})$, where $\gcd(n, r) = 1$ and $n > 4$, is at most 4, i.e., $k(a) \leq 4$ for all $a \neq 0$ if n is even, and otherwise $k(a) \leq 3$ for all $a \neq 0$. Therefore, by Lemma 4 the additive autocorrelation of these functions is at most $2^{\frac{n+3}{2}}$ if n is odd, and $2^{\frac{n+4}{2}}$, otherwise.

Li et al. [12] generalized these classes of cubic Boolean functions with more than one trace terms and deduced the lower bounds on second-order nonlinearities. There may exists more semi-bent functions whose upper bounds on additive correlation and sum-of-squares avalanche characteristic can be computed by using the results in this paper.

5 Acknowledgement

The first author would like to thank B. K. Singh for helpful suggestions and discussions.

References

1. E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 4(1), pp. 372, 1991.
2. A. Canteaut, P. Charpin and H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, IEEE Trans. Inform. Theory, Vol. 46 (1), pp. 4-8, 2000.
3. Canteaut, A., Charpin, P. and Kyureghyan, G. M.: A new class of monomial bent functions, Finite Fields and Applications 14, pp. 221-241 2008.
4. C. Carlet, 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. C. Carlet, "Boolean functions for cryptography and error correcting codes," Chapter of the monograph, "*Boolean Models and Methods in Mathematics, Computer Science and Engineering*," Cambridge Univ. Press, Y. Crama, P. Hammer (eds.), pp. 257–397, 2010.
6. T. W. Cusick and H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences, IEEE Trans. Inform. Theory, Vol. 42 (4), pp. 1238-1240, 1996.
7. H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Welch case, IEEE Trans. Inform. Theory, Vol. 45 (4), pp. 1271-1275, 1999.
8. R. Gode and S. Gangopadhyay, On second order nonlinearities of cubic monomial Boolean functions, Available at http://eprint.iacr.org/2009/502.pdf
9. G. Gong and K. Khoo, Additive autocorrelation of resilient Boolean functions, In: Selected Areas in Cryptography 2003, LNCS, Vol. ?, pp. 275-90, 2004.
10. H. Eleuch, Photon statistics of light in semiconductor microcavities, J. Phys. B: Atomic, Molecular, and Optical Physics, Vol. 41(5), pp. 055502, 2008.
11. H. Eleuch, Quantum trajectories and autocorrelation function in semiconductor microcavity, Appl. Math. Inf. Sci, 3(2), pp. 185-196, 2009.
12. X. Li, Y. Hu and J. Gao, Lower bounds on the second-order nonlinearity of Boolean functions, *Int'l J. of Found. of Comp. Sci.*, Vol. 22(6), pp. 1331-1349, 2011.
13. X. Li, Y. Hu and J. Gao, Autocorrelation coefficient of two classes of semi-bent functions, Applied Mathematics and Information Sciences, Vol. 5 (1), pp. 85-97, 2011.
14. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.
15. M. Matsui, Linear cryptanalysis method for DES cipher, In: Advances in Cryptology-Eurocrypt93, LNCS, Springer, Berlin, PP. 386-397, 1994.
16. W. Millan, Low-order approximation of cipher functions, In Cryptographic Policy and Algorithms, LNCS, Springer-Verlag, Vol. 1029, pp. 144-155, 1996.
17. O. S. Rothaus, On bent functions, *Journal of Combinatorial Theory, Series A*, Vol. 20, pp. 300-305, 1976.
18. T. Siegenthaler, "Decrypting a clss of stream ciphers using ciphertexts only", IEEE Trans. Comput., Vol. C34 (1), pp. 81-85, 1985.
19. G. Sun and C. Wu, 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, 2009.
20. Y. Tarannikov, P. Korolev and A. Botev, Autocorrelation coefficients and correlation immunity of Boolean functions, In: Advances in Cryptology-Asiacrypt01, Springer, Berlin, pp. 460479, 1994.

21. X. M. Zhang and Y. Zheng, GAC-The criterion for global acalanche criteria of cryptographic functions, Journal for Universal Computer Science, 1(5), pp. 316-333, 1995.
22. Y. Zhou, M. Xie and G. Xiao, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences 180, pp. 256-265, 2010.