一类 Bent 函数的二阶非线性度下界

李春雷[1),2)] 张焕国[1),2)] 曾祥勇[3),4)] 胡 磊[4)]

[1)](武汉大学计算机学院 武汉 430079)

[2)](空天信息安全与可信计算教育部重点实验室 武汉 430079)

[3)](湖北大学数学与计算机科学学院 武汉 430062)

[4)](中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 为了防止存在有效的低次函数逼近,对于较小的正整数r,用于对称密码系统中的布尔函数应具有较高的r-阶非线性度.当$r>1$时,准确计算布尔函数的r-阶非线性度十分困难,已有的研究工作主要是通过分析其导函数的$(r-1)$-阶非线性度来确定布尔函数的r-阶非线性度下界.对于整数$n\equiv 2 \pmod 4$,文中确定了一类由Niho指数生成的Bent函数的二阶非线性度下界.与相同变元个数的两类Bent函数和三类布尔函数相比,这类Bent函数具有更紧的二阶非线性度下界.

关键词 Bent函数;二阶非线性度;双线性函数;Walsh谱;Reed-Muller码

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01588

The Lower Bound on the Second-Order Nonlinearity for a Class of Bent Functions

LI Chun-Lei[1),2)] ZHANG Huan-Guo[1),2)] ZENG Xiang-Yong[3),4)] HU Lei[4)]

[1)](*School of Computer, Wuhan University, Wuhan* 430079)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan* 430079)

[3)](*Faculty of Mathematics and Computer Science, Hubei University, Wuhan* 430062)

[4)](*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract The Boolean functions used in symmetric ciphers should have high rth-order nonlinearity to resist against the low-degree approximation cryptanalysis. For an integer $r>1$, it is quite difficult to compute the rth-order nonlinearity of a Boolean function, and the known literatures mainly utilize the $(r-1)$th-order nonlinearity of its derivatives to deduce the lower bound on the rth-order nonlinearity. For an integer $n\equiv 2 \pmod 4$, this paper investigates the nonlinearities of the corresponding derivative functions for a class of Bent functions constructed from Niho exponents, and then determines the lower bound of the second-order nonlinearity for this class of Bent functions. Compared with two Bent functions and three classes of Boolean functions with the same number of variables, this class of Bent functions has a tighter lower bound on the second-order nonlinearity.

Keywords Bent function; second-order nonlinearity; bilinear function; Walsh spectrum; Reed-Muller codes

1 引 言

布尔函数在密码学和编码学等领域有着重要的应用.在对称密码系统中,为了抵抗已知的一些攻击,如仿射逼近攻击、相关攻击、代数攻击等,密码函数需满足一些设计准则,其中具有较高非线性度的准则尤为重要[1].为了抵抗低次函数的逼近,密码函

收稿日期:2010-06-22;最终修改稿收到日期:2011-11-16.本课题得到国家自然科学基金(60970115,60970116,61003267,91018008,61003268)资助.**李春雷**,男,1984年生,博士,主要研究方向为信息安全与密码学.E-mail:chunleili2008@yahoo.com.cn.**张焕国**,男,1945年生,教授,博士生导师,主要研究领域为信息安全与可信计算.**曾祥勇**,男,1973年生,教授,主要研究领域为密码学与序列设计.**胡 磊**,男,1967年生,教授,博士生导师,主要研究领域为序列设计、椭圆曲线公钥密码、理论密码学.

数还应具有较好的非线性度轮廓，即 $r(r\geq 1)$-阶非线性度要高. 布尔函数的 r-阶非线性度是指它和所有次数不超过 r 的布尔函数的最小汉明距离，记作 $nl_r(f)$；当 $r=1$ 时，$nl_1(f)$ 就是我们熟悉的布尔函数的非线性度 $nl(f)$. 对于布尔函数的 1-阶非线性度，人们从离散傅立叶变换、组合论等角度研究了它的性质以及和其它密码指标如代数次数、弹性、代数免疫阶之间的联系，在计算和理论方面都取得了丰硕的成果[1-3]. 然而当 $r\geq 2$ 时，关于布尔函数 r-阶非线性度的研究很困难，进展比较缓慢. 文献[4]从编码的角度给出了目前计算布尔函数二阶非线性度的最优算法，但给出的最优算法仍不能有效地计算变元个数大于 12 的布尔函数的二阶非线性度. 文献[5-6]考察了布尔函数 r-阶非线性度的上界以及和代数免疫阶的关系. 通过分析导函数的 $(r-1)$-阶非线性度与自身 r-阶非线性度的关系，Carlet 提出了利用布尔函数的导函数确定其 r-阶非线性度下界的方法，并考察了 M-M 函数、Welch 函数的二阶非线性度下界以及 Inverse 函数的 r-阶非线性度下界[7]. 此后，文献[8-10]确定了几类非线性度较高的幂函数 $tr_1^n(x^d)$ 的二阶非线性度下界.

Bent 函数作为非线性度达到极大值的一类布尔函数，一直受到广泛的关注[11]. 当 $r\geq 2$ 时，Bent 函数的 r- 阶非线性度也是人们关心的问题. 文献[12-13]研究了 M-M 类 Bent 函数的二阶非线性度下界，文献[13]给出了一类由 Semi-Bent 函数级联生成的 Bent 函数的二阶非线性度. 不过这两类 Bent 函数二阶非线性度的研究结果都不太理想. 继文献[14]，本文确定了一类由两项 Niho 指数生成的 Bent 函数

$$f(x)=tr_1^n(\mu x^{(2^k-1)/2+1}+x^{(2^k-1)/4+1})$$

(其中，$\mu+\mu^{2^k}=1$，$n=2k$，k 为奇数) 的二阶非线性度下界. 通过具体的比较，对于相同的变元数 n，较之文献[12-13]中 Bent 函数和文献[8-10]中函数 $tr_1^n(x^d)$ 的结果，本文讨论 Bent 函数的二阶非线性度下界更大，能够更好地抵抗二次函数的逼近. 与已有的研究不同，本文通过分类讨论具体确定了导函数 D_af 的 Walsh 谱分布，而不是仅给出导函数 D_af 的非线性度下界. 对于不同向量 $\boldsymbol{a}\in F_2^{2k}$，利用各导函数 D_af 的 Walsh 谱之间的数量关系，$nl_2(f)$ 的下界被进一步提高. 另外，导函数 D_af 的 Walsh 谱分布的具体确定为更精确地考察这类 Bent 函数的二阶非线性度提供了有价值的参考.

本文第 2 节介绍相关的预备知识和结论；第 3 节通过具体分析其导函数的 Walsh 谱确定一类 Bent 函数的二阶非线性度；第 4 节将本文的工作和已有的结果进行比较；最后第 5 节给出结论部分.

2　预备知识

记 $\boldsymbol{F}_{2^n}$ 表示由 2^n 个元素组成的有限域. 由于有限域 $\boldsymbol{F}_{2^n}$ 和二元域 F_2 上的 n 维向量空间 $\boldsymbol{F}_2^n$ 存在同构，故本文将有限域 $\boldsymbol{F}_{2^n}$ 和向量空间 $\boldsymbol{F}_2^n$ 等同看待. 一个 n 元布尔函数 f 是指 n 维向量空间 $\boldsymbol{F}_2^n$ 到 F_2 上的映射，所有 n 元布尔函数 f 组成的集合记为 $\mathcal{B}_n$. 一个 n 元布尔函数 f 可由如下的多项式唯一表示

$$f(x_1,x_2,\cdots,x_n)=\sum_{I\subseteq\{1,2,\cdots,n\}}a_I\prod_{i\in I}x_i,$$

其中，$a_I\in F_2$. 这种表达式被称为 f 的代数正规型. 它的代数次数被定义为代数正规型中系数非零的乘积项 $\prod_{i\in I}x_i$ 中最大次数，记为 $\deg(f)$. 给定整数 $0\leq r\leq n$，记 $RM(r,n)$ 表示所有代数次数不大于 r 的 n 元布尔函数组成的集合，即长度为 2^n 的 r 阶 Reed-Muller 码.

布尔函数 $f\in\mathcal{B}_n$ 也可由它的真值表，一条长度为 2^n 的 0，1 序列表示：

$$[f(\overline{0}),f(\overline{1}),f(\overline{2}),\cdots,f(\overline{2^n-1})],$$

其中 $\overline{a}$ 表示整数 a 的二进制表示.

函数 f 的汉明权重是指其真值表中取值为 1 的元素个数，记为 $wt(f)$. 两个布尔函数 $f,g\in\mathcal{B}_n$ 的汉明距离 $d(f,g)$ 被定义为两个函数真值表中取值不同的元素个数，换句话说，$d(f,g)=wt(f+g)$ (下面将通常意义上的加法和有限域 F_2 上的加法一并用加号“+”表示).

定义 1[5]. 对于正整数 $r\leq n$，n 元布尔函数 f 的 r-阶非线性度被定义为函数 f 和集合 $RM(r,n)$ 中所有函数的最小汉明距离，记作 $nl_r(f)$. 当 r 取遍整数 $1\sim n-1$ 时，由 r-阶非线性度组成的序列被称为是函数 f 的非线性度轮廓.

布尔函数 f 的 1-阶非线性度简称为非线性度，简记为 $nl(f)$. 可以通过布尔函数的 Walsh 变换(亦称 Hadmard 变换) 确定其非线性度. 对于向量 $\boldsymbol{\lambda}$，$\boldsymbol{x}\in F_2^n$，它们的内积被定义为

$$\boldsymbol{\lambda}\cdot\boldsymbol{x}=\lambda_1x_1+\lambda_2x_2+\cdots+\lambda_nx_n,$$

这里的加号“+”是指模 2 相加. 布尔函数 $f\in\mathcal{B}_n$ 的 Walsh 变换 W_f 是从 F_2^n 到整数环 $\mathbb{Z}$ 的一个映射

$$W_f(\lambda)=\sum_{x\in F_2^n}(-1)^{f(x)+\lambda\cdot x}.$$

$W_f(\lambda)$的值称为布尔函数 f 的 Walsh 谱值. 若 $W_f(0)=0$,即函数 f 的汉明权重等于 2^{n-1},布尔函数是平衡的. 因此,n 元布尔函数 f 的非线性度可借助 Walsh 变换确定如下:

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{\lambda\in F_2^n}|W_f(\lambda)|.$$

根据 Parseval 等式

$$\sum_{\lambda\in F_2^n}W_f(\lambda)^2=2^{2n}$$

可知$\max_{\lambda\in F_2^n}|W_f(\lambda)|\geq 2^{n/2}$,进而有

$$nl(f)\leq 2^{n-1}-2^{n/2-1}.$$

当等式成立时,布尔函数 f 被称为 Bent 函数,不难看出 Bent 函数只存在于偶变元布尔函数中.

定义 2[1]. 函数 $f\in\mathcal{B}_n$ 在向量 $\boldsymbol{a}\in F_2^n$ 处的导函数 D_af 定义为 $D_af(x)=f(x)+f(x+\boldsymbol{a})$. 对函数 f 在若干向量 $\boldsymbol{a}_i$ 处多次求导可得到其高阶导函数

$$D_{\boldsymbol{a}_1}D_{\boldsymbol{a}_2}\cdots D_{\boldsymbol{a}_m}f(x)=\sum_{u\in F_2^m}f\Big(x+\sum_{i=1}^{m}u_i\boldsymbol{a}_i\Big).$$

对于布尔函数 $f\in\mathcal{B}_n$,文献[7]利用其导函数 D_af 的 $(r-1)$-阶非线性度给出了函数 f 的 r-阶非线性度的下界.

引理 1[7]. 对于 n 元布尔函数 f 和正整数 $r\leq n$,函数 f 的 r-阶非线性度满足

$$nl_r(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{\boldsymbol{a}\in F_2^n}nl_{r-1}(D_af)}.$$

若对于所有的向量 $\boldsymbol{a}\in F_2^n$,存在正整数 K 和 k 满足 $nl_{r-1}(D_af)\geq 2^{n-1}-K2^k$,根据上面的不等式可得

$$nl_r(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)K2^{k+1}+2^n}$$

$$\approx 2^{n-1}-\sqrt{K}2^{(n+k-1)/2}.$$

对于二次函数 $f\in\mathcal{B}_n$,其代数正规型可由二次型 $\boldsymbol{x}\boldsymbol{Q}\boldsymbol{x}^{\mathrm{T}}$ 唯一表示,其中 $\boldsymbol{Q}=(q_{ij})$ 是一个 $n\times n$ 的上三角矩阵. 此外,二次函数 f 的双线性函数 $B_f(\boldsymbol{x},\boldsymbol{y})$ 定义为

$B_f(\boldsymbol{x},\boldsymbol{y})=f(0)+f(\boldsymbol{x})+f(\boldsymbol{y})+f(\boldsymbol{x}+\boldsymbol{y})=\boldsymbol{x}\mathcal{Q}\boldsymbol{y}^{\mathrm{T}}$,

其中矩阵 $\mathcal{Q}=\boldsymbol{Q}+\boldsymbol{Q}^{\mathrm{T}}$ 是一个 $n\times n$ 的对称矩阵. 二次函数 f 的根空间 rad(f)定义为

$\mathrm{rad}(f)=\{\boldsymbol{x}\in GF_{2^n}\mid\forall\boldsymbol{y}\in GF_{2^n},\ B_f(\boldsymbol{x},\boldsymbol{y})=0\}$,

与矩阵 $\mathcal{Q}$ 的零空间 $\mathcal{N}(\mathcal{Q})=\{\boldsymbol{x}\in GF_2^n\mid\boldsymbol{x}\mathcal{Q}=\boldsymbol{0}\}$ 相同.

引理 2[15]. 二次函数 $f\in\mathcal{B}_n$ 的 Walsh 谱分布可由它的根空间 rad(f)的维数 t 唯一确定(如表 1 所示).

表 1 二次函数的 Walsh 谱分布

$W_f(\lambda)$	λ 的个数
0	2^n-2^{n-t}
$2^{(n+t)/2}$	$2^{n-t-1}+(-1)^{f(0)}2^{(n-t-2)/2}$
$-2^{(n+t)/2}$	$2^{n-t-1}-(-1)^{f(0)}2^{(n-t-2)/2}$

3 三次 Bent 函数

对于整数 $n=2k$ 和有限域 F_{2^n} 上幂函数 x^d,指数 d 被称为是 Niho 指数如果 x^d 限制 F_{2^k} 上是线性函数,换句话说,存在整数 i 满足 $d\equiv 2^i\pmod{2^k-1}$. 文献[14]给出了基于两项 Niho 指数构造 Bent 函数的方法.

设偶数 $n=2k$,k 为奇数,若元素 $\mu\in F_{2^n}$ 满足 $\mu+\mu^{2^k}=1$,则布尔函数

$$\begin{aligned}f(x)&=tr_1^n(\mu x^{(2^k-1)/2+1}+x^{(2^k-1)/4+1})\\&=tr_1^n(\mu x^{2^k+1}+x^{2^k+3})\end{aligned}\tag{1}$$

是 Bent 函数[14].

上式定义的 Bent 函数 f 的代数次数等于 3,下面的定理确定了它的导函数 D_af 的根空间维数.

定理 1. 对于元素 $a\in F_{2^n}^*$,记 Bent 函数 $f(x)$ 的导函数 D_af 的根空间为 rad(D_af),则当 $a\in F_{2^k}^*$ 时,根空间 rad(D_af)的维数 $t=k+1$;否则,rad(D_af)的维数 $t=2$.

证明. Bent 函数 $f(x)$ 的在元素 $a\in F_{2^n}^*$ 处的导函数

$$\begin{aligned}D_af(x)&=tr_1^n[\mu(x+a)^{2^k+3}+(x+a)^{2^k+1}]+\\&\quad tr_1^n(\mu x^{2^k+3}+x^{2^k+1})\\&=tr_1^n[\mu(x^{2^k}a+xa^{2^k})+(x^{2^k+2}a+\\&\quad x^{2^k+1}a^2+x^3a^{2^k}xa^{2^k+2}+x^2a^{2^k+1}+\\&\quad x^{2^k}a^3)+(\mu a^{2^k+1}+a^{2^k+3})]\\&=tr_1^n(x^{2^k+2}a+x^{2^k+1}a^2+x^3a^{2^k})+\\&\quad tr_1^n[x^{2^k}(\mu a+a^3)+x^2a^{2^k+1}+\\&\quad x(a^{2^k}+a^{2^k+2})+(\mu a^{2^k+1}+a^{2^k+3})].\end{aligned}$$

由于对于任意的函数 $l(x)\in RM(1,n)$ 的双线性函数 $B_l(x,y)=0$,故二次函数 D_af 的双线性函数与函数

$$g(x)=tr_1^n(x^{2^k+2}a+x^{2^k+1}a^2+x^3a^{2^k})$$

相同. 函数 $g(x)$ 的双线性函数

$$\begin{aligned}B_g(x,y)n&=g(0)+g(x)+g(y)+g(x+y)\\&=tr_1^n[(x^{2^k+2}a+x^{2^k+1}a^2+x^3a^{2^k})+\\&\quad(y^{2^k+2}a+y^{2^k+1}a^2+y^3a^{2^k})+\\&\quad((x+y)^{2^k+2}a+(x+y)^{2^k+1}a^2+\\&\quad(x+y)^3a^{2^k})]\end{aligned}$$

$$=tr_1^n[a(x^{2^k}y^2+y^{2^k}x^2)+a^2(x^{2^k}y+y^{2^k}x)+$$
$$a^{2^k}(x^2y+y^2x)]$$
$$=tr_1^n[y(x^{2^{2k-1}}a^{2^{k-1}}+x^{2^{k+1}}a^{2^k}+$$
$$x^{2^k}(a^{2^{k+1}}+a^2)+x^{2^{k-1}}a^{2^{2k-1}}+x^2a^{2^k})].$$

记函数

$$L_a(x)=x^{2^{2k-1}}a^{2^{k-1}}+x^{2^{k+1}}a^{2^k}+$$
$$x^{2^k}(a^{2^{k+1}}+a^2)+x^{2^{k-1}}a^{2^{2k-1}}+x^2a^{2^k},$$

易知

$$\mathrm{rad}(D_af)=\{x\in GF_{2^n}\mid L_a(x)=0\}$$
$$=\{x\in F_{2^n}\mid (L_a(x))^2=0\}.$$

为简便起见，记 $y=x^{2^k}$ 和 $b=a^{2^k}$. 由 $n=2k$ 可知 $x=y^{2^k}$，$a=b^{2^k}$. 则

$$(L_a(x))^2=x^{2^{k+2}}a^{2^{k+1}}+x^{2^{k+1}}(a^{2^{k+2}}+a^4)+$$
$$x^{2^k}a+x^4a^{2^{k+1}}+xa^{2^k},$$

故方程 $(L_a(x))^2=0$ 可转化为

$$(y^4+x^4)b^2+y^2(a+b)^4+(ya+xb)=0 \quad (2)$$

下面分 $a\in F_{2^k}^*$ 和 $a\notin F_{2^k}^*$ 两种情况讨论方程(2)的解的个数.

情形 1.　$a\in F_{2^k}^*$，对于这种情形，由于 $a=b$，方程(2)可化简为

$$(y^4+x^4)a^2+(y+x)a=0.$$

记 $z=y+x\in F_{2^k}$，上面的方程为 $z(z^3a+1)=0$. 设 β 为有限域 F_{2^k} 的本原元，由 k 是奇数可知 $\gcd(2^k-1,3)=1$，故存在整数 i 满足 $a=\beta^{3i}$，进而方程 $z(z^3a+1)=0$ 在 F_{2^k} 上有两个根 $z=0,\beta^{-i}$. 进一步地，关于 x 的方程 $L_a(x)=0$ 在 F_{2^n} 有 2^{k+1} 个解，进而 $\mathrm{rad}(D_af)$ 的维数等于 $k+1$.

情形 2.　$a\in F_{2^n}\setminus F_{2^k}$. 此时对方程(2)的两边取 2^k 次方幂可得方程

$$(y^4+x^4)a^2+x^2(a+b)^4+(ya+xb)=0 \quad (3)$$

式(2)和式(3)相加等于

$$(y^4+x^4)(a+b)^2+(y^2+x^2)(a+b)^4=0.$$

由 $a\notin F_{2^k}$ 可知 $a+b\neq 0$，故上式可化简为

$$(y^4+x^4)+(y^2+x^2)(a+b)^2=0 \quad (4)$$

对方程(4)开平方(即取 2^{n-1} 次方幂)可得方程

$$(y^2+x^2)+(y+x)(a+b)=0 \quad (5)$$

$b^2\times$式(4)+式(2)可得

$$y^2(a+b)^2a^2+x^2(a+b)^2b^2+(ya+xb)=0 \quad (6)$$

将 $(a+b)^4a^4\times$式(4)的结果和式(6)的平方相加可得

$$y^2[(a+b)^6a^4+a^2]+x^4(a+b)^8+$$
$$x^2[(a+b)^6a^4+b^2]=0 \quad (7)$$

对上式开平方：

$$y[(a+b)^3a^2+a]+x^2(a+b)^4+$$
$$x[(a+b)^3a^2+b]=0 \quad (8)$$

将 $((a+b)^6a^4+a^2)\times$式(5)的结果和(7)相加，并约去结果中的 $(a+b)$ 项后可得方程

$$y[(a+b)^6a^4+a^2]+x^4(a+b)^7+x^2(a+b)+$$
$$x[(a+b)^6a^4+a^2]=0 \quad (9)$$

消去式(8)和式(9)中的 y 项可得关于 x 的方程

$$x^4(a+b)^6+x((a+b)^3a^2+a)+$$
$$x^2[(a+b)^3((a+b)^3a^2+a)+1]=0.$$

记上面的方程为 $P(x)=0$，对多项式 $P(x)$ 分解因式如下：

$$x,(x+a),(a+b)^3x+1,(a+b)^3x+1+a(a+b)^3,$$

因此方程 $P(x)=0$ 的解空间为

$$\{0,a,(a+b)^{-3},(a+b)^{-3}+a\}.$$

不难验证方程 $P(x)=0$ 的解都是方程 $L_a(x)=0$ 的解，故根空间 $\mathrm{rad}(D_af)$ 的维数等于 2.　　证毕.

基于定理 1 的结论，下面的定理确定了式(1)中 Bent 函数的二阶非线性度的下界.

定理 2.　对于奇数 k，Bent 函数 $f(x)=tr_1^{2k}(\mu x^{2^k+1}+x^{2^k+3})$，其中 $\mu+\mu^{2^k}=1$ 的二阶非线性度满足

$$nl_2(f)\geq 2^{2k-1}-\frac{1}{2}\sqrt{2^{3k+1}+2^{\frac{5k+1}{2}}-2^{2k}-2^{\frac{3k+1}{2}}}$$
$$\approx 2^{2k-1}-2^{\frac{3k-1}{2}}.$$

证明.　对于元素 $a\in F_{2^n}^*$，根据引理 2 和定理 1 可知，若 $a\in F_{2^k}^*$，$nl(D_af)=2^{2k-1}-2^{(3k-1)/2}$；否则，$nl(D_af)=2^{2k-1}-2^k$. 进一步地，由引理 1 可得出如下结论

$$nl_2(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{a\in F_{2^n}}nl(D_af)}$$
$$=2^{2k-1}-\frac{1}{2}\sqrt{2^{3k+1}+2^{\frac{5k+1}{2}}-2^{2k}-2^{\frac{3k+1}{2}}}.$$

证毕.

4　结果比较

对于奇数 k 和整数 $n=2k$，我们下面对定理 2 给出的二阶非线性度下界和已有的研究结果进行比较.

4.1　与 Bent 函数的已有结果比较

已有的研究中，对 Bent 函数二阶非线性度的讨论很少，文献[7]讨论了 M-M 类 Bent 函数的二阶非线性度下界. 对于函数 $f_{\phi,g}(x,y)=x\cdot\phi(y)+g(y)$，$x,y\in F_2^k$，其二阶非线性度

$$nl_2(f_{\phi,g})\geq 2^{2k-1}-\frac{1}{2}\sqrt{2^{3k}+2^k(2^{2k}-2^k)M(\phi)},$$

其中，$M(\phi)=\max_{u,b\in F_2^k,b\neq 0}|(D_b\phi)^{-1}(u)|$.

此下界取决于置换映射 ϕ 的导函数的性质. 文献[12]对置换 $\phi(y)=y^{2^{(k+1)/2}+1}+y^3+y$ 生成的三次 Bent 函数进行研究，确定了二阶非线性度

$$nl_2(f_{\phi,g})\geq 2^{2k-1}-\frac{1}{2}\sqrt{2^{\frac{7k}{2}+3}+2^{2k}-2^{\frac{3k}{2}+3}}$$

$$\approx 2^{2k-1}-2^{\frac{7k+2}{4}}.$$

不难看出，此下界低于定理 2 中给出的下界. 另外，文献[13]确定了一类由 Semi-Bent 函数级联而成的 Bent 函数的二阶非线性度，此类 Bent 函数的二阶非线性度为 $2^{2k-2}-2^{k-1}$，明显低于定理 2 中给出的下界. 对于奇数 $5\leq k\leq 15$，表 2 比较了文中讨论的 Bent 函数和这两类 Bent 函数的二阶非线性度下界.

表 2 Bent 函数的二阶非线性下界比较

n	文献[12]的结果	文献[13]的结果	本文的结果
10	240	0	377
14	4302	1303	7138
18	65280	53135	122757
22	1047552	1215407	2031114
26	16773120	23578638	33027271
30	268419072	424007704	532668456

4.2 与函数 $tr_1^n(x^d)$ 的已有结果比较

文献[8-10]确定了几类非线性度较高的函数 $tr_1^n(x^d)$ 的二阶非线性度下界. 对于奇数 k，当指数 $d_1=2^{k+1}+3$ 或 $2^k+2^{(k+1)/2}+1$ 时，文献[8]指出函数 $f_1(x)=tr_1^{2k}(x^{d_1})$ 的二阶非线性度满足

$$nl_2(f_1)\geq 2^{2k-1}-\frac{1}{2}\sqrt{2^{3k+1}+2^{\frac{5k}{2}+1}-2^{2k}-2^{\frac{3k}{2}+1}}.$$

对于整数 $n=6k_1$，文献[9]给出了函数 $tr_1^n(x^{2^{2k_1}+2^{k_1}+1})$ 的二阶非线性度下界，文献[10]进一步提高了文献[9]中的结果，并考察了形如 $f_2(x)=tr_1^n(x^{2^{2i}+2^i+1})$，$\gcd(n,i)=1$ 的二阶非线性度下界，对于奇数 k 和整数 $n=2k$，函数 f_2 的二阶非线性度满足

$$nl_2(f_2)\geq 2^{2k-1}-\frac{1}{2}\sqrt{2^{3k+2}+2^{2k}-2^{k+2}},$$

对于奇数 $5\leq k\leq 15$，下面的表 3 比较了本文的 Bent 函数和文献[8,10]中几类函数的二阶非线性度下界.

表 3 本文 Bent 函数与文献[8,10]函数的二阶非线性下界比较

n	文献[10]的结果	文献[8]的结果	本文的结果
10	330	374	377
14	6742	7125	7138
18	119484	122705	122757
22	2004464	2030904	2031114
26	32812965	33027271	33027271
30	530939248	532665070	532668456

事实上，函数 f 的二阶非线性度下界可以有一定的提高. 对于任意的二次函数 $h(x)$ 和 $a\in F_2^n$，

$$\Big(\sum_{x\in F_2^n}(-1)^{f(x)+h(x)}\Big)^2=\sum_{x,a\in F_2^n}(-1)^{f(x)+f(a)+h(x)+h(a)}$$

$$=\sum_{a\in F_2^n}\sum_{x\in F_2^n}(-1)^{D_af(x)+D_ah(x)}.$$

由于 $\deg(D_ah)\leq 1$，根据定理 1，对于非零向量 $\boldsymbol{a}$，指数和 $\sum_{x\in F_2^n}(-1)^{D_{\boldsymbol{a}}f(x)+D_{\boldsymbol{a}}h(x)}$ 可能等于 0，$\pm 2^{(3k+1)/2}$，$\pm 2^{k+1}$，故 $\Big(\sum_{x\in F_2^n}(-1)^{f(x)+h(x)}\Big)^2=2^{2k}+N_1\cdot 2^{(3k+1)/2}+N_2\cdot 2^{k+1}$. 其中整数 $0\leq N_1\leq 2^k-1$，$0\leq N_2\leq 2^{2k}-2^k$. 由于指数和 $\sum_{x\in F_2^n}(-1)^{f(x)+h(x)}$ 是偶数，记 $\widetilde{N}_1,\widetilde{N}_2$ 是使

$$\Phi(N_1,N_2)=2^{2k}+N_1\cdot 2^{(3k+1)/2}+N_2\cdot 2^{k+1}$$

为完全平方数且 $\sqrt{\Phi(\widetilde{N}_1,\widetilde{N}_2)}$ 是偶数的最大整数，则有

$$nl_2(f)\geq 2^{2k-1}-\frac{1}{2}\sqrt{\Phi(\widetilde{N}_1,\widetilde{N}_2)} \qquad (10)$$

由于 $\Phi(\widetilde{N}_1,\widetilde{N}_2)\leq\Phi(2^k-1,2^{2k}-2^k)$，较之定理 2 的结果，上式中的下界更优，下面的表 4 对两种结果进行了比较.

表 4 下界优化结果

n	定理 2 的下界	优化后的下界	对应的$(\widetilde{N}_1,\widetilde{N}_2)$
10	14	16	(7,46)
14	377	380	(31,949)
18	7138	7144	(127,16801)
22	122757	122768	(511,260929)
26	2031114	2089056	(2047,4191785)
30	33028116	33521984	(8191,67099737)

5 结束语

对于奇数 k 和整数 $n=2k$，本文考察了一类由 Niho 型 Bent 函数 $f(x)=tr_1^n(\mu x^{(2^k-1)/2+1}+x^{(2^k-1)/4+1})$ 的二阶非线性度的下界. 对于相同的参数 n，通过分析比较，这类函数的二阶非线性度的下界优于已有的结果，能够较好地抵抗二次函数逼近攻击. 与已有的研究工作不同，本文确定了导函数 D_af 的 Walsh 谱分布，可用来提高 f 的二阶非线性度下界，也为进一步精确考察 f 的二阶非线性度提供参考.

参 考 文 献

[1] Carlet C. Boolean functions for cryptography and error

correcting codes//Crama Y, Hammer P eds. Boolean Methods and Models. Cambridge, U. K.: Cambridge University Press, 2010: 257-397

[2] Carlet C, Zeng X, Li C, Hu L. Further properties of several classes of Boolean functions with optimum algebraic immunity. Design Codes and Cryptography, 2009, 52(3): 303-338

[3] Meng Q, Zhang H, Yang M, Wang Z. Analysis of affinely equivalent Boolean functions. Science in China Series F: Information Sciences, 2007, 50(3): 299-306

[4] Fourquet R, Tavernier C. An improved list decoding algorithm for the second order Reed-Muller codes and its applications. Design Codes and Cryptography, 2008, 49(1): 323-340

[5] Elsheh E, Ben A, Hamza, Youssef A. On the nonlinearity profile of cryptographic Boolean functions. IEEE Transactions on Information Theory, 2008, 53(1): 1767-1770

[6] Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. IEEE Transactions on Information Theory, 2008, 54(8): 3656-3662

[7] Carlet C. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. IEEE Transactions on Information Theory, 2008, 54(8): 1262-1272

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

[9] Gangopadhyay S, Sarkar S, Telang R. On the lower bounds of the second order nonlinearity of some Boolean functions. Information Sciences, 2010, 180(2): 266-273

[10] Gode R, Gangopadhyay S. On second order nonlinearities of cubic monomial Boolean functions. Information Sciences, 2010, 180(10): 1781-1795

[11] Rothaus O S. On Bent functions. Journal of Combinatorial Theory Secies A, 1976, 20: 300-305

[12] Sarkar S, Gangopadhyay S. On the second order nonlinearity of a cubic Maiorana-McFarland Bent function. International Journal of Foundations of Computer Science, 2010, 21(3): 243-254

[13] Kolokotronis N, Limniotis K, Kalouptsidis N. Best affine and quadratic approximations of particular classes of Boolean functions. IEEE Transactions on Information Theory, 2009, 55(11): 5211-5222

[14] Dobbertin H, Leander G et al. Construction of Bent functions via Niho power functions. Journal of Combinatorial Theory Secies A, 2006, 113(5): 779-798

[15] Lidl R, Niederriter H, Cohn P M, Lyndon R. Finite Fields (Encyclopedia of Mathematics and Its Applications). Addision-Wesley Publishing Company, 1983

LI Chun-Lei, born in 1984, Ph. D. candidate. His research interests include cryptography and information security.

ZHANG Huan-Guo, born in 1945, professor, Ph. D. supervisor. His research interests include information security and trusted computing.

ZENG Xiong-Yong, born in 1973, professor. His research interests include cryptography and sequence design.

HU Lei, born in 1967, professor, Ph. D. supervisor. His research interests include sequence design, ECC public key cryptosystem and theoretical cryptography.

Background

To resist against known attacks on LFSR-based stream ciphers, Boolean functions used in the cipher should have cryptographically good properties, including balancedness, high algebraic degree and high nonlinearity. Because changing one or a few bits in the output to a low degree Boolean function gives a function with high degree and does not fundamentally modify the robustness of the system against the approximation attacks with low degree functions, the nonlinearity profile and r-th order nonlinearity of a Boolean function was introduced to quantify the resistance of the system using this function. More explicitly, the r-th order nonlinearity of a Boolean function is the Hamming distances to the Reed-Muller code of order r. Computing the r-th order nonlinearity of a given function with algebraic degree strictly greater than r is a hard task for $r>1$. Instead of computing the r-th order nonlinearity, one hopes to obtain a tight lower bound of r-th order nonlinearity which can be useful to estimate the security of Boolean functions. However, it is also a quite difficult task to find a good lower bound, even for the 2^{nd} order nonlinearity. Carlet introduced a method to determine the lower bound of the r-th order nonlinearity of a function from the maximum value or the lower bounds of the $(r-1)$-th order nonlinearity of its first derivatives. With this method, the lower bounds for the 2^{nd} order nonlinearity of several classes of Boolean function with high nonlinearity were considered in literatures. However, the 2^{nd} order nonlinearity of Bent functions, which achieve the maximal 1^{st} order nonlinearity, was less studied. This paper investigated the 2^{nd} order nonlinearity of a class of Niho-type Bent function, and the lower bound for the 2^{nd} order nonlinearity of this class of Bent functions was showed to be better than the known results. Moreover, the technique used in this paper allows us determining the Walsh spectrum, instead of just nonlinearity, of the derivative functions and helps us obtain better lower bound. This technique may be valuable for further research to determine the exact 2^{nd} nonlinearity of some Boolean functions.

The work in this paper is supported by National Natural Science of China (Nos. 60970115, 60970116, 61003267, 91018008, 61003268).