bent 函数和半 bent 函数的二阶非线性度下界

李雪莲[①]　胡予濮[②]　高军涛[②]
[①](西安电子科技大学应用数学系　西安　710071)
[②](西安电子科技大学计算机网络与信息安全教育部重点实验室　西安　710071)

摘　要：该文研究了形如 $f(x,y)$ 的 $n+1$ 变元 bent 函数和半 bent 函数的二阶非线性度，其中 $x \in \mathrm{GF}(2^n)$，$y \in \mathrm{GF}(2)$。首先给出了 $f(x,y)$ 的 2^n-1 个导数非线性度的精确值；然后推导出了函数 $f(x,y)$ 的其余 2^n 个导数的非线性度紧下界。进而给出了 $f(x,y)$ 的二阶非线性度的紧下界。通过比较可知所得下界要优于现有的一般结论。结果表明 $f(x,y)$ 具有较高的二阶非线性度，可以抵抗二次函数逼近和仿射逼近攻击。

关键词：密码学；布尔函数；Walsh 变换；非线性度
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2010)10-2521-05
DOI: 10.3724/SP.J.1146.2010.00191

The Lower Bounds on the Second Order Nonlinearity of Bent Functions and Semi-bent Functions

Li Xue-lian[①]　Hu Yu-pu[②]　Gao Jun-tao[②]
[①](*Department of Applied Mathematics, Xidian University, Xi'an* 710071, *China*)
[②](*Key Laboratory of Computer networks & Information Security, Xidian University, Xi'an* 710071, *China*)

Abstract: This paper studies the lower bounds on the second order nonlinearity of bent functions and semi-bent functions $f(x,y)$ with $n+1$ variables, where $x \in \mathrm{GF}(2^n)$, $y \in \mathrm{GF}(2)$. Firstly, the values of the nonlinearity of the 2^n-1 derivatives of the Boolean function $f(x,y)$ are given. Then, the tight lower bounds on the other 2^n derivatives of $f(x,y)$ are deduced. Furthermore, the tight lower bounds on the second order nonlinearity of $f(x,y)$ are presented. The derived bounds are better than the existing general ones. The results show that these functions $f(x,y)$ have higher second order nonlinearity, and can resist the quardratic and affine approximation attacks.

Key words: Cryptography; Boolean functions; Walsh transforms; Nonlinearity

1　引言

布尔函数是许多分组密码和流密码的基本部件，布尔函数 f 的 r ($r \ge 1$)阶非线性度 $nl_r(f)$ 是衡量布尔函数抵抗相关攻击、代数攻击和线性攻击的重要指标。$nl_r(f)$ 是指 f 与所有次数至多为 r 的布尔函数间的最小距离。对于任意一个布尔函数 f，在理论上证明或者计算 r ($r \ge 1$)阶非线性度都是困难的。目前计算布尔函数的 r 阶非线性度最好的算法是由Dumer, Kabatiansky和Fourquet等人[1,2]给出的。但该算法仅适用于少量的函数。因此能够通过“理论证明”获得一类函数的 r 阶非线性度下界具有重要意义。

Carlet[3]给出了计算布尔函数 r 阶非线性度下界的递归算法，并且计算了 Welch 函数和乘法逆函数的二阶非线性度下界。当前已有结论[3–6]几乎都是计算三次布尔函数的二阶非线性度下界。本文研究了由文献[7]提出 bent 和半 bent 函数，证明了这些函数具有较高的二阶非线性度下界。这些函数与文献[3–6]所讨论的函数是完全不同的。文献[3–6]中仅给出了相应函数的导数 Walsh 谱的估计值，而这里给出了 $f(x,y)$ 的 2^n-1 个导数 Walsh 谱的精确值，从而计算出这些导数非线性度的精确值。

2　基础知识

设 n 是一个正整数，k 是 n 的一个因子且 $n=uk$。$\mathrm{GF}(2^n)$ 到 $\mathrm{GF}(2^k)$ 上的迹函数记为

$$T_k^n(x) = x + x^{2^k} + \cdots + x^{2^{k(u-1)}}, \quad x \in \mathrm{GF}(2^n) \quad (1)$$

当 $k=1$ 时，$T_k^n(x)$ 记为 $\mathrm{Tr}(x)$。

$\mathrm{GF}(2^n)$ 上的线性函数 $l_a(x)$ 可以表示为 $l_a(x)=\mathrm{Tr}(ax)$，其中 $a \in \mathrm{GF}(2^n)$。设 f 是 $\mathrm{GF}(2^n)$ 上的任意

2010-03-04 收到，2010-04-30 改回
国家 973 计划项目(2007CB311201)，国家自然科学基金项目(60833008，60803149)和广西信息与通讯技术重点实验室基金(20902)资助课题.
通信作者：李雪莲　xuelian202@163.com

布尔函数，f 的 Walsh 变换记为

$$W_f(\mu)=\sum_{x\in \mathrm{GF}(2^n)}(-1)^{f(x)+l\mu(x)}\ ,\ \ \mu\in \mathrm{GF}(2^n) \quad (2)$$

定义 f 的 Walsh 谱为集合 $\{W_f(\mu)\mid \mu\in \mathrm{GF}(2^n)\}$。$f$ 是均衡的当且仅当 $W_f(0)=0$。如果 f 的 Walsh 谱只有 3 个值 0，$\pm\lambda$，其中 $\lambda=2^m(m\geq n/2)$，则称 f 是 $\mathrm{GF}(2^n)$ 上 m 阶 Plateaued 函数[8]。当 n 是偶数，如果 $W_f(\mu)=\pm 2^{n/2}$，$\mu\in \mathrm{GF}(2^n)$，则称函数 f 是 Bent 函数。布尔函数 f 关于 $b\in \mathrm{GF}(2^n)$ 的导数：$D_bf=f(x)+f(x+b)$。

布尔函数的非线性度 $nl(f)$ 可以通过其 Walsh 谱来表示，具体如下：

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{\mu\in \mathrm{GF}(2^n)}\left|W_f(\mu)\right| \quad (3)$$

定义 1[9] 设 V 是 $\mathrm{GF}(2^k)$ 上的 n 维向量空间。如果一映射 $Q:V\mapsto \mathrm{GF}(2^k)$ 满足对于任意的 $c\in \mathrm{GF}(2^k)$ 和 $x\in V$ 有 $Q(cx)=c^2Q(x)$，且 $B(x,y)=Q(x+y)+Q(x)+Q(y)$ 是双线性的，则称映射 Q 为二次型。二次型 Q 的核 $K(Q)=\{x\in V:B(x,y)=0,\forall y\in V\}$ 是 V 的子空间。

引理 1[10] $\mathrm{GF}(2^n)$ 到 $\mathrm{GF}(2^k)$ 上的迹函数 $T_k^n(x)$ 具有如下性质:

(1) $\forall\alpha,\beta\in \mathrm{GF}(2^n),T_k^n(\alpha+\beta)=T_k^n(\alpha)+T_k^n(\beta)$;

(2) $\forall\alpha\in \mathrm{GF}(2^n),T_k^n(\alpha^{2^k})=T_k^n(\alpha)$;

(3) $\forall\alpha\in \mathrm{GF}(2^n),\forall c\in \mathrm{GF}(2^k),T_k^n(c\alpha)=cT_k^n(\alpha)$。

函数 f 是二次型，则 f 的 Walsh 谱仅依赖于它的核 $K(f)$ 的维数 k ($0\leq k\leq n-2$)。具体如表 1 所示。

表 1 f 的 Walsh 谱

$W_f(u)$	u 的个数
0	2^n-2^{n-k}
$2^{(n+k)/2}$	$2^{n-k-1}+(-1)^{f(0)}2^{n-k-2/2}$
$-2^{(n+k)/2}$	$2^{n-k-1}-(-1)^{f(0)}2^{n-k-2/2}$

定义 2[7] 任一满足 $f(0)=0$ 的 n 元布尔函数 $f(x)$，若 n 为奇数，则 f 是半 bent 函数当且仅当其 Walsh 谱如表 2 所示；若 n 为偶数，则 f 是半 bent 函数当且仅当其 Walsh 谱如表 3 所示。

表 2 奇数变元半 bent 函数 f 的 Walsh 谱

$W_f(u)$	u 的个数
0	2^n-2^{n-1}
$2^{(n+1)/2}$	$2^{n-2}+2^{(n-3)/2}$
$-2^{(n+1)/2}$	$2^{n-2}-2^{(n-3)/2}$

表 3 偶数变元半 bent 函数 f 的 Walsh 谱

$W_f(u)$	u 的个数
0	2^n-2^{n-2}
$2^{(n+2)/2}$	$2^{n-3}+2^{(n-4)/2}$
$-2^{(n+2)/2}$	$2^{n-3}-2^{(n-4)/2}$

在 $\mathrm{GF}(2^n)$ 上的二次布尔函数形如

$$f_a(x)=\sum_{i=1}^{\lfloor n/2\rfloor}\mathrm{Tr}(a_ix^{2^i+1}),\ \ a_i\in \mathrm{GF}(2^n) \quad (4)$$

由文献[9]可知，该类二次函数均为 $\mathrm{GF}(2^n)$ 到 $\mathrm{GF}(2)$ 上的二次型。关于二次函数的核有如下结论。

引理 2[7] 设 f 是二次布尔函数，则 f 的核 $K(f)$ 是使其导数 D_bf 为常数的那些 b 所构成的子空间。

可见，形如式(4)的二次函数 $f_a(x)$ 是 Bent 函数当且仅当 $k=0$；n 为奇数时，$f_a(x)$ 是半 Bent 函数当且仅当 $k=1$；n 为偶数时，$f_a(x)$ 是半 Bent 函数当且仅当 $k=2$。

3 bent 函数和半 bent 函数的二阶非线性度下界

引理 3[3] 设 f 为 n 变元布尔函数，$r\leq n$ 且 r 为正整数，则有

$$nl_r(f)\geq 2^{n-1}-(1/2)\sqrt{2^{2n}-2\sum_{a\in \mathrm{GF}(2^n)}nl_{r-1}(D_af)}$$

Carlet[3]指出引理 3 的下界是紧的。设

$$f_c(x)=\sum_{i=1}^{\lfloor (n-1)/2\rfloor}c_i\mathrm{Tr}(x^{2^i+1}),\ \ c_i\in \mathrm{GF}(2) \quad (5)$$

$c=(c_1,c_2,\cdots,c_l)$，$l=\lfloor (n-1)/2\rfloor$，$wt(c)$ 表示 c 的汉明重量。文献[7]给出了形如式(5)的函数为半 bent 函数的充要条件。进一步把两个适当选取的 n 元半 bent 函数级联后分别构造出了 $n+1$ 元的 bent 和半 bent 函数。

引理 4[7] 设 n 为奇数，$f_b(x)$ 和 $f_c(x)$ 为形如式(5)的两个不相等的 n 变元半 bent 函数，并且满足 $wt(b)$ 为偶数，$wt(c)$ 为奇数。那么 $\mathrm{GF}(2^n)\times \mathrm{GF}(2)$ 上的布尔函数 $f(x,y)=f_b(x)y+f_c(x)(y+1)$ 为三次 bent 函数。

令 $\mathrm{GF}(4)$ 的对偶为 $\mathrm{GF}(4)^{\perp}=\{u\in \mathrm{GF}(2^n)\mid \mathrm{Tr}(uv)=0,v\in \mathrm{GF}(4)\}$。当 n 为偶数时，$\mathrm{GF}(4)$ 及其对偶 $\mathrm{GF}(4)^{\perp}$ 都是 $\mathrm{GF}(2^n)$ 的子空间，这是显然的，因为 $\forall u_1,u_2\in \mathrm{GF}(4)^{\perp}$，$\mathrm{Tr}((u_1+u_2)v)=\mathrm{Tr}(u_1v)+\mathrm{Tr}(u_2v)=0$。

引理 5[7] 设 $n=2p$，$u\in \mathrm{GF}(2^n)$，$f_b(x)$ 和 $f_c(x)$ 为形如式(5)的两个不相等的半 bent 函数。

$\mathrm{GF}(2^n)\times\mathrm{GF}(2)$ 上的函数为 $f(x,y)=(f_b(x)+l_u(x))y+f_c(x)(y+1)$。集合 $I_e(b)=\{i\mid b_i\neq 0$ 且 i 是偶数$\}$，$I_e(c)=\{i\mid c_i\neq 0$ 且 i 是偶数$\}$。则

(1)若 p 为偶数或者 $\#I_e(b)$ 和 $\#I_e(c)$ 均为偶数，则 $\forall u\in\mathrm{GF}(4)^{\perp}$，$f(x,y)$ 为三次半 bent 函数。

(2)若 p 为奇数，$\#I_e(b)$ 为奇数，$\#I_e(c)$ 为偶数且 $u=0$，则 $f(x,y)$ 为三次半 bent 函数。

3.1 Bent 函数 $f(x,y)$的二阶非线性度下界

因为 $f(x,y)$ 是双变量函数，所以其导数为 $D_{(\alpha,\beta)}f(x,y)=f(x+\alpha,y+\beta)+f(x,y)$。又由于函数的 Walsh 谱具有仿射不变性，因此计算 $D_{(\alpha,\beta)}f(x,y)$ 的 Walsh 谱等于计算函数 $D_{(\alpha,\beta)}f(x+\alpha,y)$ 的 Walsh 谱。

函数 $f(x+\alpha,y)$ 关于 $\alpha\in\mathrm{GF}(2^n)$，$\beta\in\mathrm{GF}(2)$ 的导数为

$$\begin{aligned}D_{(\alpha,\beta)}f(x+\alpha,y)&=f(x+\alpha,y)+f(x,y+\beta)=yD_\alpha f_b(x)\\&\quad+(y+1)D_\alpha f_c(x)+\beta(f_b(x)+f_c(x))\end{aligned}\tag{6}$$

双变量函数 $D_{(\alpha,\beta)}f(x+\alpha,y)$ 的 Walsh 变换

$$\begin{aligned}W_{D_{(\alpha,\beta)}f}(\mu,\nu)&=\sum_{\substack{x\in\mathrm{GF}(2^n)\\y\in\mathrm{GF}(2)}}(-1)^{D_{(\alpha,\beta)}f+\mathrm{Tr}(\mu x)+\nu y}\\&=\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=0}}(-1)^{D_\alpha f_c+\beta(f_b+f_c)+\mathrm{Tr}(\mu x)}\\&\quad+\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=1}}(-1)^{D_\alpha f_b+\beta(f_b+f_c)+\mathrm{Tr}(\mu x)+\nu}\end{aligned}\tag{7}$$

下面分 3 种情形进行讨论。

情形 1　$\alpha\in\mathrm{GF}(2^n)^*$，$\beta=0$。$D_{(\alpha,0)}f(x+\alpha,y)=yD_\alpha f_b(x)+(y+1)D_\alpha f_c(x)$。

由引理 1 可知，

$$\left.\begin{aligned}D_\alpha f_b(x)&=\mathrm{Tr}\left(x\sum_{i=1}^{\lfloor(n-1)/2\rfloor}b_i(\alpha^{2^{n-i}}+\alpha^{2^i})\right)+f_b(\alpha)\\D_\alpha f_c(x)&=\mathrm{Tr}\left(x\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i(\alpha^{2^{n-i}}+\alpha^{2^i})\right)+f_c(\alpha)\end{aligned}\right\}\tag{8}$$

由于 $f_b(x)$ 和 $f_c(x)$ 为奇变元的半 bent 函数，其核的维数为 1，所以 $D_\alpha f_b(x)$ 和 $D_\alpha f_c(x)$ 为常数的非零 α 的个数是 1。显然 $\alpha=1$（单位元）就是使 $D_\alpha f_b(x)$ 和 $D_\alpha f_c(x)$ 为常数的唯一点。

$$\begin{aligned}W_{D_{(\alpha,0)}f}(\mu,\nu)&=\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=0}}(-1)^{D_\alpha f_c+\mathrm{Tr}(\mu x)}\\&\quad+\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=1}}(-1)^{D_\alpha f_b+\mathrm{Tr}(\mu x)+\nu}\\&=W_{D_\alpha f_c}(\mu)+W_{D_\alpha f_c}(\mu')\end{aligned}\tag{9}$$

$$\left.\begin{aligned}W_{D_\alpha f_b}(\mu)&=\begin{cases}2^n, & D_\alpha f_c=\mathrm{Tr}(\mu x)\\-2^n, & D_\alpha f_c=\mathrm{Tr}(\mu x)+1\\0, & \text{其它}\end{cases}\\W_{D_\alpha f_c}(\mu')&=\begin{cases}2^n, & D_\alpha f_c=\mathrm{Tr}(\mu x)+\nu\\-2^n, & D_\alpha f_c=\mathrm{Tr}(\mu x)+\nu+1\\0, & \text{其它}\end{cases}\end{aligned}\right\}\tag{10}$$

当 $\alpha\neq 1$ 时，$D_{(\alpha,0)}f(x,y)$ 为二次函数，因此 $D_{(\alpha,0)}f(x,y)$ 一定为三谱值的 Plateaued 函数，并且其 Walsh 谱为$\{0,\pm 2^n\}$。这是因为 $D_{(\alpha,\beta)}f(x,y)$ 的 Walsh 变换不可能等于 2^{n+1} 或 -2^{n+1}，否则不满足 Parseval 恒等式：对任意 n 元布尔函数 f 有

$$\sum_{\mu\in\mathrm{GF}(2^n)}W_f(\mu)^2=2^{2n}$$

因此，$nl(D_{(\alpha,0)}f)=2^n-2^{n-1}$。当 $\alpha=1$ 时，$D_{(1,0)}f(x,y)=yf_b(1)+(y+1)f_c(1)=y(f_b(1)+f_c(1))+f_c(1)$ 为一次函数或常数，$nl(D_{(1,0)}f(x,y))=0$。

情形 2　$\alpha\in\mathrm{GF}(2^n)^*$，$\beta=1$。$D_{(\alpha,1)}f(x+\alpha,y)=yD_\alpha f_b(x)+(y+1)D_\alpha f_c(x)+f_b(x)+f_c(x)$。

$$\begin{aligned}W_{D_{(\alpha,1)}f}(\mu,\nu)&=\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=0}}(-1)^{D_\alpha f_c+f_b+f_c+\mathrm{Tr}(\mu x)}\\&\quad+\sum_{\substack{x\in\mathrm{GF}(2^n)\\y=1}}(-1)^{D_\alpha f_b+f_b+f_c+\mathrm{Tr}(\mu x)+\nu}\\&=W_{f_b+f_c}(\mu')+W_{f_b+f_c}(\mu'')\end{aligned}\tag{11}$$

而 $f_b(x)+f_c(x)$ 仍为形如式(5)的二次函数。

下面利用迹函数理论和二次型的性质研究形如式(5)的二次函数 $h(x)=f_c(x)$ 核的维数，及其 Walsh 谱。

定理 1　设 $K(h)$ 是二次函数 $h(x)$ 的核，$P(x)$ 和 $L(x)$ 是 $\mathrm{GF}(2)$ 上的多项式，且

$$\left.\begin{aligned}P(x)&=\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i(x^{2^{i-s}}+x^{2^{n-i-s}})\\L(x)&=\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i(x^{2^{i+t}}+x^{2^{t-i}})\end{aligned}\right\}\tag{12}$$

其中 $s=\min\{i\mid c_i\neq 0\}$，$t=\max\{i\mid c_i\neq 0\}$。则 $K(h)$ 是由 $P(x)$ 和 $L(x)$ 的根所构成的子空间。

证明　$\forall\alpha\in\mathrm{GF}(2^n)^*$，有

$$\begin{aligned}D_\alpha h(x)&=\mathrm{Tr}\left(\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i(\alpha x^{2^i}+\alpha^{2^i}x)\right)\\&\quad+\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i\mathrm{Tr}(\alpha^{2^i+1})\\&=\mathrm{Tr}\left(x\sum_{i=1}^{\lfloor(n-1)/2\rfloor}c_i(\alpha^{2^i}+\alpha^{2^{n-i}})\right)+h(\alpha)\end{aligned}\tag{13}$$

令

$$P(x)=\left(\sum_{i=1}^{\lfloor (n-1)/2\rfloor} c_i(x^{2^i}+x^{2^{n-i}})\right)^{2^{-s}}$$
$$=\sum_{i=1}^{\lfloor (n-1)/2\rfloor} c_i(x^{2^{i-s}}+x^{2^{n-i-s}})$$
$$L(x)=\left(\sum_{i=1}^{\lfloor (n-1)/2\rfloor} c_i(x^{2^i}+x^{2^{n-i}})\right)^{2^t}$$
$$=\sum_{i=1}^{\lfloor (n-1)/2\rfloor} c_i(x^{2^{i+t}}+x^{2^{t-i}})$$

其中 $s=\min\{i\mid c_i\neq 0\}$，$t=\max\{i\mid c_i\neq 0\}$。如果 α 是 $\alpha\in \mathrm{GF}(2)$ 上的多项式 $q(x)$ 的根，则显然 α 的共轭元也是 $q(x)$ 的根。自然地，$q(x)$ 和 $q(x)^{2^k}$ 的根相同。而当 $P(\alpha)=L(\alpha)=0$ 时，$D_\alpha h(x)$ 为常数 $h(\alpha)$，由引理 2 可知 $K(h)=\{x\in \mathrm{GF}(2^n)\mid P(x)=0\text{或}L(x)=0\}$。证毕

定义 3[10] 设 q 为一个素数或素数的幂次，称系数在 $\mathrm{GF}(q)$ 的扩域 $\mathrm{GF}(q^n)$ 上的多项式 $\sum_{i=0}^{n-1}a_i x^{q^i}$ 为 $\mathrm{GF}(q^n)$ 上的 q-多项式。

命题 1[9] 设 V 是 $\mathrm{GF}(2^k)$ 上的向量空间，Q 为 V 到 $\mathrm{GF}(2^k)$ 上的二次型，那么 V 和 Q 的核的维数同奇偶。

一个 q-多项式的核与像集都是 $\mathrm{GF}(q^n)$ 上的子空间。特别地，它的核与像集中元素的个数为 q^k（k 为某个正整数）。当 $q=2$ 时，多项式 $P(x)$ 和 $L(x)$ 是 2-多项式。多项式 $P(x)$ 的次数是 2^{n-2s}，$L(x)$ 的次数是 2^{2t}，因此 $K(h)$ 中元素的个数至多为 $\min(2^{n-2s},2^{2t})$。当 n 为偶数时 $K(h)$ 的维数 $k\le\min(n-2s,2t)$ 且为偶数；当 n 为奇数时 $K(h)$ 的维数 $k\le\min(n-2s,2t)$ 且为奇数。由表 1 可得下面的定理 2。

定理 2 函数 $h(x)$ 的 Walsh 谱为 $\{0,\pm 2^{(n+k)/2}\}$。当 n 为偶数时，$k\le\min(n-2s,2t)$ 且为偶数；当 n 为奇数时，$k\le\min(n-2s,2t)$ 且为奇数。

由定理 2 可知，n 为奇数时，$W_{f_b+f_c}(\mu')$ 和 $W_{f_b+f_c}(\mu'')=0$ 或 $\pm 2^{(n+k)/2}$，所以 $D_{(\alpha,1)}f$ 的 Walsh 谱为 $\{0,\pm 2^{(n+k)/2}\}$ 或 $\{0,\pm 2^{(n+k+2)/2}\}$，$nl(D_{(\alpha,1)}f)\ge 2^n-2^{(n+k)/2}$。

情形 3 $\alpha=0$，$\beta=1$。$D_{(0,1)}f(x+\alpha,y)=f_b(x)+f_c(x)$。

$$W_{D_{(0,1)}f}(\mu,\nu)=\sum_{\substack{x\in \mathrm{GF}(2^n)\\ y=0}}(-1)^{f_b+f_c+\mathrm{Tr}(\mu x)}+\sum_{\substack{x\in \mathrm{GF}(2^n)\\ y=1}}(-1)^{f_b+f_c+\mathrm{Tr}(\mu x)+\nu}$$
$$=W_{f_b+f_c}(\mu)+W_{f_b+f_c}(\mu') \qquad (14)$$

而 $f_b(x)+f_c(x)$ 仍为形如式(5)的二次函数。同理可证，$D_{(0,1)}f$ 的 Walsh 谱为 $\{0,\pm 2^{(n+k)/2}\}$ 或 $\{0,\pm 2^{(n+k+2)/2}\}$，$nl(D_{(\alpha,1)}f)\ge 2^n-2^{(n+k)/2}$，$k\le\min(n-2s,2t)$ 且为奇数。

特别地，当 $f_b(x)+f_c(x)$ 仍为奇数变元的半 bent 函数时，$D_{(\alpha,1)}f$ 的 Walsh 谱为 $\{0,\pm 2^{(n+1)/2}\}$ 或 $\{0,\pm 2^{(n+3)/2}\}$，$nl(D_{(\alpha,1)}f)\ge 2^n-2^{(n+1)/2}$。

由引理 3 可以得到下面的定理 3。

定理 3 由引理 4 所构造的 $n+1$ 变元 bent 函数 $f(x,y)$ 的二阶非线性度满足

$$nl_2(f(x,y))\ge 2^n-\frac{1}{2}\sqrt{2^{2n}+2^{(3n+k+2)/2}+2^{n+1}} \qquad (15)$$

其中 k 为奇数，且 $k\le\min(n-2s,2t)$，$s=\min\{i\mid b_i+c_i\neq 0\}$，$t=\max\{i\mid b_i+c_i\neq 0\}$。

推论 1 当 $f_b(x)+f_c(x)$ 为半 bent 函数时，由引理 4 所构造的 $n+1$ 变元 bent 函数 $f(x,y)$ 的二阶非线性度满足

$$nl_2(f(x,y))\ge 2^n-\frac{1}{2}\sqrt{2^{2n}+2^{(3n+3)/2}+2^{n+1}}$$
$$\approx 2^{n-1} \qquad (16)$$

例 1 由文献[7]给出的形如式(5)的函数为半 bent 函数的充要条件可知：$f_b(x)=\mathrm{Tr}(x^3+x^5)$，$f_c(x)=\mathrm{Tr}(x^5)$ 均为 $\mathrm{GF}(2^{17})$ 上满足引理 4 条件的 17 变元半 bent 函数，因此 18 变元函数 $f(x,y)=f_b\,||\,f_c$ 为三次 bent 函数。而 $f_b(x)+f_c(x)=\mathrm{Tr}(x^3)$ 仍为 17 变元的半 bent 函数，由推论 1 可知 $nl_2(f(x,y))\ge 65280$。

3.2 半 bent 函数 $f(x,y)$ 的二阶非线性度下界

与 3.1 节同理可以证出引理 5 中的三次半 bent 函数的二阶非线性度下界。

定理 4 由引理 5 所构造的 $n+1$ 变元半 bent 函数 $f(x,y)$ 的二阶非线性度满足

$$nl_2(f(x,y))\ge 2^n-\frac{1}{2}\sqrt{2^{2n}+2^{(3n+k+2)/2}+2^{n+1}} \qquad (17)$$

其中 k 为偶数，且 $k\le\min(n-2s,2t)$，$s=\min\{i\mid b_i+c_i\neq 0\}$，$t=\max\{i\mid b_i+c_i\neq 0\}$。

推论 2 当 $f_b(x)+f_c(x)$ 为半 bent 函数时，由引理 5 所构造的 $n+1$ 变元半 bent 函数 $f(x,y)$ 的二阶非线性度满足 $nl_2(f(x,y))\ge 2^n-(1/2)\sqrt{2^{2n}+2^{(3n+4)/2}+2^{n+1}}\approx 2^{n-1}$。

Carlet[3]指出，一般地，$n+1$ 变元三次布尔函数的二阶非线性度下界为 2^{n-2}，而不具有仿射函数导数的 $n+1$ 变元三次布尔函数二阶非线性度下界为 $2^n-2^{n-0.5}$。这里 $f(x,y)$ 具有仿射函数的导数，本文的界不仅远远优于前者，而且也要优于后者。

4 结论

本文给出了 Charpin 等构造的 $n+1$ 元 bent 函

数和半 bent 函数 $f(x,y)$ 二阶非线性度的紧下界。主要的研究方法是利用迹函数和二次型的性质，求出 $f(x,y)$ 导数 Walsh 谱的精确值及其紧上界。从而确定出这些导函数的非线性度及其紧下界。进而利用引理 3 给出了函数 $f(x,y)$ 二阶非线性度的紧下界。通过比较可知本文的界要优于已有的一般结论。因此证明了当 n 较大时函数 $f(x,y)$ 可以有效抵抗二次逼近和仿射逼近攻击。Charpin 等[7]指出利用递归级联的方法可以构造出更高次的 bent 和半 bent 函数。因此进一步的工作将集中于求解更高次 bent 和半 bent 函数的二阶非线性度下界。

参 考 文 献

[1] Fourquet R and Tavernier C. List decoding of second order Reed–Muller and its covering radius implications[C]. Proceedings of the WCC 2007, Versailles, France, 2007: 147–156.

[2] Dumer I, Kabatiansky G, and Tavernier C. List decoding of Reed–Muller codes up to the Johnson bound with almost linear complexity[C]. Proceedings of the IEEE International Symposium on Information Theory, Seattle, WA, 2006: 138–142.

[3] Carlet C. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications[J]. *IEEE Transactions on Information Theory*, 2008, 54(3): 1262–1272.

[4] Sun G and Wu C. The lower bounds on the second order nonlinearity of three classes of Boolean functions wih high nonlinearity[J]. *Information Sciences*, 2009, 179(3): 267–278.

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

[6] Gode R and Gangopadhyay S. On second order nonlinearities of cubic monomial Boolean functions[DB/OL]. [2009-10-21]. http://eprint.iacr.org /2009/502.pdf.

[7] Charpin P, Pasalic E, and Tavernier C. On bent and semi-bent quadratic Boolean functions[J]. *IEEE Transactions on Information Theory,* 2005, 51(12): 4286–4298.

[8] Zheng Y and Zhang X M. On plateaued functions[J]. *IEEE Transactions on Information Theory*, 2001, 47(3): 1215–1223.

[9] Canteaut A, Charpin P, and Kyureghyan G M. A new class of monomial bent functions [J]. *Finite Fields and Their Applications*, 2008, 14(1): 221–241.

[10] Lidl R and Niederreiter H. Finite Fields [M]. Cambridge, U.K: Combridge Univ. Press, 1983: 54–57, 107.

李雪莲：女，1979 年生，讲师，博士，研究方向为密码函数、流密码.

胡予濮：男，1955 年生，教授，博士生导师，研究方向为信息安全和网络安全.

高军涛：男，1979年生，讲师，博士，研究方向为流密码、密码函数以及伪随机序列方面的研究.