一类多输出半 Bent函数的构造及其密码学性质

刘志高[1,2], 张福泰[1], 徐 倩[1]

(1.南京师范大学 数学与计算机科学学院, 江苏 南京 210097;
2.安徽工业大学 职业技术学院, 安徽 马鞍山 243011)

[摘要] 给出了多输出半 Bent函数的一种构造方法.该方法通过级联两个低阶多输出 Bent函数得到高阶多输出半 Bent函数.由于在多输出 Bent函数的构造方面,目前已有许多较好的结果,因此新方法是一个非常有效的方法,能构造出大量的多输出半 Bent函数.还进一步讨论了这类函数的平衡性、非线性性、稳定性及扩散性等密码学性质.这些性质显示,多输出半 Bent函数是一类密码学性质良好的奇数元多输出函数,除了可应用于多输出前馈网,它还可用作分组密码体制的非线性组合器.

[关键词] Bent函数,多输出 Bent函数,多输出半 Bent函数,Walsh循环谱
[中图分类号] O236.2;O157.4 [文献标识码] A [文章编号] 1672-1292(2006)01-0038-05

The Construction of a Class of Multi-output Semi-bent Functions and Their Cryptographic Properties

LIU Zhigao[1,2], ZHANG Futai[1], XU Qian[1]

(1. School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, China;
2. College of Vocational Technology, Anhui University of Technology, Ma'anshan 243011, China)

Abstract A method to construct multi-output semi-bent functions is presented. In the method, a higher order multi-output semi-bent function is constructed by concatenating two lower order multi-output bent functions. Since many good results on the construction of multi-output bent functions have been given, the new method is very effective and many multi-output semi-bent functions can be constructed by it. Furthermore, some cryptographic properties of this kind of functions such as balance, nonlinearity, stability and propagation characters etc. are discussed. The discussion shows that the multi-output semi-bent function is a class of multi-output functions with odd variables that hold good cryptographic properties. Besides applications in multi-output feedforward networks, multi-output semi-bent functions can also be used as nonlinear combiner in block ciphers.

Key words Bent function, multi-output bent function, multi-output semi-bent function, Walsh cyclic-spectrum

0 引言

Bent函数是由 Rothaus于 1976年提出的一类特殊的布尔函数[1].它在展频通信、编码理论、密码学等领域中有着广泛的应用.Bent函数的主要优点是它具有最高的非线性度和差分分布的均匀性,用于非线性组合器可以很好的抗击相关攻击、最佳仿射逼近攻击和差分分析攻击.但从密码学角度看, Bent函数也存在着一些缺陷.例如,它不是平衡的,其代数次数不超过 $n/2$,限制 n为偶数等.这就要求对 Bent函数进行改进,因此构造非线性度高、非线性次数大的平衡布尔函数及奇数元布尔函数等问题就成了密码学中非常重要的研究课题.半 Bent函数[2]在某种意义上弥补了 Bent函数的一些不足,同时利用半 Bent函数的结

收稿日期: 2005-09-27.
基金项目: 江苏省高校自然科学研究计划重点资助项目(03KJA520066);教育部网络与信息安全重点实验室(西安电子科技大学)开放课题资助项目.
作者简介: 刘志高(1975-),硕士研究生,讲师,主要从事密码学与网络安全的学习与研究. E-mail: zhigaoliu@126.com
通讯联系人: 张福泰(1965-),博士,教授,主要从事密码学与信息安全的教学与研究. E-mail: zhangfutai@njnu.edu.cn

果又可加深对 Bent函数的研究. 可见研究半 Bent函数是十分有意义的.

多输出布尔函数在分组密码的设计中扮演着重要的角色, 如分组密码的核心部件 S-盒的安全性设计, 常常采用具有多个良好密码学性质的多输出布尔函数, 所以如何构造具有多个良好密码学性质的多输出布尔函数一直是重要的研究课题. 多输出 Bent函数[3]就是一类具有一些良好密码性质的多输出布尔函数, 它的每个分量以及各分量的所有非零线性组合都是 Bent函数. 但多输出 Bent函数不可避免地带有 Bent函数所固有的一些缺陷, 如, 非平衡的, 其非线性次数不超过变元数目 n的一半, 限制 n为偶数等. 多输出半 Bent函数[4]可以弥补多输出 Bent函数的一些不足.

本文给出了多输出半 Bent函数的一种构造方法. 同时, 还讨论了这类函数的平衡性、非线性性、稳定性及扩散性等密码学性质. 我们发现多输出半 Bent函数是一类密码学性质良好的奇数元多输出函数, 可广泛地应用于多输出前馈网, 分组密码的 S-盒的设计等领域.

1 预备知识

定义 1 设m, n均为正整数, $m \leqslant n$, $f_i: F_2^n \to F_2$为布尔函数 ($i = 1, 2, \cdots, m$), 则称$f(x) = (f_1(x), \cdots, f_m(x))$为 $F_2^n \to F_2^m$ 的 n元m 输出函数.

定义 2[3] 设$f(x)$是n元m输出函数, 称 $S_{(f)}(u, v) = 2^{-n}\sum_{x\in F_2^n}(-1)^{u\cdot f(x)+v\cdot x}$为$f(x)$的广义一阶 Walsh 循环谱. 其中 $u \in F_2^m$, $v \in F_2^n$.

易知, 对于固定的 u, $S_{(f)}(u, v)$就是布尔函数 $u\cdot f(x)$的一阶 Walsh循环谱, 即 $S_{(f)}(u, v) = S_{(u\cdot f)}(v)$.

定义 3[3] 设 $f(x)$ 是 n元m 输出函数, 若对一切 $0 \neq u \in F_2^m$, $v \in F_2^n$均有 $|S_{(f)}(u, v)| = 2^{-\frac{n}{2}}$, 则称 $f(x)$ 为多输出 Bent函数.

由定义 3易得如下引理:

引理 1 n元m 输出函数$f(x)$是多输出 Bent函数的必要条件是 n为偶数.

引理 2 设$f(x)$是 n元m输出函数, 则$f(x)$是多输出 Bent函数的充要条件是 $\forall\, 0 \neq u \in F_2^m$, $u\cdot f(x)$是 n元 Bent函数.

定义 4[2,5] 一个 n元布尔函数$f(x)$称为半 Bent函数, 如果对任意的 $\omega \in F_2^n$, 均有 $|S_{(f)}(\omega)| = 0$或 $2^{-\frac{n-1}{2}}$.

定义 5[4] 设$f(x)$是n元m输出函数, 若对一切固定的 u, $0 \neq u \in F_2^m$, $\forall\, v \in F_2^n$, 均有 $|S_{(f)}(u, v)| = 0$或 $2^{-\frac{n-1}{2}}$, 则称 $f(x)$ 为多输出半 Bent函数.

由定义 5易得如下结论:

结论 1 n元m 输出函数$f(x)$是多输出半 Bent函数的必要条件是 n为奇数.

结论 2 设$f(x)$是 n元m 输出函数, 则 $f(x)$ 是多输出半 Bent函数的充要条件是 $\forall\, 0 \neq u \in F_2^m$, $u\cdot f(x)$是 n元半 Bent函数.

定义 6[3] 设有多输出函数$f(x) = (f_1(x), f_2(x), \cdots, f_m(x))$: $\{0, 1\}^n \to \{0, 1\}^m$, $m \leqslant n$. 对给定的 k, $1 \leqslant k \leqslant m$, 称 $N_f^{(k)} = \min_{l\in L,\ u\in F_2^m,\ 1\leqslant W_H(u)\leqslant k} d_H(u\cdot f, l)$为 $f(x)$ 的 k级非线性度. 其中 L是所有 n元仿射布尔函数组成的类. 称 $N_f = \min_{1\leqslant k\leqslant m} N_f^{(k)}$ 为 $f(x)$ 的非线性度.

显然有 $N_f^{(1)} \geqslant N_f^{(2)} \geqslant \cdots \geqslant N_f^{(m)}$, 所以 $N_f = N_f^{(m)}$. 由定义 6知, n元m 输出函数$f(x)$的 k级非线性度就是所有布尔函数 $u\cdot f(x)$ 的非线性度的最小值. 其中 $u \in F_2^m$ 且 $1 \leqslant W_H(u) \leqslant k$ 亦即 $N_f^{(k)} = \min_{u\in F_2^m,\ 1\leqslant W_H(u)\leqslant k} N_{uf}$.

n元多输出函数的非线性度上界是 $2^{n-1} - 2^{\frac{n}{2}-1}$, 且这个上界是可达的. 如 n元多输出 Bent函数的非线性度就是 $2^{n-1} - 2^{\frac{n}{2}-1}$.

定义 7[3] 设$f(x)$是 n元m 输出函数, 若对任意的 $a \in F_2^m$, $P(f = a) = \frac{1}{2^m}$, 即 $\left|\left\{x \in F_2^n \,\middle|\, f(x) = a\right\}\right| = 2^{n-m}$, 则称$f$是平衡的或正交的.

引理 **3**[3]　设 $f(x)$ 是 n元 m 输出函数, 则 $f(x)$ 是正交的充要条件是对任意的 $0 \neq u \in F_2^m$, $u \cdot f(x)$ 是一个平衡布尔函数.

定义 **8**[6]　设 $f(x)$ 是 n元布尔函数, 如果 $VS(f) = \sum_{\omega \in F_2^n} [S_{(f)}^2(\omega) - 2^{-n}]^2 = 0$, 则称 $f(x)$ 是稳定的.

定义 **9**[7]　如果对任意固定的 $a \in F_2^n$, $1 \leqslant W_H(a) \leqslant k$, $f(x+a) + f(x)$ 是平衡函数, 则称 $f(x)$ 满足 k次扩散准则.

2　一类多输出半 *Bent*函数的构造

设 $n = 2k$, 记 $X_1 = (x_1, x_2, \cdots, x_n)$, $X = (X_1, x_{n+1})$, 设 $g_1(X_1)$和 $g_2(X_1)$均是 n元 m 输出布尔函数, 令

$$f(X) = g_1(X_1)(x_n + 1) + g_2(X_1)x_n \tag{1}$$

定理 **1**　若 $g_1(X_1)$和 $g_2(X_1)$均是 n元 m 输出 Bent函数, 则由(1)式构造的 $f(X)$ 是 $n+1$元 m 输出半 Bent函数.

证明　对一切固定的 u, $0 \neq u \in F_2^m$, $uf(X) = (1 + x_{n+1})ug_1(X_1) + x_{n+1}ug_2(X_1)$, 所以,

$$S_{(uf)}(\omega, 0) = \frac{1}{2^{n+1}} \sum_{X \in F_2^{n+1}} (-1)^{uf(X) + (\omega, 0) \cdot X} = \frac{1}{2^{n+1}} \sum_{X \in F_2^{n+1}} (-1)^{(1+x_{n+1})ug_1(X_1) + x_{n+1}ug_2(X_1) + \omega \cdot X_1} =$$

$$\frac{1}{2}\left[\frac{1}{2^n} \sum_{X_1 \in F_2^n} (-1)^{ug_1(X_1) + \omega \cdot X_1} + \frac{1}{2^n} \sum_{X_1 \in F_2^n} (-1)^{ug_2(X_1) + \omega \cdot X_1}\right] =$$

$$\frac{S_{(ug_1)}(\omega) + S_{(ug_2)}(\omega)}{2}.$$

类似可得, $S_{(uf)}(\omega, 1) = \dfrac{S_{(ug_1)}(\omega) - S_{(ug_2)}(\omega)}{2}$, 其中 $\omega \in F_2^n$.

又因为 $g_1(X_1)$和 $g_2(X_1)$均是 n元 m 输出 Bent函数, 所以, 由引理 2可得, $ug_1(X_1)$和 $ug_2(X_1)$均是 n元 Bent函数, 于是有:

$$|S_{(uf)}(\omega, 0)| = \left|\frac{S_{(ug_1)}(\omega) + S_{(ug_2)}(\omega)}{2}\right| = \begin{cases} 2^{-\frac{n}{2}}, & S_{(ug_1)}(\omega) = S_{(ug_2)}(\omega) \\ 0 & S_{(ug_1)}(\omega) \neq S_{(ug_2)}(\omega) \end{cases} \omega \in F_2^n$$

$$|S_{(uf)}(\omega, 1)| = \left|\frac{S_{(ug_1)}(\omega) - S_{(ug_2)}(\omega)}{2}\right| = \begin{cases} 0 & S_{(ug_1)}(\omega) = S_{(ug_2)}(\omega) \\ 2^{-\frac{n}{2}}. & S_{(ug_1)}(\omega) \neq S_{(ug_2)}(\omega) \end{cases} \omega \in F_2^n$$

因此, $\forall v \in F_2^{n+1}$, $|S_{(uf)}(v)| = 0$或 $2^{-\frac{n}{2}}$, 且取值为零的个数与取值为 $2^{-\frac{n}{2}}$ 的个数相等, 均为 2^n, 即 $|\{v \in F_2^{n+1} \mid |S_{(uf)}(v)| = 0\}| = |\{v \in F_2^{n+1} \mid |S_{(uf)}(v)| = 2^{-\frac{n}{2}}\}| = 2^n$. 所以, $u \cdot f(X)$ 是 $n+1$元半 Bent函数. 再由结论 2知, $f(X)$ 是 $n+1$元 m 输出半 Bent函数.

由于目前对多输出 Bent函数已作了许多深入的研究, 已经有了一些较好的结果[3, 8~10], 所以, 本文所给出的多输出半 Bent函数的构造方法具有广泛的适用性.

3　多输出半 *Bent*函数的密码学性质

3.1　平衡性

一般地, 多输出半 Bent函数不一定是平衡函数. 但对于由(1)式构造的多输出半 Bent函数 $f(X)$ 而言, 下面的定理 2给出了 $f(X)$ 为平衡函数的一个充分条件.

定理 **2**　若 $\forall 0 \neq u \in F_2^m$, 有 $S_{(ug_1)}(0) = -S_{(ug_2)}(0)$, 则由(1)式构造的 $f(X)$ 是平衡函数.

证明　由定理 1的证明知,

$|S_{(uf)}(\omega, 0)| = \left|\dfrac{S_{(ug_1)}(\omega) + S_{(ug_2)}(\omega)}{2}\right|$, $\omega \in F_2^n$. 从而, $\forall 0 \neq u \in F_2^m$, 有

$$|S_{(uf)}(0,0)| = \left|\frac{S_{(ug_1)}(0)+S_{(ug_2)}(0)}{2}\right| = 0$$

所以, 对任意的 $0 \neq u \in F_2^m$, $u \cdot f(x)$ 是一个平衡布尔函数. 由引理 3知, $f(X)$ 是平衡函数.

3.2 非线性度

定理 **3** $n+1$元多输出半 Bent函数 $f(X)$ 的非线性度为 $N_f = 2^n - 2^{\frac{n}{2}}$.

证明 由定义 5知, 对一切固定的 u, $0 \neq u \in F_2^m$, $\forall v \in F_2^{n+1}$, 均有 $|S_{(f)}(u,v)| = 0$或 $2^{-\frac{n}{2}}$, 亦即 $S_{(u,f)}(v) = 0$或 $2^{-\frac{n}{2}}$. 因此, $N_{uf} = 2^n(1 - \max\limits_{v \in F_2^{n+1}} |S_{uf}(v)|) = 2^n\left(1 - 2^{-\frac{n}{2}}\right) = 2^n - 2^{\frac{n}{2}}$. 所以, 由定义 6可得,

$$N_f = N_f^{(m)} = \min_{u \in F_2^m,\ 1 \leqslant W_H(u) \leqslant m} N_{uf} = 2^n - 2^{\frac{n}{2}}.$$

Piepryzk J与 Finkelstein G在文[11]中证明了 $n+1$元平衡函数所具有的最高的非线性度是 $2^n - 2^{\frac{n}{2}}$. 这说明多输出半 Bent函数具有很强的抵抗最佳仿射出逼近攻击 (BAA) 的能力.

3.3 稳定性

设 $f(X)$ 是 $n+1$元多输出半 Bent函数, 则对一切固定的 u, $0 \neq u \in F_2^m$, $\forall v \in F_2^{n+1}$, $|S_{(u,f)}(v)| = 0$ 或 $2^{-\frac{n}{2}}$. 又由能量守恒定理[3]可知, $\sum\limits_{v \in F_2^{n+1}} S_{(uf)}^2(v) = 1$, 所以有,

$$|\{v \in F_2^{n+1} \mid |S_{(u,f)}(v)| = 0\}| = |\{v \in F_2^{n+1} \mid |S_{(u,f)}(v)| = 2^{-\frac{n}{2}}\}| = 2^n.$$

于是, 对一切固定的 u, $0 \neq u \in F_2^m$, 有

$$VS(uf) = \sum_{\omega \in F_2^{n+1}} [S_{(uf)}^2(\omega) - 2^{-(n+1)}]^2 = (2^{-n} - 2^{-(n+1)})^2 \cdot 2^n + (2^{-(n+1)})^2 \cdot 2^n = 2^{-(n+1)} \to 0 \ (n \to +\infty).$$

所以, $f(X)$ 的任意非零线性组合都是近似稳定的. 故多输出半 Bent函数是近似稳定的.

3.4 扩散性

定理 **4** 对一切 $s^* = (s,0)$, $s \in F_2^n$且 $s \neq 0$, 由 (1) 式构造的 $n+1$元多输出半 Bent函数 $f(X)$ 满足 n次扩散准则.

证明 对一切固定的 u, $0 \neq u \in F_2^m$, $uf(X) = (1+x_{n+1})ug_1(X_1) + x_{n+1}ug_2(X_1)$, 且 $u \cdot g_1(X_1)$ 和 $u \cdot g_2(X_1)$ 均是 n元 Bent函数. 所以, $u \cdot f(X)$ 在 $s^* = (s,0)$ 处的自相关函数

$$r_{uf}(s,0) = \frac{1}{2^{n+1}} \sum_{s \in F_2^n,\ s^* = (s,0)} (-1)^{uf(X+s^*)+uf(X)} =$$

$$\frac{1}{2^{n+1}} \sum_{s \in F_2^n} (-1)^{(1+x_{n+1})ug_1(X_1+s)+x_{n+1}ug_2(X_1+s)+(1+x_{n+1})ug_1(X_1)+x_{n+1}ug_2(X_1)} =$$

$$\frac{r_{ug_1}(s) + r_{ug_1}(s)}{2} = \begin{cases} 0, & s \neq 0 \\ 1, & s = 0 \end{cases} \quad s \in F_2^n$$

因此, 对一切 $s^* = (s,0)$, $s \in F_2^n$且 $s \neq 0$, $uf(X+s^*) + uf(X)$ 是平衡函数. 由引理 3可得, $f(X)$ 是平衡函数. 再由定义 9可知, 对一切 $s^* = (s,0)$, $s \in F_2^n$且 $s \neq 0$, $f(X)$ 满足 n次扩散准则.

4 结束语

本文给出了多输出半 Bent函数的一种构造方法. 同时, 还讨论了这类函数的平衡性、非线性性、稳定性及扩散性等密码学性质. 多输出半 Bent函数是一类密码学性质良好的奇数元多输出函数, 用作分组密码体制的非线性组合器时, 能有效地抵抗差分分析和线性分析的攻击. 另外, 多输出半 Bent函数还可应用于多输出前馈网[12,13]等方面.

[参考文献](References)

[1] ROTHAUS O S. On bent functions[J]. J of Combinatorial Theory Series A, 1976, 20: 300-305.

[2] CHEE S, LEE S, KIM K. Semi-bent Functions Advances in Cryptology Asiacrypt'94[M]. Berlin: Springer-Verlag, 1995: 107-118.

[3] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000: 39-132.
FENG Dengguo. Spectrum Theory and Its Applications in Cryptology[M]. Beijing: Science Press, 2000: 95-132. (in Chinese)

[4] 刘志高, 张福泰, 徐倩. 一类多输出 Bent函数的构造[J]. . 南京师范大学学报: 工程技术版, 2005, 5(2): 46-49.
LIU Zhigao, ZHANG Futai, XU Qian. Construction of a class of multi-output bent functions[J]. Journal of Nanjing Normal University: Engineering and Technology, 2005, 5(2): 46-49. (in Chinese)

[5] 胡磊, 裴定一, 冯登国. 一类 Bent函数的构造[J]. 中国科学院研究生院学报, 2002, 19(2): 103-106.
HU Lei, PEI Dingyi, FENG Dengguo. Construction of a class of bent functions[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2002, 19(2): 103-106. (in Chinese)

[6] 丁存生, 肖国镇. 流密码学及其应用[M]. 北京: 国防工业出版社, 1994: 136-138.
DING Chunsheng, XIAO Guozhen. Stream Cipher and Its Applications[M]. Beijing: Military Industry Press, 1994: 136-138. (in Chinese)

[7] 胡予濮, 张玉清, 肖国镇. 对称密码学[M]. 北京: 机械工业出版社, 2002: 56-58.
HU Yupu, ZHANG Yuqing, XIAO Guozhen. Symmetry Cryptology[M]. Beijing: Mechanism Industry Press, 2002: 56-58. (in Chinese)

[8] KAISA NYBERG. Perfect nonlinear S-boxed[C]//Advances in Cryptology Eurocrypt'91. Berlin: Springer-Verlag, 1992: 378-383.

[9] 张文英, 滕吉红, 李世取. 布尔函数的谱分解式及其在多维 Bent函数构造中的应用[C]//张焕国. 第三届中国信息和通信安全学术会议论文集 CCICS. 北京: 科学出版社, 2003: 290-296.
ZHANG Wenying, TENG Jiehong, LI Shiqu. Decomposition formula of spectrum of boolean functions and construction of k-dimension bent functions[C]//ZHANG Huanguo. The Collection of The Third China Conference on Information and Communications Security. Beijing: Science Press, 2003: 290-296. (in Chinese)

[10] 张文英, 李世取, 傅培利. 具有最高代数次数的 $2n$元 n维 Bent函数的构造[J]. 应用数学, 2004, 17(3): 444-449.
ZHANG Wenying, LI Shiqu, FU Peili. The construction of multi-output bent functions with highest algebraic degree[J]. Mathematica Applicata, 2004, 17(3): 444-449. (in Chinese)

[11] PIEPRZYK J, FINKELSTEIN G. Towards effective nonlinear cryptosystem design[C]//IEEE Proceedings, Part E: Computers and Digital Techniques, 1998, 135: 325-335.

[12] 杨义先, 胡正名. 抗熵漏前馈网络的研究[J]. 电子科学学刊, 1991, 20(3): 232-241.
YANG Yixian, HU Zhengming. Researches on anti-entropy leakage feedforward networks[J]. Journal of Electronics Science, 1991, 20(6): 232-241. (in Chinese)

[13] 胡一平, 冯登国. 多输出前馈函数的一种相关分析方法[J]. 电子与信息学报, 1998, 20(6): 787-793.
HU Yiping, FENG Dengguo. A correlation analysis on multi-output feedforward functions[J]. Journal of Electronics and Information Technology, 1998, 20(6): 787-793. (in Chinese)

[责任编辑: 刘 健]