AAECC (2011) 22:37–45
DOI 10.1007/s00200-010-0136-y

The lower bound on the second-order nonlinearity of a class of Boolean functions with high nonlinearity

Guanghong Sun · Chuankun Wu

Received: 15 October 2009 / Revised: 25 September 2010 / Published online: 8 December 2010

Abstract The r-th order nonlinearity of Boolean functions is an important cryptographic criterion associated with some attacks on stream and block ciphers. It is also very useful in coding theory, since it is related to the covering radii of Reed-Muller codes. By investigating the lower bound of the nonlinearity of the derivative of the function f, this paper tightens the lower bound of the second-order nonlinearity of a class of Boolean functions over F_{2^n} with high nonlinearity in the form $f(x) = tr\left(\lambda x^d\right)$, where $\lambda \in F_{2^r}^*$, $d = 2^{2r} + 2^r + 1$ and $n = 4r$.

Keywords Boolean function · Cryptography · Nonlinearity · Derivation · Walsh spectrum · Reed-Muller code

1 Introduction

In designing many symmetric key cryptosystems (stream ciphers and block ciphers), the role of Boolean functions as the core component has been universally acknowledged. And the nonlinearity profile of Boolean functions, a characteristic of them,

This work was supported by the Natural Science Foundation of China under Grant No.60673068, the Fundamental Research Funds for the Central Universities No. 2009B27414, and the Natural Science Foundation of Hohai University under Grant No. 2084/409270.

G. Sun (✉)
College of Sciences, Hohai University, 210098 Nanjing, China
e-mail: sgh1976@gmail.com

G. Sun · C. Wu
The State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, 100190 Beijing, China
e-mail: ckwu@is.iscas.ac.cn

has a significant position when the affine approximation attack on the cryptosystems is concerned. Let $f : F_{2^n} \to F_2$ be an n-variable Boolean function. For every non-negative integer $r \leq n$, we denote by $nl_r(f)$ the minimum Hamming distance of f and all functions of algebraic degrees at most r (in the case of $r = 1$, we shall simply write $nl(f)$). In other words, $nl_r(f)$ equals the distance from f in its truth table representation to the Reed-Muller code $RM(r, n)$ of length 2^n and of order r. This distance is called the *r-th order nonlinearity* of f (simply the nonlinearity in the case when $r = 1$). It is perceived by definition that the maximum r-th order nonlinearity of all Boolean functions in n variables equals the covering radius of $RM(r, n)$ [11]. The *nonlinearity profile* of a function f is the sequence of those values $nl_r(f)$ for r ranging from 1 to $n - 1$. Unfortunately, so far very little is known about $nl_r(f)$ for $r > 1$. The best known upper bound [9] on $nl_r(f)$ has an asymptotic version

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

Computing the r-th order nonlinearity of a given Boolean function with algebraic degree strictly greater than r is a difficult task for $r > 1$. Most research work has so far been theoretically and practically focused on the case where $r = 1$, probably attributed to the nonlinearity's relation with Walsh transform, which can be computed by the algorithm of the fast Fourier transform (FFT). However, as for $r > 1$, few academic result has been achieved, even the second-order nonlinearity is known only for a few particular functions and for functions in small number of variables. Fortunately, a nice algorithm due to Kabatiansky and Tavernier was improved and implemented by Fourquet et al. [14,15,18], which works well for $r = 2$ and $n \leq 11$ (in some cases, $n \leq 13$). What encourages us is that the algorithm can be applied for higher orders of nonlinearity, but few insight has been shed when the function is in very small number of variables.

While significantly useful as the lower bound can be, the exact value of the r-th order nonlinearity of a Boolean function is difficult to compute, furthermore, to find a good lower bound is also thorny. This is why until recently, there has been only one attempt, by Iwata-Kurosawa [17], to construct functions with lower bounded r-th order nonlinearity. However, limitations still remain: the lower bound is a small value $2^{n-r-3}(r + 5)$, $r \leq n - 3$.

A lower bound on the r-th order nonlinearity of functions with given algebraic immunity has been studied in [7] and improved in [4]. It gives better results than those of [17] for functions f with good algebraic immunity $AI(f)$, i.e., when $AI(f)$ is close to its upper bound $\lceil \frac{n}{2} \rceil$. In this case, the lower bound is roughly equal to

$$\max\left(\sum_{i=0}^{AI(f)-r-1} \binom{n}{i},\ 2\sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}\right)$$

which is still a small value in many cases.

Another insightful attempt was made by Carlet, who deduced in [5] that the lower bounds of the second-order nonlinearity of several classes of Boolean functions, such

as the Welch function $f(x) = tr(x^{2^t+3})$, when $t = \frac{n-1}{2}$ and n odd, or when $t = \frac{n+1}{2}$ and n odd, and the inverse function $f(x) = tr\left(x^{2^n-2}\right)$. Here $tr(x)$ denotes the trace function $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ from F_{2^n} into F_2. The approach was to study the nonlinearity of the derivative of the function f. Using this approach, G. Sun and C. Wu in [20] and S. Gangopadhyay et al. in [16] 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 $F_{2^{4r}}$, then f has differential uniformity of four and $nl(tr(bf)) = 2^{4r-1} - 2^{2r}$ for any $b \in F^*_{2^{4r}}$ (see [1,13]). Since the nonlinearity of f is high and it has also low differential uniformity, it is an interesting problem whether its second-order nonlinearity is also high so that it can withstand the second-order affine approximation attack. The present paper is engaged in deducing the lower bound of the second-order of nonlinearity of the above function.

Since an introduction of the paper has been given in Sect. 1, the rest of the paper is structured in the following scheme : Sect. 2 will present some preliminaries that will be needed in the sequel. Section 3 is concentrated on obtaining the main results, the lower bound of the second-order nonlinearity of a class of Boolean functions. A conclusion is therefore conducted in Sect. 4, and ends the paper.

2 Preliminaries

Let $F_2 = \{0, 1\}$ be the binary field, F_2^n be the n-dimensional vector space over F_2 and F_{2^n} be the Galois field of 2^n elements. The set containing all invertible elements of F_{2^n} is denoted by $F^*_{2^n}$. Since there is a natural isomorphic mapping from F_2^n to the Galois field F_{2^n}, for the simplicity of discussion, we will identify the vector space F_2^n the same as the Galois field F_{2^n} in the sequel.

Any function f from F_{2^n} into F_2 is called a *Boolean function in n variables* and the set of all Boolean functions in n variables is denoted by B_n. The *Hamming weight* of a Boolean function $f \in B_n$ is the cardinality of the set $\{x \in F_{2^n} | f(x) = 1\}$, denoted by $\mathrm{wt}(f)$. The Hamming distance $d(f, g)$ between two Boolean functions $f(x)$ and $g(x)$ is the number of their different coordinates, which equals the Hamming weight of their sum $f + g$, where $+$ denotes the addition on F_2, i.e., the XOR. If the Hamming weight of a Boolean function f in n variables is 2^{n-1}, then f is balanced.

Every Boolean function f over F_{2^n} can be written as the univariate polynomials over F_{2^n} [6,8]:

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

where $a_0,\ a_{2^n-1} \in F_2$, and $a_{2i} = a_i^2 \in F_{2^n},\ 1 \le i \le 2^n - 2$. It is well known that the *algebraic degree* of the Boolean function $f \neq 0$, denoted by $\deg(f)$, expressed by univariate polynomials is

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

where, given the 2-adic expansion $j = j_0 + j_1 2 + \cdots + j_{n-1}2^{n-1}$, $j_i \in F_2, 0 \le i \le n-1$ and $w_2(j)$ denotes the number of all nonzero j_i, $0 \le i \le n-1$. A Boolean function is *affine* if it has algebraic degree at most 1. The set of all affine functions is denoted by A_n.

Let $m|n$, $E = F_{2^m}$ and $L = F_{2^n}$. 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 $E = F_2$, we denote $tr_{L/E}$ simply by tr which is called the *absolute trace function*. The trace function has the following properties [19]:

(a) $tr_{L/E}(ax + by) = atr_{L/E}(x) + btr_{L/E}(y)$ for all $x, y \in L$ and $a, b \in E$.
(b) $tr_{L/E}(x^q) = tr_{L/E}(x)$ for all $x \in L$ and $q = 2^m$.
(c) 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 $x \in E$.

The Walsh transform of $f \in B_n$ at $a \in L = F_{2^n}$ is defined by

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

where

$$\chi(x) = (-1)^{tr(x)}$$

is the canonical additive character on L. The set $\{W_f(a) | a \in F_{2^n}\}$ is said to be the *Walsh spectrum* of f. Nonlinearity of $f \in B_n$, written as $nl(f)$, is defined as the minimum Hamming distance between the function f and all affine functions over F_{2^n}, namely, $nl(f) = \min_{l \in A_n} \{d(f, l)\}$. It is trivial to deduce that the relation between the nonlinearity and the Walsh spectrum is

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

By Parseval's equality, $\sum_{a \in F_{2^n}} W_f(a)^2 = 2^{2n}$, 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, only if n is even, it is possible for a bent function to exit. 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 [10], and can also well withstand the correlation attack [3,12].

We define the *derivative* of f with respect to $a \in F_{2^n}$, denoted by $D_a f$, is the Boolean function $D_a f(x) = f(x) + f(x + a)$ for any $x \in F_{2^n}$. Let V be a k dimensional subspace of F_{2^n} generated by $\alpha_1, \alpha_2, \ldots, \alpha_k$, the k-th order derivative of $f \in B_n$ is defined by

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

for any $x \in F_{2^n}$.

It is to be noted that when $\alpha_1, \ldots, \alpha_k$ are not linearly independent, then $D_{\alpha_1} \ldots D_{\alpha_k} f$ is zero; otherwise, the set $\left\{x + \sum_{i=1}^{k} u_i \alpha_i | u \in F_{2^k}\right\}$ 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 $C_s = \{s, 2s, 2^2 s, \ldots, 2^{n_s - 1} s\}$, 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.

3 The lower bound of the second-order nonlinearity of a class of Boolean function with high nonlinearity

In this section, we first give some lemmas that are needed in the sequel.

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

(a) $Q(cx) = c^2 Q(x)$ for any $c \in F_q$ and $x \in V$;
(b) $B(x, y) := Q(x + y) + Q(x) + Q(y)$ is bilinear on V.

The *kernel* K of a bilinear form Q is the subspace of V defined by $K = \{x \in V | B(x, y) = 0 \text{ for any } y \in V\}$. The following lemmas are obtained from the definitions.

Lemma 1 **([2])** *Let V be a vector space over a field F_q of characteristic 2 and $Q : V \to F_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Lemma 2 **([2])** *If $f : F_{2^n} \to F_2$ 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:*

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

Lemma 3 **([2])** *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.*

The following lemmas are important to prove our conclusions.

Lemma 4 ([5]) *Let f be any n-variable function and r be a positive integer smaller than n. Then we have*

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

Lemma 5 *Let $f(x) = tr\left(\lambda x^d\right)$ where $\lambda \in F_{2^r}^*$, $d = 2^{2r} + 2^r + 1$ and $n = 4r$. Then*

$$nl(D_a f) \geq \begin{cases} 0, & a \in F_{2^r} \\ 2^{4r-1} - 2^{3r-1}, & a \notin F_{2^r} \end{cases}.$$

Proof Since $f(x) = tr(\lambda x^{2^{2r}+2^r+1})$ and $\lambda \in F_{2^r}^*$, we have

$$\begin{aligned} D_a f(x) &= f(x) + f(a+x) \\ &= tr\left(\lambda x^{2^{2r}+2^r+1}\right) + tr\left(\lambda (x+a)^{2^{2r}+2^r+1}\right) \\ &= tr\left(\lambda x^{2^{2r}+2^r+1}\right) + tr\left(\lambda\left(x^{2^{2r}+2^r} + x^{2^{2r}}a^{2^r} + x^{2^r}a^{2^{2r}} + a^{2^{2r}+2^r}\right)(x+a)\right) \\ &= tr\left(\lambda\left(x^{2^{2r}+2^r}a + x^{2^{2r}+1}a^{2^r} + x^{2^{2r}}a^{2^r+1} + x^{2^r+1}a^{2^{2r}}\right.\right. \\ &\quad \left.\left. + x^{2^r}a^{2^{2r}+1} + xa^{2^{2r}+2^r} + a^{2^{2r}+2^r+1}\right)\right). \end{aligned}$$

The Walsh spectrum of the function $D_a f$ is equal to the one of the following functions:

$$\begin{aligned} F(x) &= tr\left(\lambda\left(x^{2^{2r}+2^r}a + x^{2^{2r}+1}a^{2^r} + x^{2^r+1}a^{2^{2r}}\right)\right) \\ &= tr\left(\lambda a^{2^r}x^{2^{2r}+1} + \left(\lambda a^{2^{2r}} + \lambda^{2^{3r}}a^{2^{3r}}\right)x^{2^r+1}\right). \end{aligned}$$

Since $2^r + 1$ and $2^{2r} + 1$ are not in the same cyclotomic coset, $F(x) \neq 0$ for any value of $a \neq 0$. Clearly, when $a = 0$, the lemma holds. Hence, we only consider the case when $a \neq 0$. In this case, F is a quadratic Boolean function. Therefore, by Lemma 2, the Walsh spectrum of F only depends on the dimension k of the kernel of F. By Lemma 3, the kernel of F is the subspace of those b such that the derivative $D_b F(x)$ is constant. Hence, in the following, we calculate those b such that the derivative $D_b F$ is constant.

$$\begin{aligned} D_b F(x) &= F(x) + F(x+b) \\ &= tr\left(\lambda\left(x^{2^{2r}+2^r}a + x^{2^{2r}+1}a^{2^r} + x^{2^r+1}a^{2^{2r}}\right)\right) \\ &\quad + tr\left(\lambda\left((x+b)^{2^{2r}+2^r}a + (x+b)^{2^{2r}+1}a^{2^r} + (x+b)^{2^r+1}a^{2^{2r}}\right)\right) \\ &= tr\left(\lambda\left(\left(x^{2^{2r}}b^{2^r} + x^{2^r}b^{2^{2r}}\right)a + \left(x^{2^{2r}}b + xb^{2^{2r}}\right)a^{2^r}\right.\right. \\ &\quad \left.\left. + \left(x^{2^r}b + xb^{2^r}\right)a^{2^{2r}} + b^{2^{2r}+2^r}a + b^{2^{2r}+1}a^{2^r} + b^{2^r+1}a^{2^{2r}}\right)\right) \end{aligned}$$

$$= tr\left(x\left(\left(a^{2^{2r}}\lambda^{2^{2r}} + a^{2^r}\lambda^{2^{3r}}\right)b^{2^{3r}} + \left(a^{2^{3r}}\lambda^{2^{2r}} + a^{2^r}\lambda\right)b^{2^{2r}} + \left(a^{2^{3r}}\lambda^{2^{3r}} + a^{2^{2r}}\lambda\right)b^{2^r}\right) + \lambda\left(b^{2^{2r}+2^r}a + b^{2^{2r}+1}a^{2^r} + b^{2^r+1}a^{2^{2r}}\right)\right).$$

Therefore $D_bF(x)$ is constant if and only if

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

Since $\lambda \in F_{2^r}^*$, Eq. (3) is equivalent to the equation

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

Raising 2^{-r}-th power to the both sides of Eq. (4) gives the following equation

$$\left(a^{2^r} + a\right)b^{2^{2r}} + \left(a^{2^{2r}} + a\right)b^{2^r} + \left(a^{2^{2r}} + a^{2^r}\right)b = 0. \tag{5}$$

In the following, we consider three cases: (1) $a \in F_{2^r}$, (2) $a \in F_{2^{2r}} \setminus F_{2^r}$, and (3) $a \notin F_{2^{2r}}$.

Case (1): $a \in F_{2^r}$. In this case, for any $b \in F_{2^{4r}}$, Eq. (5) holds. This shows that $k = 4r$.

Case (2): $a \in F_{2^{2r}} \setminus F_{2^r}$. In this case, Eq. (5) is equivalent to the equation $b^{2^{2r}} + b = 0$, which is equivalent to $b \in F_{2^{2r}}$. Hence $k = 2r$.

Case (3): $a \notin F_{2^{2r}}$. In this case, Eq. (5) is a 2^r-polynomial. As a consequence, the dimension k of the kernel of the equation $P(b) := \left(a^{2^r} + a\right)b^{2^{2r}} + \left(a^{2^{2r}} + a\right)b^{2^r} + \left(a^{2^{2r}} + a^{2^r}\right)b$ equals lr, $l = 0,\ 1$, or 2. In the following, we prove that $l = 0$ or $l = 2$.

Consider now the quadratic from F_{q^4} to F_q ($q = 2^r$):

$$H(x) = tr_{L/E}\left(\lambda\left(x^{2^{2r}+2^r}a + x^{2^{2r}+1}a^{2^r} + x^{2^r+1}a^{2^{2r}}\right)\right),$$

where $L = F_{2^{4r}}$ and $E = F_{2^r}$.

The set of roots of $P(x)$ is also the kernel of $H(x)$. In fact, the kernel of $H(x)$ is the set of those such that $B(x) = 0$ for all x with

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

Since $D_bF(x) = tr_{E/F_2}(B(x))$, we get

$$B(x) = tr_{L/E}(P(b)x).$$

Hence the kernel of $H(x)$ is equal to the kernel of $P(x)$. By Lemma 1, the dimension of the kernel of $H(x)$ must have the same parity as 4, so it is even. So we conclude that the dimension of the kernel of $H(x)$ is either 0 or 2, implying that the one of $P(x)$ is either 0 or $2r$, that is, $k = 0$ or $k = 2r$.

Therefore, by Lemma 2 and Eq. (1), we have

$$nl(D_a f) \geq \begin{cases} 0, & a \in F_{2^r} \\ 2^{4r-1} - 2^{3r-1}, & a \notin F_{2^r} \end{cases}.$$

The lemma follows. □

By the above lemmas, we get the following theorem:

Theorem 1 *Let* $f(x) = tr\left(\lambda x^d\right)$ *where* $\lambda \in F_{2^r}^*$, $d = 2^{2r} + 2^r + 1$ *and* $n = 4r$. *Then*

$$nl_2(f) \geq 2^{4r-1} - 2^{2r-1}\sqrt{2^{3r} + 2^r - 1}.$$

Proof By Lemmas 4 and 5, we have

$$\begin{aligned} nl_2(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_{2^n}} nl(D_a f)} \\ &\geq 2^{4r-1} - \frac{1}{2}\sqrt{2^{8r} - 2\left(2^{4r} - 2^r\right)\left(2^{4r-1} - 2^{3r-1}\right)} \\ &\geq 2^{4r-1} - 2^{2r-1}\sqrt{2^{3r} + 2^r - 1}. \end{aligned}$$

The theorem follows. □

4 Concluding remarks

By making an effort to probe 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 with high nonlinearity and low differential uniformity. Results are finally achieved which reveal that the second-order nonlinearity of the class of Boolean functions is also high. Compared with the results illustrated by Iwata-Kurosawa and that of Theorem 1 of [16], our lower bound is much better as seen from the following table. However, it should be noted that the algebraic degree of our considered functions is 3, the algebraic immunity hence is at most 3. In this case, the lower bound cannot be obtained by the relation between algebraic immunity and the r-th order nonlinearity as studied in [7] and [4].

r	2	3	4	5	6
Iwata-Kurosawa's bound	56	896	14,336	22,9376	3670,016
Bound of Theorem 1 of [16]	N/A	960	N/A	N/A	4.17792×10^6
Bound of Theorem 1	62	1,318	24,561	431,562	7.33991×10^6

r	7	8	9	10	11
Iwata-Kurosawa's bound	5.87203×10^7	9.39524×10^8	1.50324×10^{10}	2.40518×10^{11}	3.84829×10^{12}
Bound of Theorem 1 of [16]	N/A	N/A	1.71757×10^{10}	N/A	N/A
Bound of Theorem 1	1.22354×10^8	2.01326×10^9	3.28412×10^{10}	5.32576×10^{11}	8.60172×10^{12}

Acknowledgments The authors would like to thank the anonymous referees and the editors for their valuable comments that improved the paper.

References

1. Bracken, C., Leander, G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Available at. http://arxiv.org/abs/0901.1824
2. Canteaut, A., Charpin, P., Kyureghyan, G.M.: A new class of monomial bent functions. Finite Fields Appl. **14**, 221–241 (2008)
3. Canteaut, A., Trabbia, M.: Improved fast correlation attacks using parity-check equations of weight 4 and 5. Advances in Cryptology-Eurocrypt 2000, LNCS 1807, Springer-Verlag, pp. 573–588 (2000)
4. Carlet, C.: On the higher order nonlinearities of algebraic immune functions. Advances in Cryptology -CRYPTO 2006, LNCS 4117, Springer-Verlag, pp. 584–601 (2006)
5. Carlet, C.: 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., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs Codes Cryptography **15**(2), 125–156 (1998)
7. Carlet, C., Dalai, D., Gupta, K., Maitra, S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory **52**(7), 3105–3121 (2006)
8. Carlet, C., Feng, K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and goold nonlinearity. Advances in Cyrptology-ASIACRYPT 2008, LNCS 5350, Springer-Verlag, pp. 425–440 (2008)
9. Carlet, C., Mesnager, S.: Improving the upper bounds on the covering radii of binary Reed-Muller codes. IEEE Trans. Inform. Theory **53**(1), 162–173 (2007)
10. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. Advances in Cryptology -EUROCRYPT'94, LNCS 950, Springer-Verlag, pp. 356–365 (1995)
11. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes. Amsterdam, The Netherlands: North-Holland (1977)
12. Ding, C., Xiao, G., Shan, W.: The Stability Theory of Stream Ciphers. LNCS 561, Springer-Verlag (1991)
13. Dobbertin, H.: One-to-one highly nonlinear power functions on $GF(2^n)$. Appl. Algebra Eng. Commun. Comput. **9**, 139–152 (1998)
14. Dumer, I., Kabatiansky, G., Tavernier, C.: List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity. In: Proceedings IEEE International Symposium Information Theory, Seattle, WA, pp.138–142 Jul. (2006)
15. Fourquet, R., Tavernier, C.: List decoding of second order Reed-Muller and its covering radius implications. In: Proceedings WCC 2007, Versailles, France, pp. 147–156, Apr. (2007)
16. Gangopadhyay, S., Sarkar, S., Telang, R.: On the lower bounds of the second-order nonlinearity of some Boolean functions. Inf. Sci. **180**(2), 266–273 (2010)
17. Iwata, T., Kurosawa, K.: Probabilistic higher order differential attack and higher order bent functions. In: Proceedings ASIACRYPT'99, LNCS 1716, Berlin, Germany: Springer-Verlag, pp. 62–74 (1999)
18. Kabatiansky, G., Tavernier, C.: List decoding of second-order Reed-Muller codes. In: Proceedings 8th International Symposium Communication Theory and Applications, Ambelside, UK, Jul. (2005)
19. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Reading, MA (1983)
20. Sun, G., Wu, C.: The lower bounds on the second-order nonlinearity of three classes of Boolean functions with high nonlinearity. Inf. Sci. **179**(3), 267–278 (2009)