The Good lower bound of Second-order nonlinearity of a class of Boolean function

Sugata Gangopadhyay, Manish Garg
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee-247667, Uttarakhand, India
gsugata@gmail.com, manishiitr8@gmail.com

Abstract

In this paper we find the lower bound of second-order nonlinearity of Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. It is also demonstrated that the lower bound obtained in this paper is much better than the lower bound obtained by Iwata-Kurosawa [14], and Gangopadhyay et al. (Theorem 1, [12]).

Key words: Boolean function · Higher-order derivatives · Second-order nonlinearity · Walsh-spectrum
Mathematics Subject Classifications (2000) 94A60 · 94C10 · 06E30

1 Introduction

Let $\mathbb{F}_2 = \{0, 1\}$ be the prime field of characteristic 2. Let $\mathbb{F}_2^n$ be an n-dimensional vector space over $\mathbb{F}_2$. There is a vector space isomorphism between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, $\mathbb{F}_{2^n}$ is the finite extension field over $\mathbb{F}_2$ of degree n. Therefore, $\mathbb{F}_2^n$ can be viewed as $\mathbb{F}_{2^n}$. Boolean function on n-variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$(equivalently from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$). The set of all Boolean functions on n- variables is denoted $\mathcal{B}_n$. The Hamming weight of $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ is defined as $wt(x) = \sum_{i=1}^n x_i$. The hamming distance between two Boolean functions f and g is defined as $d(f, g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|$, where the cardinality of a set S is denoted by $|S|$. The Algebraic Normal Form (ANF) of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$f(x = x_1, x_2, ..., x_n) = \bigoplus_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a(\prod_{i=1}^n x_i^{a_i}),$$

where $\mu_a \in \mathbb{F}_2$ for all $a \in \mathbb{F}_2^n$. The maximum value of wt(a) such that $\mu_a \neq 0$ is called the algebraic degree of f and denoted by $\deg(f)$. The rth-order Reed–Muller code $R(r, n)$ of length 2^n and of order r is the set of all Boolean functions on n-variables with algebraic degree at most r.

Definition 1.1 *The nonlinearity of Boolean function $f \in \mathbb{F}_2^n$ is defined as the minimum Hamming distance of f from all affine Boolean functions (affine Boolean functions are those Boolean functions whose algebraic degree are at most 1). Mathematically*

$$nl(f) = min\{d_H(f, l)|l \in \mathcal{A}_n\},$$

where $\mathcal{A}_n$ is the set of all affine Boolean function on n-varibles.

Definition 1.2 *Let $f \in \mathcal{B}_n$. For every non-negative integer $0 < r \leq n$, the rth-order nonlinearity of f is the minimum Hamming distance of f from all n-variables Boolean functions of degrees at most r $(r \geq 1)$ and denoted denoted by $nl_r(f)$. In other words, the rth-order nonlinearity of f is equal to the minimum Hamming distance of f from the rth-order Reed–Muller code $R(r, n)$ of length 2^n and of order r. The sequence of values $nl_r(f)$, for r ranging 1 to $n - 1$, is said to be nonlinearity profile of Boolean function f.*

When Boolean functions are used in stream or block ciphers their nonlinearities play an important role with respect to the security of the considered ciphers. The relationship between explicit attack and nonlinearity on symmetric ciphers was found by Matsui [18]. There is a lot of research on first-order nonlinearity but very little is known about higher-order nonlinearity. The best known upper bound [**?**] on $nl_r(f)$ has asymptotic version

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

There are no efficent algorithm to compute the rth-order nonlinearity of Boolean function f for $(r \geq 1)$. However, In [10, 11, 15] list decoding algorithms for higher order Reed-Muller codes are used to compute second-order nonlinearities. These algorithms are good for $n \leq 11$ and for $n \leq 13$ for some particular functions. Sun and Wu [24] have found lower bounds of the second-order nonlinearities of three classes of cubic bent Boolean functions. Gangopadhyay et al. [12] have found the second order-nonlinearity of $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^n}^*$ and $n = 6r$. Sun and Wu [25], Deep Singh [23] have found the second order-nonlinearity of $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ for $n = 4r$, $n = 3r$ respectively.

The lower bound of rth-order nonlinearity of Boolean function f from a given algebraic immunity has been studied in [4]. It was improved in [2]. It gives better results than the results obtained by Iwata-Kurosawa [14]. In this paper we find the lower bound of second-order nonlinearity of Boolean function

$f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. It is also demonstrated that the lower bound obtained in this paper is much better than the lower bound obtained by Iwata-Kurosawa [14], and Gangopadhyay et al. (Theorem 1, [12]).

2 Preliminaries

Definition 2.1 *The Walsh transform of $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as*

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\lambda \cdot x}.$$

The multiset $[W_f(\lambda) : \lambda \in \mathbb{F}_2^n]$ is said to be the Walsh spectrum of the Boolean function f. The relation between nonlinearity and Walsh spectrum is given as follows

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

Using Parseval's equality it can be proved that for any positive integer n, their exists a $\lambda \in \mathbb{F}_2^n$, such that $|W_f(\lambda)| \geq 2^{\frac{n}{2}}$, which implies $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

The derivative of Boolean function $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as a Boolean function $D_a f(x) = f(x + a) + f(x)$ for all $x \in \mathbb{F}_{2^n}$.

Definition 2.2 *Let $a_1, a_2, ..., a_k$ is a basis of k-dimensional subspace V_k of $\mathbb{F}_{2^n}$. The k-th derivative of f with respect to V_k is defined as a function*

$$D_{V_k} f(x) = D_{a_k} D_{a_{k-1}} ... D_{a_1} f(x) \text{ for all } x \in \mathbb{F}_{2^n}.$$

Remark 2.1 *It is to be noted that the $D_{V_k} f$ is independent of the choice of the basis of V_k.*

The trace function from $L = \mathbb{F}_{2^n}$ into $S = \mathbb{F}_{2^c}$ (where $c|n$) is defined as

$$Tr_S^L(x) = \sum_{i=0}^{\frac{n}{c}-1} x^{2ci}, \text{for all } x \in \mathbb{F}_{2^n}.$$

If $c = 1$, we called absolute trace function and denoted as Tr_1^n (or Tr). $Tr_1^n(xy)$ is called an inner product of x and y for any $x, y \in \mathbb{F}_{2^n}$. The some known properties of trace function are following [].

1. $Tr_S^L(\alpha x + \beta y) = \alpha Tr_S^L(x) + \beta Tr_S^L(y)$ for all $\alpha, \beta \in Q$ and $x, y \in L$.
2. $Tr_S^L(x^s) = Tr_S^L(x)$ for all $x \in L$ and $s = 2^c$.
3. (Transitivity property) Let R be a finite field. Let F be a finite extension of R and L be a finite extension of F, that is $L \supset F \supset R$. Then

$$Tr_R^L(\alpha) = Tr_R^F(Tr_F^L(\alpha)) \text{ for all } \alpha \in L.$$

2.1 Quadratic Boolean functions

In this subsection, we give some lemmas which are used in this paper.

Let q be a some power of 2. Let W be a vector space over $\mathbb{F}_q$ with n-variables. A function Q from V to $\mathbb{F}_q$ is said to a quadratic function on V. If it satisfy following:

1. $Q(cx) = c^2 Q(x)$ for any $c \in \mathbb{F}_q$ and $x \in V$,
2. $\mathcal{B}(x, y) := Q(x + y) + Q(x) + Q(y)$ is bilinear on V.

The kernel [1, 21] of $\mathcal{B}(x, y)$ is the subspace of V defined by

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

Lemma 2.1 *([1], Proposition 1) Let V be a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $Q : V \to \mathbb{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Lemma 2.2 *([1], Lemma 1) Let f be a quadratic Boolean function . The kernel of f is the subspace of $\mathbb{F}_{2^n}$ having those b such that $D_b(f)$ is constant. Mathematically*

$$\mathcal{E}_f = \{b \in \mathbb{F}_{2^n} : D_b(f) = constant\}.$$

Lemma 2.3 *[1, 21] if $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $\mathcal{B}(x, y)$ is the quadratic form associated to it, then the Walsh Spectrum of f depends only on the dimension k, of the kernel, $\mathcal{E}_f$, of $\mathcal{B}(x, y)$. The weight distribution of the Walsh spectrum of f is:*

$W_f(\alpha)$	Number of α
0	$2^n - 2^{n-k}$
$2^{\frac{n+k}{2}}$	$2^{\frac{n-k-1}{2}} + (-1)^{f(0)} 2^{\frac{n-k-2}{2}}$
$-2^{\frac{n+k}{2}}$	$2^{\frac{n-k-1}{2}} - (-1)^{f(0)} 2^{\frac{n-k-2}{2}}$

2.2 The lower bounds which have been obtained previously

Carlet [3] proved the following results.

Proposition 2.1 ([3], Proposition 2) *Let f be an n-variables Boolean function and r be a positive integer smaller then n, we have*

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

Corollary 2.1 ([3], Corollary 2) *Let f be an n-variables Boolean function and r be a positive integer smaller then n Assume that, for some non negative integers M and m, we have*

$$nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m \tag{1}$$

for every nonzero $a \in \mathbb{F}_{2^n}$. Then we have

$$\begin{aligned} nl_r(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{m+1} + 2^n} \\ &\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}. \end{aligned} \tag{2}$$

Definition 2.3 ([17], Page 99) *A polynomial of the form*

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

with the coefficients β_i in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called Linearized Polynomial over $\mathbb{F}_{q^m}$.

3 Main Results

Lemma 3.1 *Consider the Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. Then the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either r or $3r$.*

Proof The algebraic degree of Boolean function $f_\lambda(x)$ is 3. The derivative $D_a(f_\lambda(x))$ with respect to $a \in \mathbb{F}_{2^n}^*$ is

$$\begin{aligned} D_a(f_\lambda(x)) = &\ f_\lambda(x+a) + f_\lambda(x) \\ = &\ Tr_1^n(\lambda(x+a)^{2^{2r}+2^r+1}) + Tr_1^n(\lambda x^{2^{2r}+2^r+1}) \\ = &\ Tr_1^n(\lambda(ax^{2^{2r}+2^r} + a^{2^r}x^{2^{2r}+1} + a^{2^{2r}}x^{2^r+1} + a^{2^r+1}x^{2^{2r}} \\ &+a^{2^{2r}+1}x^{2^r} + a^{2^{2r}+2^r}x + a^{2^{2r}+2^r+1})). \end{aligned}$$

which is a quadratic Boolean function. Therefore, the Walsh spectrum of Boolean function $D_a(f_\lambda(x)))$ is equal to the Walsh spectrum of the function $G_\lambda(x)$, where $G_\lambda(x)$ is obtained by removing all affine monomials from $D_a(f_\lambda(x))$.

$$G_\lambda(x) = Tr_1^n(\lambda(ax^{2^{2r}+2^r} + a^{2^r}x^{2^{2r}+1} + a^{2^{2r}}x^{2^r+1})).$$

$G_\lambda(x)$ can also be written as

$$G_\lambda(x) = Tr_1^n(\lambda a^{2^r}x^{2^{2r}+1} + (\lambda^{2^{4r}}a^{2^{4r}} + \lambda a^{2^{2r}})x^{2^r+1}).$$

Because $2^{2r}+1$ and 2^r+1 are not lie in the same cyclotomic coset. Therefore, $G_\lambda(x)$ is not equal to zero for $a \in \mathbb{F}_{2^n}^*$. Therefore $G_\lambda(x)$ is a quadratic Boolean function. By Lemma 2.2, 2.3, the Walsh spectrum of $G_\lambda(x)$ depends on the dimension k of the kernel of $G_\lambda(x)$ which is the subspace of those b such that $D_b(G_\lambda(x))$ is constant. The derivative $D_b(G_\lambda(x))$ is

$$\begin{aligned} D_b(G_\lambda(x)) = &\ G_\lambda(x+b)+G_\lambda(x) \\ = &\ Tr_1^n(\lambda(a(x+b)^{2^{2r}+2^r}+a^{2^r}(x+b)^{2^{2r}+1}+a^{2^{2r}}(x+b)^{2^r+1})) \\ &+Tr_1^n(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1})) \\ = &\ Tr_1^n(\lambda((ab^{2^r}+a^{2^r}b)x^{2^{2r}}+(ab^{2^{2r}}+a^{2^{2r}}b)x^{2^r}+(a^{2^r}b^{2^{2r}}+a^{2^{2r}}b^{2^r})x)) \\ &+Tr_1^n(\lambda(ab^{2^{2r}+2^r}+a^{2^r}b^{2^{2r}+1}+a^{2^{2r}}b^{2^r+1})). \end{aligned}$$

Since $x, a, b \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^r}^*$. Therefore, $x^{2^n}=x$, $a^{2^n}=a$, $b^{2^n}=b$, $\lambda^{2^r}=\lambda$. We get

$$\begin{aligned} D_b(G_\lambda(x)) = &\ Tr_1^n(\lambda x((a^{2^{3r}}+a^{2^r})b^{2^{4r}}+a^{2^{4r}}b^{2^{3r}}+a^{2^r}b^{2^{2r}}+(a^{2^{4r}}+a^{2^{2r}})b^{2^r})) \\ &+Tr_1^n(\lambda(ab^{2^{2r}+2^r}+a^{2^r}b^{2^{2r}+1}+a^{2^{2r}}b^{2^r+1})) \end{aligned}$$

Clearly , $D_b(G_\lambda(x))$ is equal to the constant if and only if

$$(a^{2^{3r}}+a^{2^r})b^{2^{4r}}+a^{2^{4r}}b^{2^{3r}}+a^{2^r}b^{2^{2r}}+(a^{2^{4r}}+a^{2^{2r}})b^{2^r}=0.$$

Or it is equivalent to the following

$$(a^{2^{2r}}+a)b^{2^{3r}}+a^{2^{3r}}b^{2^{2r}}+ab^{2^r}+(a^{2^{3r}}+a^{2^r})b=0. \tag{3}$$

It is to be noted that equation 3 is a 2^r-polynomial. Since a polynomial of the form $L(x)=\sum_{i=0}^n \beta_i x^{q^i}$ with the coefficients β_i in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called q-Polynomial over $\mathbb{F}_{q^m}$. Let

$$M(b)=(a^{2^{2r}}+a)b^{2^{3r}}+a^{2^{3r}}b^{2^{2r}}+ab^{2^r}+(a^{2^{3r}}+a^{2^r})b.$$

As a consequence, the dimension of the kernel of $M(x)$ equals to sr, for $s=0,1,2,$ or 3.

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

$$N(x)=Tr_E^L(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1})),$$

where $L=\mathbb{F}_{2^{5r}}$ and $E=\mathbb{F}_{2^r}$.

The set of roots of $M(x)$ is also the kernel of $N(x)$. Indeed, the kernel of $N(x)$ is the set of those b such that $B(x)=0$ for all x where $B(x)$ is given as

$$B(x)=N(x)+N(b)+N(x+b).$$

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

$$B(x) = Tr_E^L(xM(b)).$$

Therefore, the kernel of $N(x)$ is equal to the kernel of $M(x)$. By Lemma 2.1, the dimension of the kernel of $N(x)$ must have the same parity as 5. Hence this is odd. Therefore, the the dimension of the kernel of $N(x)$ is either 1 or 3 which imply that the one root of $M(x)$ is either r or $3r$, that is, the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either r or $3r$ ($k = r$ or $k = 3r$).

Theorem 3.1 *Consider the Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. Then*

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{3n+3r-4}{4}}.$$

Proof From lemma 3.1, the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either r or $3r$ ($k = r$ or $k = 3r$). From equation **??**, nonlinearity of $D_a(f_\lambda(x))$ that is, $nl(D_a(f_\lambda(x)))$ is either $2^{n-1} - \frac{1}{2}2^{\frac{n+r}{2}}$ or $2^{n-1} - \frac{1}{2}2^{\frac{n+3r}{2}}$. Therefore, we have

$$\max_{a \in \mathbb{F}_2^n}(nl(D_a(f_\lambda(x))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+r}{2}}.$$

Therefore, by proposition 2.1, we have

$$nl_2(f_\lambda(x)) \geq (2^{n-2} - 2^{\frac{n+r-4}{2}}). \tag{4}$$

For $a \in \mathbb{F}_{2^n}^*$, we also have

$$nl(D_a(f_\lambda(x))) = 2^{n-1} - \frac{1}{2}2^{\frac{n+3r}{2}}. \tag{5}$$

We can also improve the lower bound on comparing equation 5 with the equation 1. After comparing , we get $M = 1$ and $m = \frac{n+3r-2}{2}$. Therefore, using the value of M and m in equation 2, we get

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{3n+3r-4}{4}}. \tag{6}$$

From the above it is clear, the lower bound obtained by equation 6 is better than the lower bound obtained by equation 4 for $r > 1$. So, we have

$$nl_2(f_\lambda(x)) \geq 2^{n-1} - 2^{\frac{3n+3r-4}{4}}.$$

4 Comparison

We compare our lower bound obtained in Theorem 3.1 with the lower bound obtained by Iwata-Kurosawa [14], and also compare with the lower bound obtained by Gangopadhyay, Sarkar and Telang (Theorem 1, [12]) in the following table.

n , r	10, 2	15, 3	20, 4	25, 5	30, 6
Bound obtained in Theorem 1	256	10592	393216	1.3811×10^7	4.6976×10^8
Iwata-Kurosawa's bound	192	6144	196608	6.2914×10^6	2.0132×10^8
Bound obtained in (Theorem 1, [12])	N/A	N/A	N/A	N/A	4.4196×10^8

35, 7	40, 8	45, 9	50, 10	55, 11	60, 12
1.5661×10^{10}	5.1539×10^{11}	1.6814×10^{13}	5.4535×10^{14}	1.7616×10^{16}	5.6745×10^{17}
6.4424×10^9	2.0615×10^{11}	6.5970×10^{12}	2.1110×10^{14}	6.7553×10^{15}	2.1617×10^{17}
N/A	N/A	N/A	N/A	N/A	5.5844×10^{17}

It is clear from the above that our lower bound is much better than lower bound obtained in [14] and (Theorem 1, [12]).

5 Conclusion

In this paper we find the lower bound of second-order nonlinearity of a Boolean function $f_\lambda(x) = Tr_1^n(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1$, $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 5r$. The algebraic immunity of $f_\lambda(x)$ is at most 3 because the algebraic degree of $f_\lambda(x)$ is 3 ($AI(f) \leq d^0(f)$). Therefore, the lower bound of second-order nonlinearity of $f_\lambda(x)$ can not be obtained from the relation between rth-order nonlinearity and the algebraic immunity as given in [2, 4]. The lower bound of second-order nonlinearity of $f_\lambda(x)$ is much better than lower bound obtained in [14] and (Theorem 1, [12]). So, this Boolean function may be used in stream ciphers as well as block ciphers.

Acknowledgement

Manish Garg is thankful to the **"Ministry of Human and Research Development"**, New Delhi, India for financial support to carry out the above work.

References

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

[2] C. Carlet. On the higher order-nonlinearities of algebraic immune functions. Advances in Cryptology-CRYPTO 2006, LNCS 4117, Springer-Verlag, pp. 584-601, 2006.

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

[4] C. Carlet, D. Dalai, K. Gupta, S. Maitra. Algebraic immunity for cryptographyically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory, 52(7), pp. 3105-3121, 2006.

[5] C. Carlet and S. Mesnager.Improving the upper bounds on the covering radii of binary ReedMuller codes. IEEE Trans. Inf. Theory, vol.53, no. 1, pp. 162-173, jan. 2007.

[6] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. Covering Codes. Amsterdam, The Netherlands: North-Holland, 1997.

[7] N. Courtois. Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt. in Proc. ICISC 2002 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol. 2587, pp. 182-199, 2002.

[8] C. Ding, G.Xiao and W. Shan. The stability Theory of Stream Ciphers. LNCS, vol. 561. Springer, Heidelberg, 1991.

[9] H. Dobbertin et al. Construction of bent functions via Niho power functions. Journal of Combinatorial Theory. Series A 113, pp. 779-798, 2006.

[10] I. Dumer, G. Kabatiansky and C. tavernier. List decoding of second order Reed-Muller codes up to the johnson bound with almost linear complexity. In: Proceedings of the IEEE International Symposium on Information Theory, Seattle, pp. 138-142, WA 2006.

[11] R. Fourquet and C. tavernier. An improved list decoding algorithm for the second order Reed-Muller codes and its applications. Designs Codes Cryptogr., Vol, 49, pp. 323-340, 2008.

[12] S. Gangopadhyay et al. On the lower bounds of the second-order nonlinearity of some Boolean functions. Inf. Sci. 180(2), pp. 266-273, 2010.

[13] J. Golić. Fast low order approximation of cryptographic functions. in Proc. EUROCRYPT'96 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol.1070, pp. 268-282, 1996.

[14] T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. in Proc. ASIACRYPT'99 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol.1716, pp. 62-74, 1999.

[15] G. Kabatiansky and C. Tavernier. List decoding of second order Reed-Muller codes. In : Proceedings of the Eighteen International Symposium of Communication Theory and Applications, Ambleside, UK, 2005.

[16] L. R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. in Proc. EUROCRYPT'96 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol.1070, pp. 224-236, 1996.

[17] R.Lidi, H.Niederreiter. Introduction to finite fields and their applications. North-Holland, Amsterdam, 1994.

[18] M. Matsui. Linear cryptanalysis method for DES cipher. In: Proceeding of the EUROCRYPT'93, LNCS, Vol. 765, pp. 386-397, 1994.

[19] U. M. Maurer. New approaches to the design of self-synchronizing stream ciphers. in Proc. EUROCRYPT'91 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol.547, pp. 458-471, 1991.

[20] W. Millan. Low order approximation of cipher functions. in Cryptographic Policy and Algorithms (Lecture notes in Computer Science), Berlin, Germany: Springer-Verlag, vol.1029, pp. 144-155, 1996.

[21] F.J.Macwilliams and N.J.A.Solane. The theory of Error-correcting Codes. Amsterdam: North-holland publishing Company, 1978.

[22] O.S.Rothaus. On bent functions. Journal of Combinatorial Theory, Series A, 20, pp.300-305, 1976.

[23] D. Singh. Second-order nonlinearities of some classes of cubic Boolean functions based on secondary constructions. Int'l J. Comput. Sci. Inform. Technol, vol. 2, no 2, pp. 786-791, 2011.

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

[25] G.Sun, C.Wu. The lower bound on the second-order nonlinearity of a class of Boolean function with high nonlinearity. Appl. Algebra Engrg. Comm. Comput. (AAECC), vol. 22, pp. 37-45, 2011.