On second-order nonlinearity and maximum algebraic immunity of some bent functions in $\mathcal{PS}^{+}$ [1]

Brajesh Kumar Singh

Department of Mathematics,
Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
bksingh0584@gmail.com

Abstract

In this paper, by modifying a subclass of bent functions in $\mathcal{PS}_{ap}$, we construct another subclass of bent functions in $\mathcal{PS}^{+}$ with maximum algebraic degree. We demonstrate that the algebraic immunity of the constructed functions is maximum. The result is proved by using the well known conjecture proposed by Tu and Deng (Des. Codes Cryptogr. 60(1), pp. 1-14, 2011) which has been proved recently by Cohen and Flori (http://eprint.iacr.org/ 2011/400.pdf). Finally, we identify a class of $\mathcal{D}_0$ type bent functions constructed by modifying Dillon functions whose lower bound on second-order nonlinearity is very high.

Keywords: Boolean function, bent function, algebraic immunity, Dillon functions, $\mathcal{D}_0$ type bents, second-order nonlinearities.

1. Introduction

The Boolean functions with desirable cryptographically significant properties is used in various fields and play a prominent role in the security of cryptosystems. One of the most vital roles in cryptography of Boolean functions is to be used as filter and combination generators of stream ciphers based on linear feedback shift registers (LFSRs). Thus, the study of the cryptographic criteria of Boolean functions (mainly balancedness, high algebraic degree, high nonlinearity, correlation immunity and algebraic immunity) is important because of the connections between known cryptanalytic attacks and these criteria.

The first-order nonlinearity, one of the most significant cryptographic property of a Boolean function f (the minimum of Hamming distances of f to all the affine Boolean functions) is related to the immunity of f against *best affine approximation attacks* and *fast correlation attacks*, when f is used as a combiner function or a filter function in a stream cipher. The relationship between nonlinearity and explicit attack on symmetric cipher was discovered by Matsui [23]. The *higher-order nonlinearities* of a Boolean function is the measure of the resistance of the function against various *low-order approximation attacks*, see e.g. [20, 12, 21]. Unlike first-order nonlinearity there is no efficient algorithm to compute second-order nonlinearities for $n > 11$. Most efficient algorithm due to Fourquet and Tavernier [17] works for $n \leq 11$ and, upto $n = 13$ for some special functions.

In recent years algebraic attack (that uses cleverly over defined systems of multivariate nonlinear equations to recover the secret key) has become an important method in cryptographic analyzing stream and block cipher systems, see e.g. [1, 3, 11, 10, 14]. A new cryptographic property, the algebraic immunity that measure the ability of the designed Boolean functions to resist this kind of attack, has been introduced and studied in [2, 11, 3, 14, 15, 24]. The core of the analysis is to find low degree annihilators of f or of $1 \oplus f$. One needs only low-degree annihilators (rather than one) of f or of $1 \oplus f$ to mount algebraic attack easily, e.g. [11, 24]. Several constructions of Boolean functions with optimal algebraic immunity were found subsequently in [2, 4, 14, 15]. Unfortunately, most of the function do

[1] This paper is extended version of the paper presented in NWC 2011

not present high nonlinearity where as the others are unbalanced. Further constructions with high nonlinearity were found in [9, 30, 27, 25, 29].

Bent functions were introduced by Rothaus [26] and later extensively studied in many articles, e.g. [16, 8, 4]. Even though bent functions (exists only for even n) achieve the maximum possible nonlinearity $2^{n-1} - 2^{n/2-1}$, they are not suitable for a direct cryptographic use due to their statistical bias. More precisely, bent functions are unbalanced and therefore possess certain statistical weakness if such a function is used in some standard cryptographic applications. Nevertheless, a classification of bent functions has been extremely dynamic research area for more than 30 years, see e.g. [8, 16]. Recently, a series of construction methods for Boolean functions fulfilling several cryptographic criteria, based on some modifications of a certain class of bent functions called partial spreads [16], has been proposed, see e.g. [30, 27]. The main idea behind the constructions of such type of functions is the use of a particular subclass of functions from $\mathcal{PS}_{ap}$ and extend the support set, that is, the domain set of these functions so that it would give a rise to some new classes of Boolean functions which possess in particular, an optimal resistance to standard algebraic cryptanalysis (it may possibly not to fast algebraic cryptanalysis). This property is closely related to the algebraic properties of the bent function used in the construction.

In connection to the above discussion it is both of theoretical and of practical importance to classify bent functions in terms of their algebraic properties. In this paper, by modifying a subclass of bent functions in $\mathcal{PS}_{ap}$, we construct a subclass of bent functions in $\mathcal{PS}^+$ with maximum algebraic degree and demonstrate that the algebraic immunity of the constructed functions is maximum. We further obtain the lower bound of second-order nonlinearity of $\mathcal{D}_0$ type bent functions constructed by modifying Dillon functions of the form $Tr_1^m(\alpha x y^{2^m-2})$, $\alpha \in \mathbb{F}_{2^m}^*$.

The rest of this paper is organized as follows. In Section 2 some basic definitions and notions are introduced. In Section 3, the algebraic immunity and nonlinearity of the constructed function is derived. In Section 4, second-order nonlinearity of $\mathcal{D}_0$ type bent functions constructed by modifying Dillon functions is obtained. Some concluding remarks are given in Section 5.

2. Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field consisting of 2^n elements. The group of units of $\mathbb{F}_{2^n}$, denoted by $\mathbb{F}_{2^n}^*$, is a cyclic group consisting of $2^n - 1$ elements. Every generator of the multiplicative group $\mathbb{F}_{2^n}^*$ is said to be a primitive element of $\mathbb{F}_{2^n}$. An element in $x \in \mathbb{F}_{2^n}$ can be uniquely associated to an element $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ once a basis of $\mathbb{F}_{2^n}$ is fixed and therefore $\mathbb{F}_2^n$ is isomorphic to $\mathbb{F}_{2^n}$ as $\mathbb{F}_2$-vector spaces. Thus, any function from $\mathbb{F}_{2^n}$ or $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables. Let us denote $\mathcal{B}_n$ be the set of all Boolean functions on n variables. The truth-table of $f \in \mathcal{B}_n$ is a binary string of length 2^n as $[f(0,\ldots,0,0), f(0,\ldots,0,1), f(0,\ldots,1,0), \ldots, f(1,\ldots,1,1)]$. Let $\mathbb{Z}$ be the set of integers. The additions in both $\mathbb{Z}$ and $\mathbb{F}_{2^n}$ are denoted by '+', whereas '⊕' denotes the addition in $\mathbb{F}_2^n$. The Hamming weight of an element $\mathbf{x} \in \mathbb{F}_2^n$ is defined by $w_H(\mathbf{x}) := \sum_{i=1}^n x_i$, where the sum is over $\mathbb{Z}$. The *binary representation* of an integer $d \in \mathbb{Z}$ is

$$d = d_{m-1}2^{m-1} + d_{m-2}2^{m-2} + \ldots + d_1 2 + d_0, \tag{1}$$

where $d_0, d_1, \ldots, d_{m-1} \in \{0, 1\}$. Once the order in which the exponents of 2 appear in (1) is fixed the finite sequence $(d_{m-1}, \ldots, d_0)$ is referred to as the binary representation of d. The Hamming weight of an integer d is $w_H(d) = \sum_{i=0}^{m-1} d_i$. The algebraic normal form (ANF) of $f \in \mathcal{B}_n$ is defined by

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \left(\prod_{i=1}^{n} x_i^{a_i} \right), \mu_{\mathbf{a}} \in \mathbb{F}_2. \tag{2}$$

The algebraic degree of f as represented in (2), is defined by $\deg(f) := \max\{w_H(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0, \mathbf{a} \in \mathbb{F}_2^n\}$. Every Boolean function $h : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ can be expressed in terms of a polynomial of two variables on $\mathbb{F}_{2^m}$ as

$$h(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j, \text{ where } h_{i,j} \in \mathbb{F}_{2^k}. \tag{3}$$

The algebraic degree, denoted by $\deg(h)$, of $h \in \mathcal{B}_{2m}$, as represented in (3), is the largest positive integer w for which $w_H(i) + w_H(j) = w$ and $h_{i,j} \neq 0$. The Hamming distance between f and g in $\mathcal{B}_n$ is defined by $d_H(f, g) =$

$|\{x \in \mathbb{F}_{2^n} | f(x) \neq g(x)\}|$, where $|S|$ is the cardinality of any set S. The support of a Boolean function $f \in \mathcal{B}_n$ is $supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$. The weight of f is $w_H(f) = |\{x \in \mathbb{F}_{2^n} : f(x) = 1\}|$. It is easily observed that $d_H(f, g) = w_H(f + g) = 2^{n-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+g(x)}$.

A Boolean function $g \in \mathcal{B}_n$ is said to be an annihilator of $f \in \mathcal{B}_n$ if and only if g is not identically zero and $g(x)f(x) = 0$ for all $x \in \mathbb{F}_{2^n}$ ($g \neq 0$ and $gf = 0$, in short). Let $\mathcal{AN}(f)$ be the set of all annihilators of $f \in \mathcal{B}_n$, that is

$$\mathcal{AN}(f) = \{g \in \mathcal{B}_n : g \neq 0, gf = 0\}.$$

Definition 2.1. *The algebraic immunity, $\mathcal{AI}(f)$, of $f \in \mathcal{B}_n$ is defined as*

$$\mathcal{AI}(f) = \min\{\deg(g) : g \in \mathcal{AN}(f) \cup \mathcal{AN}(\bar{f})\},$$

where $\bar{f}$ denotes the complement of the function f.

Suppose $gf = h$ where $\deg(g)$ and $\deg(h)$ both are at most d, and $g \neq h$. Then by [24, Proposition 1] f has an annihilator with algebraic degree at most d and hence $\mathcal{AI}(f) \leq d$. Since $\bar{f}f = 0$ is it trivial that $\mathcal{AI}(f) \leq \deg(f)$.

Proposition 2.1. *[11, Theorem 6.0.1] Let $f \in \mathcal{B}_n$. Then there is a Boolean function $g \in \mathcal{B}_n$ with $g \neq 0$ of degree at most $\lceil \frac{n}{2} \rceil$ such that gf is of degree at most $\lceil \frac{n}{2} \rceil$.*

Thus, for any $f \in \mathcal{B}_n$, we have

$$\mathcal{AI}(f) \leq \min\left\{\deg(f), \left\lceil \frac{n}{2} \right\rceil\right\}. \tag{4}$$

A trace function $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$, 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 Walsh–Hadamard transform (WHT) of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}. \tag{5}$$

For $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, the WHT at $(\lambda, \mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is

$$W_f(\lambda, \mu) = \sum_{(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}} (-1)^{f(x,y)+Tr_1^m(\lambda x + \mu y)}.$$

The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}]$ is said to be the Walsh–Hadamard spectrum of the Boolean function f. The Walsh–Hadamard spectrum of $f \in \mathcal{B}_n$ satisfies Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f^2(\lambda) = 2^{2n}. \tag{6}$$

The nonlinearity of $f \in \mathcal{B}_n$ in terms of WHT is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_f(\lambda)|. \tag{7}$$

For any even positive integer $n = 2m \in \mathbb{Z}$, there exist Boolean functions with "flat" Walsh–Hadamard spectra. These functions are said to be bent functions and as a consequence of (6), a function $f \in \mathcal{B}_n$ (for $n = 2m$) is bent if and only if $|W_f(\lambda)| = 2^m$ for all $\lambda \in \mathbb{F}_{2^n}$. The dual, $\tilde{f}$, of a bent function $f \in \mathcal{B}_{2m}$ is defined by $W_f(x) = (-1)^{\tilde{f}(x)} 2^m$ for all $x \in \mathbb{F}_{2^{2m}}$, is again bent. It is known that the bent functions provide maximum resistance to linear approximations and therefore play a major role in construction of cryptographic Boolean functions.

Definition 2.2. *The derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as*

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

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 be further generalized. For more details we refer to [7].

2.1. Higher-order nonlinearities of Boolean functions

The set of all Boolean functions in $\mathcal{B}_n$ with algebraic degrees less than or equal to r is said to be the Reed–Muller code of order r and length 2^n and denoted by $RM(r,n)$.

Definition 2.3. *The rth-order nonlinearity of $f \in \mathcal{B}_n$ is defined as*

$$nl_r(f) = \min_{h \in RM(r,n)} d_H(f,h) = 2^{n-1} - \frac{1}{2} \max_{h \in RM(r,n)} |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+h(x)}|.$$

The sequence of values $\{nl_r(f)\}_{r=1}^{n-1}$ is said to be the nonlinearity profile of f. The first order nonlinearity of f is $nl_1(f)$, is the nonlinearity $nl(f)$ of f.

A vectorial Boolean function $F_{inv} : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ defined by $F_{inv}(x) = x^{2^n-2}$ is called an inverse function. It is a permutation because of $\gcd(2^n-2, 2^n-1) = \gcd(2^{n-1}-1, 2^n-1) = 2^{\gcd(n,n-1)}-1 = 1$. Let us denote $g_\alpha(x) = Tr_1^n(\alpha x^{2^n-2})$, $\alpha \in \mathbb{F}_{2^n}^*$. Then all the Boolean functions g_α, $\alpha \in \mathbb{F}_{2^n}^*$, are affine equivalent to each other. Thus, the nonlinearity profiles of these functions are same. The following proposition is due to Carlet [5].

Proposition 2.2. *[5] The nonlinearity of an inverse function $g_\alpha(x) = Tr_1^n(\alpha x^{2^n-2})$, where $\alpha \in \mathbb{F}_{2^n}^*$ is lower bounded by $2^{n-1} - 2^{\frac{n}{2}}$ or equivalently*

$$|W_{g_\alpha}(\mathbf{u})| \leq 2^{\frac{n+2}{2}}, \textit{ for all } \mathbf{u} \in \mathbb{F}_{2^n}.$$

The nonlinearity of the first derivative of a Dillon function at every point $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and hence its second-order nonlinearity due to Carlet [6] is provided in the following

Proposition 2.3. *[6, Lemma 1] Every derivative $D_{(a,b)}f_\alpha$, $a \in \mathbb{F}_{2^m}, b \in \mathbb{F}_{2^m}^*$, of the Dillon function has first-order nonlinearity at least $2^{2m-1} - 2^{m+1}$. Every derivative $D_{(a,0)}f_\alpha$, $a \in \mathbb{F}_{2^m}^*$ has first-order nonlinearity at least $2^{2m-1} - 2^{\frac{3m}{2}} - 2^m$.*

Proposition 2.4. *[6] The second-order nonlinearity of a Dillon function, $f_\alpha(x,y) = Tr_1^m(\alpha xy^{2^m-2})$, for all $x, y \in \mathbb{F}_{2^m}$, where $\alpha \in \mathbb{F}_{2^m}^*$ is*

$$nl_2(f_\alpha) \quad \geq \quad 2^{2m-1} - 2^{\frac{3m}{2}}. \tag{8}$$

In the following proposition Garg and Gangopadhyay [19] obtained the lower bound of second-order nonlinearities of cubic Niho bent functions.

Proposition 2.5. *[6] Let $f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, where $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$, with $\alpha_1 + \overline{\alpha_1} = ||\alpha_2||$, e be a positive integer such that $n = 2e$, and $d_1 = (2^e - 1)\frac{1}{2} + 1$ and $d_1 = (2^e - 1)\frac{1}{4} + 1$ are Niho exponents. Then*

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

Following proposition is due to Carlet [5] for the computation of lower bounds on nonlinearity profiles of Boolean functions in a recursive framework which we use to compute our bound.

Proposition 2.6. *[5, Proposition 3] Let $f \in \mathcal{B}_n$ and r be a positive integer $(r < n)$, then we have*

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

3. Bent functions with optimal algebraic immunity in $\mathcal{PS}$

Throughout this section $n = 2m$. The partial spreads ($\mathcal{PS}$) class of bent functions has been introduced by Dillon [16], and the properties of this class have been studied in many recent works. This class is divided into two subclasses, namely $\mathcal{PS}^-$ and $\mathcal{PS}^+$ depending on the size of the supports. A function $f \in \mathcal{B}_{2m}$ is in the $\mathcal{PS}^-$ class if its support is a collection of 2^{m-1} "disjoint" m-dimensional subspaces of $\mathbb{F}_{2^{2m}}$ with the additive identity $0 \in \mathbb{F}_{2^{2m}}$ discarded, where "disjoint" means that any pair of these subspaces intersects only in 0. In a similar way, a function in the $\mathcal{PS}^+$ class is constructed by selecting $2^{m-1} + 1$ "disjoint" m-dimensional subspaces of $\mathbb{F}_2^{2m}$ (with the $0 \in \mathbb{F}_{2^{2m}}$ included). It is to be noted that, depending on the choice of these m-dimensional flats it might be the case that the support of a bent function f in $\mathcal{PS}^-$ (or in $\mathcal{PS}^+$) is such that $\tilde{f}$ is not in $\mathcal{PS}^+$ (or in $\mathcal{PS}^-$).

There are some fundamental differences between the two subclasses. It is well known that the degree of any function $f \in \mathcal{B}_{2m}$ in $\mathcal{PS}^-$ class is always equal to m whereas this is not the case for functions in $\mathcal{PS}^+$ whose degrees may be less than m, see e.g. [16, 28]. The algebraic representation of the bent functions in the $\mathcal{PS}$ class appears to be hard. Dillon [16] exhibits one explicit representation of a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, consisting of functions defined as follows:

$$\begin{aligned} f \quad &: \quad \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2 \\ f(x,y) \quad &= \quad g(xy^{2^m-2}), \quad x, y \in \mathbb{F}_{2^m}, \end{aligned} \tag{9}$$

where $g \in \mathcal{B}_m$ is any balanced Boolean function such that $g(0) = 0$. It was shown [27] that the selection of the support of g is of great importance. Indeed, if we consider a balanced $g : \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$supp(g) = \{\alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+2^{m-1}-1}\} = \triangle(\text{say}), \tag{10}$$

for some integer $s \geq 0$ and a primitive element $\alpha \in \mathbb{F}_{2^m}$, then $\mathcal{AI}(f) = m$ [27, Construction 1]. This result was proved using the famous BCH bound and a conjecture (given below) proposed by Tu and Deng [27] which has been proved quite recently [13].

Conjecture 1. [27, Tu and Deng] For any $t \in \mathbb{Z}_{2^m-1} \setminus \{0\}$, if

$$S_t = \{(a,b) \in \mathbb{Z}_{2^m-1} \times \mathbb{Z}_{2^m-1}, a + b = t \mod (2^m - 1), w_H(a) + w_H(b) \leq m - 1\},$$

then $|S_t| \leq 2^{m-1}$.

The definition of BCH bound as well as BCH code in coding theory [22], provided below

Theorem 3.1. *(The BCH bound) Let α be a primitive n-root of unity. Let Φ be a cyclic code of length n and with a generator polynomial $g(x)$ such that for some integers $b \geq 0$, $\delta \geq 1$*

$$g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+\delta-2}) = 0,$$

that is, the code has string of $\delta - 1$ consecutive powers of α as zeroes, then the minimal distance of Φ is at lest δ.

The BCH code is defined as follows:

Definition 3.1. *A cyclic code of length n over $\mathbb{F}_q$ is a BCH code of designed distance δ if, for some integer $b \geq 0$*

$$g(x) = \mathrm{lcm}\{m^{(b)}(x), m^{(b+1)}(x), \ldots, m^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the lowest degree monic polynomial over $\mathbb{F}_q$ having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeroes, when $m^{(i)}$ is the minimal polynomial of α^i over $\mathbb{F}_q$.

A natural question whether there exist a class of bent functions in $\mathcal{PS}^+$ having maximum algebraic immunity. We answer this in affirmative by considering a subclass of bent functions as mentioned in the following section.

3.1. Algebraic immunity of bent functions obtained by modifying Dillon functions

In this section, we construct a subclass of functions by modifying functions in $\mathcal{PS}_{ap}$ and demonstrate that these functions are bent functions belonging to $\mathcal{PS}^+$ having maximum algebraic immunity.

Construction 1 Let $n = 2m$ and α be a primitive element of $\mathbb{F}_{2^m}$. Let $g \in \mathcal{B}_m$ and $\triangle$ are same as in (10). If the support of the Boolean function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined as

$$supp(f) = \{(0, y) : y \in \mathbb{F}_{2^m}\} \cup \{(\gamma y, y) : y \in \mathbb{F}^*_{2^m}, \gamma \in \triangle\}.$$

Then f is bent and $\mathcal{AI}(f) = m$.

Theorem 3.2. *Let $f \in \mathcal{B}_n$ as defined in Construction 1, then $\mathcal{AI}(f) = m$.*

Proof 3.1. *To prove that f have algebraic immunity m, it is sufficient to prove that both f and $\bar{f}$ have no annihilators of algebraic degrees less than m.*

Let us suppose $h \in \mathcal{B}_{2m}$ be a non zero function as expressed in (3) with $\deg(h) < k$ and $fh = 0$, then we will show that $h = 0$. By assumption, we have $h(x, y) = 0$ for all $(x, y) \in supp(f) = \{(0, y) : y \in \mathbb{F}_{2^m}\} \cup \{(\gamma y, y) : y \in \mathbb{F}^*_{2^m}, \gamma \in \triangle\}$, and $h_{i,j} = 0$ if $w_H(i) + w_H(j) \geq m$.

$h(0, y) = 0$ for all $y \in \mathbb{F}_{2^m}$ implies that $h_{0,t} = 0$ for all $0 \leq t \leq 2^m - 1$. Also, $h(\gamma y, y) = 0$ for all $y \in \mathbb{F}^*_{2^m}$ and $\gamma \in \triangle$.

$$h(\gamma y, y) = \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^m-1} h_{i,j}(\gamma y)^i y^j = \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^m-1} h_{i,j}\gamma^i y^{i+j} = h_{0,0} + \sum_{t=0}^{2^m-1} h_t(\gamma) y^t,$$

where

$$h_t(\gamma) = \sum_{i=0}^{t} h_{i,t-i}\gamma^i + \sum_{i=t}^{2^m-1} h_{i,2^m-1+t-i}\gamma^i.$$

It is observed from [27] that $w_H(i) + w_H(2^m - 1 - i) = m$ which implies that $h_{2^m-1} = 0$ and $h_{t,2^m-1} = h_{2^m-1,t} = 0$ for all t. Using these values in the above equation, we have

$$h_t(\gamma) = \sum_{i=0}^{t} h_{i,t-i}\gamma^i + \sum_{i=t+1}^{2^m-2} h_{i,2^m-1+t-i}\gamma^i,$$

which implies that

$$h(\gamma y, y) = h_{0,0} + \sum_{i=1}^{2^m-2} h_t(\gamma) y^t.$$

For some fixed $\gamma \in \triangle$, since $h(\gamma y, y) = 0$ for all $y \in \mathbb{F}^*_{2^m}$, it follows that

$$h_{0,0} = 0 \text{ and } h_t(\gamma) = 0, 1 \leq t \leq 2^m - 1, \text{ for all } \gamma \in \triangle.$$

By the definition of BCH code, $(h_{0,t}, h_{1,t-1}, \ldots, h_{t,0}, h_{t+1,2^m-2}, \ldots, h_{2^m-2,t+1})$ be a codeword in some BCH code of length $2^m - 1$ over $\mathbb{F}_{2^m}$, having the elements in $\triangle$ as zeros and with designed distance $2^{m-1} + 1$. If this codeword is nonzero, then by definition of BCH bound the weight should be greater than or equal to $2^{m-1} + 1$. Further, from Conjecture 1 and $h_{0,t} = 0$, the weight should be strictly less than 2^{m-1}, leads a contradiction. Hence, $h = 0$. It means that there exist no annihilator of f having algebraic degree strictly less than m.

Now, we will prove that $\bar{f}$ also have no annihilator of algebraic degree strictly less than m.

Let us suppose $h : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a non zero function with $\deg(h) < m$ and $\bar{f}h = 0$, then we will show that $h = 0$. It can be easily observed that

$$supp(\bar{f}) = \{(\gamma y, y) : y \in \mathbb{F}^*_{2^m}, \gamma \in \mathbb{F}^*_{2^m} \setminus \triangle\} \cup \{(x, 0) : x \in \mathbb{F}^*_{2^m}\}.$$

$h(x, 0) = 0$ for all $x \in \mathbb{F}^*_{2^m}$ which implies that $h_{t,0} = 0$ for all $1 \leq t \leq 2^m - 1$. Similarly $h(\gamma y, y) = 0$ for all $y \in \mathbb{F}^*_{2^m}$ and $\gamma \in \mathbb{F}^*_{2^m} \setminus \triangle$. It follows that $h_{0,0} = 0$ and $h_t(\gamma) = 0$, $1 \leq t \leq 2^m - 2$ for all $\gamma \in \mathbb{F}^*_{2^m} \setminus \triangle$. Thus we can see that

$(h_{0,t}, h_{1,t-1}, \dots, h_{t,0}, h_{t+1,2^m-2}, \dots, h_{2^m-2,t+1})$ be a codeword in some BCH code of length $2^m - 1$ over $\mathbb{F}_{2^m}$, having the elements in $\mathbb{F}_{2^m}^* \setminus \triangle = \{\alpha^{2^{m-1}}, \alpha^{2^{m-1}+1}, \dots, \alpha^{2^m-2}\}$ as zeros and with designed distance 2^{m-1}. If this codeword is nonzero, then by definition of BCH bound the weight should be greater than or equal to 2^{m-1}. Further, from Conjecture 1 and $h_{t,0} = 0$, the weight should be strictly less than 2^{m-1}, leads a contradiction, this implies that $h = 0$.

Thus, we have neither f nor $\overline{f}$ have an annihilator of degree strictly less than m. This completes the theorem.

Theorem 3.3. *The function $f(x, y)$ as defined in Construction 1 is bent and its dual $\tilde{f}$ is given by*

$$supp(\tilde{f}) = \{(x, \gamma x) : x \in \mathbb{F}_{2^m}^*, \gamma \in \triangle\} \cup \{(x, 0) : x \in \mathbb{F}_{2^m}\}.$$

Proof 3.2. *Since $supp(f) = \{(0, y) : y \in \mathbb{F}_{2^m}\} \cup \{(\gamma y, y) : y \in \mathbb{F}_{2^m}^*, \gamma \in \triangle\}$. Therefore, $w_H(f) = 2^m + 2^{m-1}(2^m - 1) = 2^{2m-1} + 2^{m-1}$ which implies that $W_f(0, 0) = -2^m$. Let $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ such that both a and b are not zero simultaneously. We compute,*

$$\begin{aligned} W_f(a, b) &= \sum_{(x,y)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}} (-1)^{f(x,y)+Tr(ax+by)} = -2 \sum_{(x,y)\in supp(f)} (-1)^{Tr(ax+by)} \\ &= -2 \sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr(by)} - 2 \sum_{\gamma\in\triangle} \sum_{y\in\mathbb{F}_{2^m}^*} (-1)^{Tr((a\gamma+b)y)} \\ &= -2^{m+1}\delta_0(b) - 2 \sum_{\gamma\in\triangle} \left(\sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr((a\gamma+b)y)} - 1 \right) \\ &= -2^{m+1}\delta_0(b) + 2^m - 2 \sum_{\gamma\in\triangle} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr((a\gamma+b)y)} \\ &= -2^{m+1}\delta_0(b) + 2^m - 2^{m+1} \sum_{\gamma\in\triangle} \delta_0(a\gamma + b) \end{aligned}$$

Consider the following cases

***Case 1.** If $b = 0$ and $a \neq 0$ then $a\gamma \neq 0$ for all $\gamma \in \triangle$ which implies that $\delta_0(a\gamma) = 0$ for all $\gamma \in \triangle$. Therefore, $W_f(a, 0) = -2^{m+1} + 2^m = -2^m$ for all $a \in \mathbb{F}_{2^m}^*$.*

***Case 2.** If $a = 0$ and $b \neq 0$, clearly $\delta_0(b) = 0$. Therefore, $W_f(0, b) = 2^m$ for all $b \in \mathbb{F}_{2^m}^*$.*

***Case 3.** If $a, b \in \mathbb{F}_{2^m}^*$. Now, consider the following two subcases.*

(i) If $(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}^*$ such that $a\gamma = b$ for some $\gamma_0 \in \triangle$, then $a\gamma_0 + b = 0$, that is $\delta_0(a\gamma + b) = 1$ if $\gamma = \gamma_0$ which implies that $W_f(a, b) = 2^m - 2^{m+1} = -2^m$.

(ii) If $(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}^*$ such that there exists no element $\gamma \in \triangle$ so that $a\gamma = b$, then $a\gamma + b \neq 0$, that is $\delta_0(a\gamma + b) = 0$ for all $\gamma \in \triangle$. This implies that $W_f(a, b) = 2^m$.

Thus, we have $W_f(a, b) = 2^m(-1)^{\tilde{f}(a,b)}$ for all $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where the support of $\tilde{f}$ is given by

$$supp(\tilde{f}) = \{(x, \gamma x) : x \in \mathbb{F}_{2^m}^*, \gamma \in \triangle\} \cup \{(x, 0) : x \in \mathbb{F}_{2^m}\}.$$

This completes the theorem.

Corollary 3.1. *The algebraic degree of the Boolean function f as defined in Construction 1 is $\deg(f) = m$.*

Proof 3.3. *It is well known that $\deg(f) \geq \mathcal{AI}(f)$ for all the Boolean functions. Since the algebraic immunity of $f \in \mathcal{B}_{2m}$ as defined in Construction 1 is $\mathcal{AI}(f) = m$ and therefore $\deg(f) \geq m$. Moreover, since f is bent which implies that $\deg(f) = m$.*

Remark 3.1. *The Boolean function f as defined in Construction 1 is represented by*

$$f(x, y) = g(xy^{2^m-2}) + \prod_{j=1}^{m} (x_j \oplus 1),$$

where $g \in \mathcal{B}_m$ be a balanced Boolean function with $g(0) = 0$.

4. Second-order nonlinearities of $\mathcal{D}_0$ type functions

A function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined as $f(x,y) = Tr_1^m(x\pi(y)) + \ell(y)$ for all $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where π is a permutation on $\mathbb{F}_{2^m}$ and ℓ is any function on $\mathbb{F}_{2^m}$, is bent. The collection of bent functions of this type is called the Maiorana-McFarland class, denoted by $\mathcal{M}$. Carlet [8] constructed a class of bent functions referred to as the class $\mathcal{D}$ by modifying the functions of the class $\mathcal{M}$. Further Carlet constructed a subclass $\mathcal{D}_0$ of $\mathcal{D}$ which is defined below.

Definition 4.1. *A Boolean function $h : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ belongs to $\mathcal{D}_0$ if and only if*

$$h(x,y) = Tr_1^m(x\pi(y)) + g(x) \textit{ for all } (x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where π be a permutation on $\mathbb{F}_{2^m}$ and $g(x) = \prod_{i=1}^m (x_i \oplus 1)$.

For details we refer [8].

The following proposition is due to Gangopadhyay and Singh [18] which we use to obtain our bound.

Proposition 4.1. *[18, Theorem 3.1] Suppose $h(x,y) = f(x,y) + \prod_{j=1}^m (x_j \oplus 1)$, for all $x,y \in \mathbb{F}_2^m$, where $f(x,y) = Tr_1^m(x\pi(y))$, for some permutation π on $\mathbb{F}_{2^m}$. Then*

$$|W_{D_{(a,b)}h}(\mu,\eta)| \le |W_{D_{(a,b)}f}(\mu,\eta)| + 4|W_{a\cdot\pi}(\eta)|.$$

Using Proposition 4.1, Gangopadhyay and Singh obtained the lower bounds on second-order nonlinearities of two classes [18, Theorem 3.3, 3.4] of $\mathcal{D}_0$ type bent functions constructed by modifying the cubic Maiorana-McFarland type bent functions. It is observed that even the constructed functions are bent having maximum algebraic degree and good second-order nonlinearities but their algebraic immunity is still remain at most 4 for all n, and therefore, could not be improved. In the following section we obtain the lower bound of second-order nonlinearities of $\mathcal{D}_0$ type functions by modifying Dillon functions of the form $Tr_1^m(\alpha x y^{2^m-2})$, $\alpha \in \mathbb{F}_{2^m}^*$.

4.1. Functions obtained by modifying $Tr_1^m(\alpha x y^{2^m-2})$

The lower bounds of nonlinearities of the derivatives of the constructed functions at every point $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is provided in the following

Lemma 4.1. *Let $h_\alpha : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function defined as*

$$h_\alpha(x,y) = f_\alpha(x,y) + \prod_{j=1}^m (x_j \oplus 1), \textit{ for all } x,y \in \mathbb{F}_{2^m},$$

where $f_\alpha(x,y) = Tr_1^m(\alpha x y^{2^m-2})$ and $\alpha \in \mathbb{F}_{2^m}^*$. Then every derivative, $D_{(a,b)}h_\alpha$, $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ of the function h_α has first-order nonlinearity at least

$$nl(D_{(a,b)}f_\alpha) - 2\max_{\beta \in \mathbb{F}_{2^m}} |W_{a\cdot g_\alpha}(\beta)|,$$

where $g_\alpha(y) = Tr_1^m(\alpha y^{2^m-2})$. Therefore,

$$nl(D_{(a,b)}h_\alpha) \ge \begin{cases} 2^{2m-1} - 2^{\frac{3m}{2}} - 2^m - 2^{\frac{m+4}{2}}, & \textit{if } a \in \mathbb{F}_{2^m}^*, b = 0, \\ 2^{2m-1} - 2^{m+1}, & \textit{if } a = 0, b \in \mathbb{F}_{2^m}^*, \\ 2^{2m-1} - 2^{m+1} - 2^{\frac{m+4}{2}}, & \textit{if } a, b \in \mathbb{F}_{2^m}^*. \end{cases} \tag{11}$$

Proof 4.1. *By Proposition 4.1, the nonlinearity of $D_{(a,b)}h_\alpha$ is*

$$\begin{aligned} nl(D_{(a,b)}h_\alpha) &= 2^{n-1} - \frac{1}{2}\max_{(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}} |W_{D_{(a,b)}h_\alpha}| \\ &\ge (2^{2m-1} - \frac{1}{2}\max_{(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}} |W_{D_{(a,b)}f_\alpha}|) - 2\max_{\mu\in\mathbb{F}_{2^m}} |W_{a\cdot g_\alpha}(\mu)| \\ &= nl(D_{(a,b)}f_\alpha) - 2\max_{\mu\in\mathbb{F}_{2^m}} |W_{a\cdot g_\alpha}(\mu)|. \end{aligned}$$

Using Proposition 2.2 and Proposition 2.3 in the above equation, we have

$$nl(D_{(a,b)}h_\alpha) \geq \begin{cases} 2^{2m-1} - 2^{\frac{3m}{2}} - 2^m - 2^{\frac{m+4}{2}}, & if\, a \in \mathbb{F}_{2^m}^*, b = 0, \\ 2^{2m-1} - 2^{m+1}, & if\, a = 0, b \in \mathbb{F}_{2^m}^*, \\ 2^{2m-1} - 2^{m+1} - 2^{\frac{m+4}{2}}, & if\, a, b \in \mathbb{F}_{2^m}^*. \end{cases}$$

Theorem 4.1. *Let $h_\alpha(x,y) = Tr_1^m(\alpha x y^{2^m-2}) + \prod_{j=1}^m (x_j \oplus 1)$, for all $x, y \in \mathbb{F}_{2^m}$, where $n = 2m$ and $\alpha \in \mathbb{F}_{2^m}^*$, then*

$$nl_2(h_\alpha) \geq 2^{2m-1} - \frac{1}{2}\sqrt{2^{3m+2} + 10(2^{\frac{5m}{2}} - 2^{\frac{3m}{2}}) - 2^{2m} - 2^{m+1}}.$$

Proof 4.2. *Using (11) we have*

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^m}} nl(D_{(a,b)}h_\alpha) &= nl(D_{(0,0)}h\alpha) + \sum_{b\in\mathbb{F}_{2^m}^*} nl(D_{(0,b)}h\alpha) + \sum_{a\in\mathbb{F}_{2^m}^*} nl(D_{(a,0)}h\alpha) + \sum_{a,b\in\mathbb{F}_{2^m}^*} nl(D_{(a,b)}h\alpha) \\ &\geq (2^m - 1)(2^{2m-1} - 2^{m+1}) + (2^m - 1)(2^{2m-1} - 2^{\frac{3m}{2}} - 2^m - 2^{\frac{m+4}{2}}) \\ &\quad + (2^m - 1)(2^m - 1)(2^{2m-1} - 2^{m+1} - 2^{\frac{m+4}{2}}) \\ &= (2^m - 1)(2^{2m-1} - 2^{\frac{3m}{2}} - 2^m + 2^{3m-1} - 2^{2m+1} - 2^{\frac{3m+4}{2}}) \\ &= 2^{4m-1} + 2^{2m-1} - 5(2^{\frac{5m}{2}} - 2^{\frac{3m}{2}}) - 2^{3m+1} + 2^m\end{aligned}$$

Using Proposition 2.6 we have

$$\begin{aligned} nl_2(h_\alpha) &\geq 2^{2m-1} - \frac{1}{2}\sqrt{2^{4m} - 2(2^{4m-1} + 2^{2m-1} - 5(2^{\frac{5m}{2}} - 2^{\frac{3m}{2}}) - 2^{3m+1} + 2^m)} \\ &= 2^{2m-1} - \frac{1}{2}\sqrt{2^{3m+2} + 10(2^{\frac{5m}{2}} - 2^{\frac{3m}{2}}) - 2^{2m} - 2^{m+1}}. \end{aligned} \quad (12)$$

From Table 1, it is observed that the lower bounds of second-order nonlinearities of f_α and h_α as represented in (8) and (12) respectively, are asymptotically equal.

Table 1: Comparison of the values of lower bounds of second-order nonlinearities $\mathcal{D}_0$ and associated Dillon functions and the functions obtained in [19]

$n = 2m$	8	10	12	14	16	18	20
Bounds obtained in Theorem 4.1	48	297	1464	6595	28367	118868	490270
The bound obtained in [19]	51	256	1187	5296	23027	98304	414071
The bound obtained in [6]	64	331	1536	6744	28672	119487	491520
Hamming Distance in [17]	84	400	1760	7416	−−	−−	−−

Open problem: The lower bounds of rth-order nonlinearities for $r > 2$ of the constructed functions, h_α as represented in Theorem 4.1, is still a challenging problem.

5. Conclusion

In this paper, we construct a subclass of $\mathcal{PS}^+$ type bent functions modifying bent functions in $\mathcal{PS}_{ap}$ class. By using the conjecture proposed in [27], we demonstrate that the constructed functions have maximum algebraic immunity and hence algebraic degree. Further, using the technique proposed in [18, Theorem 3.1], we deduce a sharper lower bound on second-order nonlinearities some $\mathcal{D}_0$ type bent functions constructed by modifying Dillon functions [6].

From Table 1, we observed that the bound of second-order nonlinearity the functions considered in Theorem 4.1 is improved upon the bound obtained by Garg and Gangopadhyay [19] for all $n > 8$. Moreover, the bounds are asymptotically equal to the associated Dillon functions. Thus we identify a class of bent functions with maximum algebraic degree and high possible second-order nonlinearities.

Acknowledgment: The author, B. K. Singh would like to thank CSIR, India for financial support.

References

[1] F. Armknecht, *Improving fast algebraic attacks*, in Proc. Workshop on Fast Software Encryption (FSE-2004), LNCS 3017, 6582, 2004.

[2] A. Braeken and B. Preneel, *On the algebraic immunity of symmetric Boolean functions*, INDOCRYPT 2005, LNCS 3797, 35–48, 2005.

[3] A. Canteaut, *Open problems related to algebraic attacks on stream ciphers*, WCC 2005, LNCS 3969, 120–134, 2006.

[4] C. Carlet, *Improving the algebraic immunity of resilient and nonlinear functions and constructing bent functions*, available at: http://eprint.iacr.org/2004/276.

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

[6] Carlet C., *More vectorial Boolean functions with unbounded nonlinearity profile*, *Int'l J. of Found. of Comp. Sci.*, 22(6), 1259-1269, 2011.

[7] 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.), 257–397, 2010.

[8] C. Carlet, *Two new classes of bent functions,* in Proc. EROCRYPT 1993, LNCS 765, 77-101, 1994.

[9] C. Carlet and K. Feng, *An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity*, Adv. in Crypto. ASIACRYPT 2008, LNCS 5350, 425-440, 2008.

[10] N. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, CRYPTO 2003, LNCS 2729, 176-194, 2003.

[11] N. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, EUROCRYPT 2003, LNCS 2656, 346–359, 2003.

[12] N. Courtois, Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, in: Proceedings of the ICISC 2002, LNCS 2587, 182-199, 2002.

[13] G. Cohen and J-P. Flori, *On a generalized combinatorial conjecture involving addition mod* $2^k - 1$, available at http://eprint.iacr.org/2011/400.

[14] D. K. Dalai, K. C. Gupta and S. Maitra, *Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity*, FSE 2005, LNCS 3557, 98-111, 2005.

[15] D. K. Dalai, S. Maitra and S. Sarkar, *Basic theory in construction of Boolean functions with maximum possible annihilator immunity*, Des. Codes Cryptography, 40 (1), 41–58, 2006.

[16] J. F. Dillon, *Elementary Haddamard Difference Sets*, Ph. D. thesis, University of Maryland, U.S.A., 1974.

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

[18] S. Gangopadhyay and B. K. Singh, *On second-order nonlinearities of some* $\mathcal{D}_0$ *type bent functions*, Fundamenta Informaticae, 114(3-4), 271-285, 2012.

[19] M. Garg and S. Gangopadhyay, *A lower bound of the second-order nonlinearities of Boolean bent functions*, Fundamenta Informaticae, 111(4), 413-422, 2011.

[20] J. Golić, *Fast low order approximation of cryptographic functions*, in: Proceedings of the EUROCRYPT 1996, LNCS 1070, 268-282, 1996.

[21] T. Iwata and K. Kurosawa, *Probabilistic higher order differential attack and higher order bent functions*, ASIACRYPT 1999, LNCS 1716, 62-74, 1999.

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

[23] M. Matsui, *Linear cryptanalsis methods for DES cipher*, in Proc. of the EUROCRYPT 1993, LNCS 765, 386–397, 1994.

[24] W. Meier, E. Pasalic, and C. Carlet, *Algebraic attacks and decomposition of Boolean functions*, EUROCRYPT 2004, LNCS 3027, 474–491, 2004.

[25] L. Qu, K. Feng, F. Liu, and L. Wang, *Constructing symmetric Boolean functions with maximum algebraic immunity*, IEEE Trans. Inform. Theory, 55 (5), 2406–2412, 2009.

[26] O. S. Rothaus, *On bent functions*, J. Combin. Theory, IDA CRD W. P. 169(1966).

[27] Z. Tu and Y. Deng, *A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity*, Des. Codes Cryptography, 60 (1),1–14, 2011.

[28] G. Vega, *Some precisions on* $\mathcal{PS}$ *bent functions*, International Mathematical Forum, 5, 537–544, 2010.

[29] Q. Wang, J. Peng, H. Kan, and X. Xue, *Constructions of cryptographically significant Boolean functions using primitive polynomials*, IEEE Trans. Inform. Theory, 56 (6), 3048–3053, 2010.

[30] X. Zeng, C. Carlet, J. Shan and L. Hu, *More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks,* IEEE Trans. on Inform. Theory, IT-57(9), 6310-6320, 2010.