PAPER

The Lower Bound of Second-Order Nonlinearity of a Class of Boolean Functions*

Luozhong GONG[†a)] ***and*** **Shangzhao LI**[††b)]**,** ***Nonmembers***

SUMMARY The r-th nonlinearity of Boolean functions is an important cryptographic criterion associated with higher order linearity attacks on stream and block ciphers. In this paper, we tighten the lower bound of the second-order nonlinearity of a class of Boolean function over finite field F_{2^n}, $f_\lambda(x) = Tr(\lambda x^d)$, where $\lambda \in \mathrm{F}_{2^r}^*$, $d = 2^{2r} + 2^r + 1$ and $n = 7r$. This bound is much better than the lower bound of Iwata-Kurosawa.

key words: *Boolean function, higher-order nonlinearity, higher-order derivative*

1. Introduction

To resist the many kinds of crypt analysis, Boolean functions used in stream ciphers should have many good cryptographic properties: high algebraic degree, balancedness, high algebraic immunity and high nonlinearity etc. Now, many classes of Boolean functions with some good cryptographic properties have been constructed. In [1], [7], [10], [12]–[14], [19], [26], many classes of Boolean functions achieving optimum algebraic immunity have been introduced. The Carlet-Feng functions have optimum algebraic degree, optimum algebraic immunity and higher nonlinearity [10], but it is not enough to resistance to fast correlation attacks [23], [25]. In [26], the Tu-Ding fuctions are another class Boolean functions with optimum algebraic degree, optimum algebraic immunity and a provable good nonlinearity. However, they are also weak against fast algebraic attacks.

A characteristic of Boolean functions, called their *nonlinearity profile*, plays an important role with respect to the linear approximation attack of the cryptosystems in which they are involved. For every nonnegative integer $r \le n$, we denote the $nl_r(f)$ the minimum distance of f and all functions of algebraic degrees at most r. The nonlinearity profile of a function f is the sequence of those values $nl_r(f)$ for $r(1 \le r \le n-1)$. In the case $r = 1$, we simply write $nl(f)$. Clearly, it is the minimum Hamming distance between the function f and all affine functions over F_{2^n}, called the *nonlinearity* of f. Attributed to the $nl(f)$'s relation with Walsh transform, most research work so far has been theoretically and practically focused on $nl(f)$ (see [2], [8]). However, computing the $nl_r(f)$ of a given function with algebraic degree strictly greater than r is a hard task for $r > 1$, and, so far, few acdemic result has been achieved. Even proving lover bounds on the $nl_2(f)$ of functions is also a quite difficult task. In recently, Wang et al. in [20] give an upper bound on the second-order of the hidden weighted bit function and Carlet (see [4]) introduce a new method for lower bounding the nonlinearity of a given function, which tell us how to derive a lower bound on the r-th order nonlinearity of a function f from a lower bound on the $(r-1)$-th nonlinearity of at least one of the derivatives of f. Using this approach, G. Sun and C. Wu in [16], S. Gangopadhyay et al. in [22] and L. Gong and G. Fan in [18] recently also obtained the lower bounds of the second-order nonlinearity of several classes of Boolean functions.

Let $f(x) = x^{2^{2r}+2^r+1}$ be a function defined on F_{2^n}, then f has a low differential uniformity of four and higher $nl(tr(bf))$. So, it is an interesting problem whether its second-order nonlinearity is also high so that it can withstand the second-order affine approximation attack. When $n = 3r, 4r, 6r$, the lower bounder of $nl(tr(bf))$ has been obtained (see [11], [16], [17]). The present paper is engaged in deducing the lower bound of the second-order of nonlinearity of the above function with $n = 7r$.

2. Notation and Preliminaries

Let $\mathrm{F}_2 = \{0, 1\}$ be the prime field of characteristic 2, F_2^n be an n-dimensional vector space over F_2. Any mapping from F_2^n to F_2 is called a Boolean function on n-variables. They play the core role in cryptography and error-correction coding. We denote by $\mathcal{B}_n$ the set of the Boolean functions on n-vavriables. Any Boolean function is defined as

$$f(x_1, x_2, ..., x_n) = \bigoplus_{a=(a_1,...,a_n)\in F_2^n} \mu_a(\prod_{i=1}^{n} x_i^{a_i}),$$

where $\mu_a \in \mathrm{F}_2$ for all $a \in \mathrm{F}_2^n$, which is called it's algebraic normal form (ANF). Define $wt(a)$ the numbers of nozero components of vector a. The maximum value of $wt(a)$ such that $\mu_a \neq 0$ is called the *algebraic degree* of f which is denoted by $\deg(f)$. Every Boolean function f over F_2^n also can be written as the univariate polynomials over F_{2^n}:

Manuscript received November 9, 2021.
Manuscript revised January 20, 2022.
Manuscript publicized March 10, 2022.

[†]The author is with the Faculty of the School of Mathematics, Changsha Nomal University, China.
[††]The author is with the Faculty of School of Mathematics and Statistics, Changshu Institute of Technology, China.

*The paper was supported by the NNSFC (No.12071484, 11701046).

a) E-mail: gonglztop@126.com
b) E-mail: lszfd2004@126.com

DOI: 10.1587/transfun.2021EAP1146

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_0, a_{2^n-1} \in \mathrm{F}_2$, and $a_{2i(\mod 2^n-1)} = a_i^2 \in \mathrm{F}_2, 1 \le i \le 2^n - 2$. So the *algebraic degree* of the Boolean function

$$deg(f) = max\{w_2(j)|a_j \neq 0, 0 \le j \le 2^n - 1\},$$

where, given the 2-adic expansion $j = j_0 + j_1 2 + \cdots + j_{n-1}2^{n-1}, j_s \in \mathrm{F}_2, 0 \le s \le n-1$ and $w_2(j)$ denotes the number of all nonzero $j_s, 0 \le s \le n-1$. A Boolean function is affine if it has algebraic degree at most 1. The set of all affine functions is denoted by $\mathcal{A}_n$.

Let $m|n, E = \mathrm{F}_{2^m}$ and $L = \mathrm{F}_{2^n}$. The function

$$tr_{L/E}(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$$

is called a trace function from L to E. If $m = 1$, namely $E = \mathrm{F}_2$, we denote $tr_{L/E}$ simply by tr which is called the absolute trace function. The trace function has the following properties [21]:

(i) $tr_{L/E}(ax+by) = atr_{L/E}(x)+btr_{L/E}(y)$ for all $x, y \in L$ and $a, b \in E$.

(ii) $tr_{L/E}(x^q) = tr_{L/E}(x)$ for all $x \in L$ and $q = 2^m$.

(iii) Let K be a finite field, F be a finite extension of K, and E be a finite extension of F, that is $K \subset F \subset E$. Then $tr_{E/K}(x) = tr_{F/K}(tr_{E/F}(x))$ for all $x \in E$.

Difinition 2.1: Let $f \subset \mathcal{B}_n$ and $a \in L = \mathrm{F}_{2^n}$, we called

$$W_f(a) = \sum_{x \in L} (-1)^{f(x)} \chi(ax), a \in L,$$

the Walsh transform of f, where $\chi(x) = (-1)^{tr(x)}$ is the canonical additive character on L. The set $\{W_f(a)|a \in \mathrm{F}_{2^n}\}$ is said to be the Walsh spectrum of f.

It is trivial to deduce that the relation between the nonlinearity and the Walsh spectrum is

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

By Parseval's equality, $\sum_{a \in \mathrm{F}_{2^n}} W_f(a)^2 = 2^{2n}$, we have $nl(f) \le 2^{n-1} - 2^{\frac{n}{2}-1}$. When $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, f is called a bent function. Obviously, it is possible for a bent function to exist when n is even. Since the nonlinearity of *bent functions* reaches the maximum value, it can withstand the linear attack (to be more precise, linear approximation or affine approximation attack) to the most extent ([15]), and can also well withstand the correlation attack ([2], [9]).

Difinition 2.2: We call the Boolean function $D_a f(x) = f(x) + f(x + a)$ for any $x \in \mathrm{F}_{2^n}$ as the derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathrm{F}_{2^n}$, which is denoted by $D_a f$. Let V be a k dimensional subspace of F_{2^n} generated by $\alpha_1, \alpha_2, \cdots, \alpha_k$, the k-th order derivative of $f \in \mathcal{B}_n$ is defined by

$$D_V f(x) = D_{\alpha_1} \cdots D_{\alpha_k} f(x) = \sum_{u \in F_{2^k}} f(x + \sum_{i=1}^{k} u_i \alpha_i).$$

Table 1 Walsh spectrum.

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

for any $x \in \mathrm{F}_{2^n}$, which $u = \sum_{i=1}^{k} u_i \alpha_i$.

It is to be noted that when $\alpha_1, \alpha_2, \cdots, \alpha_k$, are not linearly independent, then $D_{\alpha_1} \cdots D_{\alpha_k} f$ is zero; otherwise, the set $\{x + \sum_{i=1}^{k} u_i \alpha_i | u \in \mathrm{F}_{2^k}\}$ is a k-dimensional flat. Also, the k-th order derivative of f depends only on the choice of the k dimensional subspace V and is independent of the choice of the basis of V. On the Galois field F_{2^n}, a cyclotomic coset C_s is defined by $C_s = \{s, 2s, 2^2 s, \cdots, 2^{n_s-1} s\}$, where n_s is the smallest positive integer such that $s \equiv 2^{n_s} s \pmod{2^n - 1}$. The subscript s is chosen as the smallest integer in C_s, and s is called the coset leader of C_s.

Difinition 2.3: Let q be a power of 2 and V be an n-dimensional vector space over F_q. A map $Q : V \to \mathrm{F}_q$ is called a quadratic form on V if

(a) $Q(cx) = c^2 Q(x)$ for any $c \in \mathrm{F}_q$ and $x \in V$;

(b) $\mathcal{B}(x, y) := Q(x + y) + Q(x) + Q(y)$ is bilinear on V.

The kernel K of a bilinear form Q is the subspace of V defined by $K = \{x \in V | \mathcal{B}(x, y) = 0, \forall y \in V\}$.

The following lemmas are obtained from the definitions.

Lemma 2.4: ([3]) Let V be a vector space over a field F_q of characteristic 2 and $Q : V \to \mathrm{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity

Lemma 2.5: ([3]) If $f : \mathrm{F}_{2^n} \to \mathrm{F}_2$ is a quadratic Boolean function, then the Walsh spectrum of f depends only on the dimension k of the kernel of f. More precisely, the Walsh spectrum of f is shown in Table 1.

Lemma 2.6: ([3]) Let f be any quadratic Boolean function. The kernel of f is the subspace of those b such that the derivative $D_b f$ is constant. That is

$$\mathcal{E}_f = \{b \in \mathrm{F}_{2^n} | D_b f = constant\}$$

3. Main Results

Lemma 3.1: ([4]) Let f be any n-variable function and r be a positive integer smaller than n. Then we have

$$nl_r(f) \ge 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_{2^n}} nl_{r-1}(D_a f)}. \quad (2)$$

Lemma 3.2: Let $f_\lambda(x) = Tr(\lambda x^p)$ with $p = 2^{2r} + 2^r + 1, \lambda \in \mathrm{F}_{2^r}^*$ and $n = 7r$. Then the dimension of the kernel of bilinear form associated to $D_a(f_\lambda(x))$ is either $3r$ or $5r$.

Proof The derivative of $f_\lambda(x) = Tr(\lambda x^p)$ with respect to $a \in \mathrm{F}_{2^n}^*$ is

$$\begin{aligned}D_a(f_\lambda(x)) &= f_\lambda(x)+f_\lambda(x+a)\\ &= Tr(\lambda x^{2^{2r}+2^r+1})+Tr(\lambda(x+a)^{2^{2r}+2^r+1})\\ &= Tr(\lambda x^{2^{2r}+2^r+1})+Tr(\lambda(x+a)(x^{2^{2r}+2^r}\\ &\quad + x^{2^{2r}}a^{2^r}+a^{2^{2r}}x^{2^r}+a^{2^{2r}+2^r})\\ &= Tr(\lambda(x^{2^{2r}+2^r}a+x^{2^{2r}+1}a^{2^r}+x^{2^{2r}}a^{2^r+1}\\ &\quad + x^{2^r+1}a^{2^{2r}}+x^{2^r}a^{2^{2r}+1}\\ &\quad + xa^{2^{2r}+2^r}+a^{2^{2r}+2^r+1})).\end{aligned}$$

Since the Walsh spectrum is affine invariant, the Walsh spectrum of the function $D_a(f_\lambda(x))$ is equal to the one of the function

$$\begin{aligned}G(x) &= Tr(\lambda(x^{2^{2r}+2^r}a+x^{2^{2r}+1}a^{2^r}+x^{2^r+1}a^{2^{2r}}))\\ &= Tr(\lambda x^{2^{2r}+1}a^{2^r}+(\lambda a^{2^{2r}}+\lambda^{2^{6r}}a^{2^{6r}})x^{2^r+1})\end{aligned}$$

Noticed that 2^r+1 and $2^{2r}+1$ are not in the same cyclotomic coset, so $G(x)\neq 0$ and $G(x)$ is a quadratic Boolean function. By Lemma 2.5, the Walsh spectrum of $G(x)$ only depends on the dimension k of the kernel of $G(x)$. By lemma 2.6, the kernel of $G(x)$ is the subspace of those b such that the derivative of $D_b(G(x))$ is constant. Since

$$\begin{aligned}&D_b(G(x))\\ &= G(x)+G(x+b)\\ &= Tr(\lambda(x^{2^{2r}+2^r}a+x^{2^{2r}+1}a^{2^r}+x^{2^r+1}a^{2^{2r}}))\\ &\quad +Tr(\lambda((x+b)^{2^{2r}+2^r}a+(x+b)^{2^{2r}+1}a^{2^r}\\ &\quad +(x+b)^{2^r+1}a^{2^{2r}}))\\ &= Tr(\lambda((ab^{2^r}+a^{2^r}b)x^{2^{2r}}+(ab^{2^{2r}}+a^{2^{2r}}b)x^{2^r}\\ &\quad +(a^{2^r}b^{2^{2r}}+a^{2^{2r}}b^{2^r})x))\\ &\quad +Tr(\lambda(ab^{2^{2r}+2^r}+a^{2^r}b^{2^{2r}+1}+a^{2^{2r}}b^{2^r+1}))\\ &= Tr(\lambda(a^{2^{5r}}b^{2^{6r}}+a^{2^{6r}}b^{2^{5r}}+a^{2^{6r}}b^{2^r}+a^{2^r}b^{2^{6r}}\\ &\quad +a^{2^r}b^{2^{2r}}+a^{2^{2r}}b^{2^r})x)\\ &\quad +Tr(\lambda(ab^{2^{2r}+2^r}+a^{2^r}b^{2^{2r}+1}+a^{2^{2r}}b^{2^r+1}))\end{aligned}\tag{3}$$

Clearly, $D_b(G(x))$ is constant if an only if

$$(a^{2^{5r}}b^{2^{6r}}+a^{2^{6r}}b^{2^{5r}})+(a^{2^{6r}}b^{2^r}+a^{2^r}b^{2^{6r}})+(a^{2^r}b^{2^{2r}}+a^{2^{2r}}b^{2^r})=0$$

That is

$$(a^{2^{5r}}+a^{2^r})b^{2^{6r}}+a^{2^{6r}}b^{2^{5r}}+a^{2^r}b^{2^{2r}}+(a^{2^{6r}}+a^{2^{2r}})b^{2^r}=0$$

Raising 2^{-r}-th power to the both sides of above equation gives the following equation

$$(a^{2^{4r}}+a)b^{2^{5r}}+a^{2^{5r}}b^{2^{4r}}+ab^{2^r}+(a^{2^{5r}}+a^{2^r})b=0\tag{4}$$

If $a\in \mathrm{F}_{2^{4r}}$, Eq. (4) is equivalent to the equation $a^{2^r}b^{2^{4r}}+ab^{2^r}=0$. This follows $b\in a\mathrm{F}_{2^{3r}}$, and so $k=3r$. Hence, we only consider the case when $a\notin \mathrm{F}_{2^{4r}}$. In this case, Eq. (4) is a 2^r-polynomial. Write $P(b):=(a^{2^{4r}}+a)b^{2^{5r}}+a^{2^{5r}}b^{2^{4r}}+ab^{2^r}+(a^{2^{5r}}+a^{2^r})b$. We are all know, the dimension of the kernel of $P(b)$ is $lr, l=0,1,2,3,4$, or 5. Because $a\notin \mathrm{F}_{2^{4r}}$, $l\neq 0,1$.

Now consider the quadratic form from F_{q^7} to $\mathrm{F}_q(q=2^r)$

$$Q(x)=Tr_{L/E}(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1})),$$

where $L=\mathrm{F}_{q^7}$ and $E=\mathrm{F}_q$.

In fact, the kernel of $Q(x)$ is the set of those b such that $\mathcal{B}(x,b)=0$ for all x, where

$$\mathcal{B}(x,b)=Q(x)+Q(b)+Q(x+b)=Tr_{L/E}(x(P(b))^{2^r}.$$

Since

$$\begin{aligned}&\mathcal{B}(x,b)\\ &= Tr_{L/E}(\lambda(ax^{2^{2r}+2^r}+a^{2^r}x^{2^{2r}+1}+a^{2^{2r}}x^{2^r+1}))\\ &+ Tr_{L/E}(\lambda(ab^{2^{2r}+2^r}+a^{2^r}b^{2^{2r}+1}+a^{2^{2r}}b^{2^r+1}))\\ &+ Tr_{L/E}(\lambda(a(x+b)^{2^{2r}+2^r}+a^{2^r}(x+b)^{2^{2r}+1}+a^{2^{2r}}(x+b)^{2^r+1}))\\ &= Tr_{L/E}(\lambda(a(x^{2^{2r}}b^{2^r}+x^{2^r}b^{2^{2r}})+a^{2^r}(x^{2^{2r}}b+b^{2^{2r}}x)+a^{2^{2r}}(x^{2^r}b+\\ &b^{2^r}x)))\\ &= Tr_{L/E}(\lambda(a^{2^{5r}}b^{2^{6r}}+a^{2^{6r}}b^{2^r}+a^{2^{6r}}b^{2^{5r}}+a^{2^r}b^{2^{2r}}+a^{2^r}b^{2^{6r}}+\\ &a^{2^{2r}}b^{2^r})x)\\ &= Tr_{L/E}(\lambda(a^{2^{4r}}b^{2^{5r}}+a^{2^{5r}}b+a^{2^{5r}}b^{2^{4r}}+ab^{2^r}+ab^{2^{5r}}+\\ &a^{2^r}b)^{2^r}x)\\ &= Tr_{L/E}((P(b))^{2^r}x).\end{aligned}$$

Therefore the set of roots of $P(b)$ is also the kernel of $Q(x)$. By lemma 2.4, the kernel of $Q(x)$ must have the same parity 7, so it is odd. Hence the dimension of the kernel of $Q(x)$ is 3 or 5, which implies the one of roots space of $P(b)$ is $3r$ or $5r$, that is the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either $3r$ or $5r$.

Theorem 3.3: Let $f_\lambda(x)=Tr(\lambda x^p)$ with $p=2^{2r}+2^r+1, \lambda\in \mathrm{F}_{2^r}^*$ and $n=7r$. Then

$$nl_2(f_\lambda(x))\geq 2^{7r-1}-2^{4r-1}\sqrt{2^{5r}+2^r}.$$

Proof From Lemma 3.2, the dimension of the kernel of the bilinear form associated to $D_a(f_\lambda(x))$ is either $3r$ or $5r$.Thus the Waksh transform of $D_a(f_\lambda(x))$ at any point α is $|W_{D_a(f_\lambda(\alpha))}|=2^{\frac{n+3r}{2}}$ or $2^{\frac{n+5r}{2}}$. And then by Eq. (1), we get

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

if $a\in \mathrm{F}_{2^{4r}}$.

$$nl(D_a(f_\lambda(x))\geq 2^{n-1}-\frac{1}{2}2^{\frac{n+5r}{2}}=2^{n-1}-2^{6r-1},$$

if $a\notin \mathrm{F}_{2^{4r}}$. Therefore,

$$\begin{aligned}\sum_{a\in F_{2^n}} nl(D_af) &= \sum_{a\in F_{2^{4r}}} nl(D_af)+\sum_{a\notin F_{2^{4r}}} nl(D_af)\\ &\geq 2^{14r-1}+2^{10r-1}-2^{13r-1}-2^{9r-1}\end{aligned}$$

By lemma 3.1, we have

$$nl_2(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{a\in F_{2^n}} nl(D_af)}$$

Table 2 The second-order nonlinearity.

r	2	3	4	6
Bound obtained in Theorem 3.3	4088	677803	1.0066304 $\times 10^8$	1.92414 $\times 10^{12}$
Iwata-Kurosawa's bound	3072	393216	5.0332 $\times 10^7$	8.42633 $\times 10^{11}$

$$\geq 2^{7r-1} - \frac{1}{2}\sqrt{2^{13r} + 2^{9r}}$$
$$= 2^{7r-1} - 2^{4r-1}\sqrt{2^{5r} + 2^{r}}.$$

4. Conclusion Remarks

By studying the lower bound of the nonlinearity of the derivatives of the functions, the present paper obtains the lower bound of the second-order nonlinearity of a class of Boolean functions. Results show that the second-order nonlinearity of the class of Boolean functions with high nonlinearity is also high (Table 2). We compare our lower bound obtained in Theorem 3.3 with the lower bound obtained by Iwata-Kurosawa [24] in the following table. It is seen from the following table that our lower bound is much better than the lower bound of Iwata-Kurosawa. In this case, the lower bounds can- not be obtained by the relation between algebraic immunity and the r-th order nonlinearity as studied in [5], [6].

Acknowledgments

The authors are thankful to the anonymous reviewers whose comments have improved the technical as well as editorial quality of the paper. The paper was supported by the NNSFC (No.12071484,11701046), the Natural Science Foundation of Hunan Province, China (No.2020JJ4675; 2018JJ2450) and the Qing Lan Project of Jiangsu Province.

References

[1] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," LNCS, vol.3797, pp.35–48, 2005.
[2] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," LNCS, vol.1807, pp.573–588, 2000.
[3] A. Canteaut, P. Charpin, and G.M. Kyureghyan, "A new class of monomial bent functions," Finite Fields Appl., vol.14, no.1, pp.221–241, 2008.
[4] C. Carlet, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," IEEE Trans. Inf. Theory, vol.54, no.3, pp.1262–1272, 2008.
[5] C. Carlet, "On the higher order nonlinearities of algebraic immune functions," LNCS, vol.4117, pp.584–601, 2006.
[6] C. Carlet, D. Dalai, K. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," IEEE Trans. Inf. Theory, vol.52, no.7, pp.3105–3121, 2006.
[7] C. Carlet, D.K. Dalai, K.C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," IEEE Trans. Inf. Theory, vol.52, no.7, pp.3105–3121, 2006.
[8] C. Bracken and G. Leander, "A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree," Available at. http://arxiv.org/abs/0901.1824
[9] C. Ding, G. Xiao, and W. Shan, The Stability Theory of Stream Ciphers, Springer-Verlag Berlin Heidelberg, 1991.
[10] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," LNCS, vol.5350, pp.425–440, 2008.
[11] 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.
[12] D.K. Dalai, K.C. Gupta, and S. Maitra, "Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity," LNCS, vol.3557, pp.98–111, 2005.
[13] D.K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," Des. Codes Cryptogr., vol.40, no.1, pp.41–58, 2006.
[14] E. Pasalic, "Almost fully optimized infinite classes of Boolean functions resistant to (fast) algebraic cryptanalysis," LNCS, vol.5461, pp.399–414, 2009.
[15] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," LNCS, vol.950, pp.356–365, 1995.
[16] G. Sun and C. Wu, "The lower bounds on the second-order nonlinearity of three classes of Boolean functions with high nonlinearity," Inf. Sci., vol.179, no.3, pp.267–278, 2009.
[17] G. Sun and C. Wu, "The lower bounds on the second-order nonlinearity of three classes of Boolean functions with high nonlinearity," AAECC, no.22, pp.37–45, 2011.
[18] L.Z. Gong and G.B. Fan, "The lower bound of the second-order nonlinearity of cubic functions," ARS Combinatoria, vol.136, pp.255–261, 2018.
[19] N. Li and W.F. Qi, "Construction and analysis of Boolean functions of 2t+1 variables with maximum algebraic immunity," LNCS, vol.4284, pp.84–98, 2006.
[20] Q.C. Wang and C.H. Tan, "On the second-order nonlinearity of the hidden weighted bit function," Discret. Appl. Math., vol.215, pp.197–202, 2016.
[21] R. Lidl and H. Niederreiter, eds., Finite Fields, Addison-Wesley, Reading, MA, 1983.
[22] S. Gangopadhyay, S. Sarkar, and R. Telang, "On the lower bounds of the second-order nonlinearity of some Boolean functions," Inf. Sci., vol.180, no.2, pp.266–273, 2010.
[23] T. Johansson and F. Jonsson, "Fast correlation attacks through reconstruction of linear polynomials," LNCS, vol.1880, pp.300–315, 2000.
[24] T. Iwata and K. Kurosawa, "Probabilistic higher order differential attack and higher order bent functions," LNCS, vol.1716, pp.62–74, 1999.
[25] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," LNCS, vol.330, pp.301–314, 1988.
[26] Z. Tu and Y. Deng, "A conjecture on binary string and its application on constructing Boolean functions of optimal algebraic immunity," Des. Codes Cryptogr, vol.60, pp.1–14, 2011.

Luozhong Gong received the B.S. and M.S. degrees in Applied Mathematics from School of Mathematics and statistics, Central South University of China in 2005 and 2010, respectively. During 2005–2016, he stayed in School of science, Hunan University of Science and Engineering of China to study Cryptology and Group Theory. He is now with Changsha Normal University.

Shangzhao Li received the B.S. and M.S. degrees in Applied Mathematics from Central South University of China and Suzhou University in 2008 and 2014, respectively. During 2008 to now, he stayed in Changshu Institute of Technology of China to study Group Theory.