文章编号:1674-2869(2010)09-0108-03

两类多输出一阶拟 Bent 函数的构造

刘志高

(马鞍山职业技术学院,安徽 马鞍山 243031)

摘 要:利用映射的特征矩阵给出了两类多输出一阶拟 Bent 函数的构造方法.分别构造出平衡多输出一阶拟 Bent 函数和具有相关免疫性的多输出一阶拟 Bent 函数.

关键词:拟 Bent 函数;多输出拟 Bent 函数;Walsh;循环谱

中图分类号:O158;TN918 文献标识码:A doi:10.3969/j.issn.1674-2869.2010.09.027

0 引 言

Bent 函数是由 Rothaus 于 1976 年提出的一类特殊的非线性组合函数[1].它的非线性度达到最大,稳定性强,差分分布均匀.用于非线性组合器可以很好的抗击最佳仿射逼近攻击和差分分析攻击.但 Bent 函数也存在着一些缺陷.如:它不具有平衡性和相关免疫性,n 元 Bent 函数的代数次数不超过 $n/2$,限制 n 为偶数等.为了弥补 Bent 函数的这些不足,为弥补 Bent 函数的这些不足,胡磊等定义了半 Bent 函数[2],李世取教授等提出了 k 阶拟 Bent 函数的概念[3],它是包含 Bent 函数和半 Bent 函数的更大的函数类.它可以具有 Bent 函数所不具有的密码学性质,如:平衡性、扩散性、相关免疫性等.随后,人们对拟 Bent 函数作出了一系列的研究成果[4-9].这些研究表明,拟 Bent 函数是一类密码学性质良好的布尔函数,在密码设计及通信领域中有着广泛的应用.

分组密码的核心部件 S-盒的设计中,常常采用具有多个良好密码学性质的多输出布尔函数.如何构造具有多种良好密码学性质的多输出布尔函数至为关键.人们在研究多输出函数时,总希望所选取的多输出函数的某些线性组合谱的绝对值尽可能均匀.仅就这一点而言,多输出 Bent 函数无疑就是最佳待选函数.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:非平衡性,相关免疫阶为零,其代数次数不超过变元数目 n 的一半,限制 n 为偶数等等.多输出拟 Bent 函数[10]可以弥补多输出 Bent 函数的这些不足,且具有多种良好的密码学性质,可广泛地应用于多输出前馈网,分组密码的 S-盒设计等领域.

本文给出了两类多输出一阶拟 Bent 函数的构造方法,其中一类是平衡的,另一类是具有相关免疫性的.它们可广泛应用于分组密码的 S-盒设计和最佳信号设计等领域.

1 基本定义

定义 1[11] 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 2[3] 一个 n 元布尔函数 $f(x)$ 称为 k 阶拟 Bent 函数,如果对任意的 $w\in F_2^n$,均有 $\left|S_{(f)}(w)\right|=0$ 或 $2^{-\frac{n-k}{2}}$.

将此定义推广到多输出函数情形即得如下定义:

定义 3 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 $\left|S_{(f)}(u,v)\right|=0$ 或 $2^{-\frac{n-k}{2}}$,则称 $f(x)$ 为多输出 k 阶拟 Bent 函数.

特别地,当 $k=0$ 时,上述 $f(x)$ 即为多输出 Bent 函数.当 $k=1$ 时,上述 $f(x)$ 即为多输出半 Bent 函数[12].

收稿日期:2009-05-31

基金项目:安徽省高等学校省级优秀青年人才基金项目资助(2010SQRL223)

作者简介:刘志高(1975-),男,安徽郎溪人,副教授,硕士.研究方向:高等数学的教学与研究工作,研究兴趣为应用学、密码学.

由定义3易得如下结论：

结论1　n元m输出函数$f(x)$是多输出k阶拟Bent函数的必要条件是n与k奇偶性相同.

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

定义4[11]　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$\left|\{x\in F_2^n | f(x)=a\}\right|=2^{n-m}$，则称$f(x)$是平衡的或正交的.

引理1[11]　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5[11]　设$f(x):\to F_2^m$，$m\leqslant n$，$x_1,x_2,\cdots,x_n$是n个独立的、均匀分布的布尔随机变量，随机向量$z=f(x)=f(x_1,x_2,\cdots,x_n)$. 如果对任意的$i_1,i_2,\cdots,i_j$，$1\leqslant i_1<\cdots,<i_j\leqslant n$及$u\in F_2^m$：$1\leqslant W_H(u)\leqslant k$，有$u\cdot z$与$(x_{i_1},x_{i_2},\cdots,x_{i_j})$统计独立，则称多输出函数$f(x)$是$k$级$j$阶相关免疫的.

引理2[11]　设$f(x)$如定义5中所述，$1\leqslant k\leqslant m$，则$f(x)$是k级j阶相关免疫的充要条件是对任意的$v\in F_2^n$，$1\leqslant W_H(v)\leqslant j$及$u\in F_2^m$，$1\leqslant W_H(u)\leqslant k$，有$S_{(f)}(u,v)=0$.

2　一类平衡多输出一阶拟*Bent*函数的构造

文献[2]给出了一类半Bent函数的构造方法，具体如下：

设n是奇数，$n=2k-1$，构造n元半Bent函数如下：

令$X_1=(x_1,x_2,\cdots,x_{k-1})$，$X_2=(x_k,x_{k+1},\cdots,x_n)$，$X=(X_1,X_2)$，再令$\tau$是$F_2^{k-1}\to F_2^k$的单射，$\tau(X_1)=(\tau_1(X_1),\cdots,\tau_k(X_1))$，其中$\tau_i$是$k-1$元布尔函数.

$$令 f(X)=\tau(X_1)X_2=\tau_1(X_1)x_k+\tau_2(X_1)x_{k+1}+\cdots+\tau_k(X_1)x_{2k-1} \quad (1)$$

引理3[2]　由(1)式定义的$f(X)$是n元半Bent函数，并且

$$\left|S_{(f)}(W)\right|=\begin{cases}2^{-\frac{n-1}{2}} & 若\ w_2\in \mathrm{Im}(\tau)\\ 0 & 否则\end{cases}$$

其中，$W=(W_1,W_2)$，$W_1=(w_1,\cdots,w_{k-1})$，$W_2=(w_k,w_{k+1},\cdots,w_n)$.

基于引理3，笔者于文献[12]中给出了一类多输出半Bent函数的构造方法，具体如下：

引理4[12]　设n是奇数，$n=2k-1$，记$X_1=(x_1,x_2,\cdots,x_{k-1})$，$X_2=(x_k,x_{k+1},\cdots,x_n)$，$X=(X_1,X_2)$，设$\pi_i:F_2^{k-1}\to F_2^k$是满足下列条件的$m$个单射：对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$，$\pi_{i1}\oplus\pi_{i_2}\oplus\cdots\oplus\pi_{i_j}$仍是单射. 设$f_i$：$F_2^n=F_2^{k-1}\times F_2^k\to F_2$，令$f_i(X)=\pi_i(X_i)X_2(1\leqslant i\leqslant m)$，则$f(X)=(f_1(X),f_2(X),\cdots,f_m(X))$是$n$元多输出半Bent函数.

显然该方法的关键在于如何构造满足引理中条件的m个单射$\{\pi_i\}_{i=1}^m$. 我们已于文献[12]中给出了构造这种单射集的一种具体方法，在此不再赘述.

一般地，多输出一阶拟Bent函数不一定是平衡函数. 下面将给出一类平衡多输出一阶拟Bent函数的构造方法.

以引理4中单射$\pi_i(X_1)=(\varphi_1^i(X_1),\varphi_2^i(X_1),\cdots,\varphi_k^i(X_1))$的所有项为行向量作矩阵

$$\boldsymbol{E}_i=\begin{pmatrix}\varphi_1^i(X_1^{(0)}) & \varphi_2^i(X_1^{(0)}) & \cdots & \varphi_k^i(X_1^{(0)})\\ \varphi_1^i(X_1^{(1)}) & \varphi_2^i(X_1^{(1)}) & \cdots & \varphi_k^i(X_1^{(1)})\\ \vdots & \vdots & \vdots & \vdots\\ \varphi_1^i(X_1^{(2^{k-1}-1)}) & \varphi_2^i(X_1^{(2^{k-1}-1)}) & \cdots & \varphi_k^i(X_1^{(2^{k-1}-1)})\end{pmatrix}$$

称$\boldsymbol{E}_i$为$\pi_i(X_1)$的特征矩阵，其中$X_1^{(j)}$，$0\leqslant j\leqslant 2^{k-1}-1$为$j$的二进制表示. $\boldsymbol{E}_i$的各列恰好是单射$\pi_i(X_1)$相应分量函数的真值表.

定理1　设$f(X)$是按引理4的方法所构造的多输出一阶拟Bent函数，则它为平衡函数的充要条件是对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$，矩阵$\boldsymbol{E}_{i_1}\oplus\boldsymbol{E}_{i_2}\oplus\cdots\oplus\boldsymbol{E}_{i_j}$中均不存在全0的行向量.

证明　由引理1可知，$f(X)$是多输出平衡函数，当且仅当对一切固定的u，$0\neq u\in F_2^m$，$u\cdot f(X)$是平衡布尔函数，当且仅当$S_{(u\cdot f)}(0,0')=0$，其中$0\in F_2^{k-1}$. 再由引理3可得，$S_{(u\cdot f)}(0,0')=0$当且仅当对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$，$0'\notin\mathrm{Im}(\pi_{i_1}\oplus\pi_{i_2}\oplus\cdots\oplus\pi_{i_j})$，当且仅当对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$，矩阵$\boldsymbol{E}_{i_1}\oplus\boldsymbol{E}_{i_2}\oplus\cdots\oplus\boldsymbol{E}_{i_j}$中均不存在全0的行向量.

上述定理1给出了一类平衡多输出一阶拟Bent函数的构造方法. J. Pieprzyk与G. Finkelstein在文献[13]中证明了$n+1$元平衡函数所具有的最高的非线性度是$2^n-2^{\frac{n}{2}}$. 笔者于文献[14]中已证明$n+1$元多输出一阶拟Bent函数的非线性度是$2^n-2^{\frac{n}{2}}$. 这说明平衡多输出一阶拟Bent函数已达到平衡函数所具有的最高非线性度. 因此，定理1所构造出的平衡多输出一阶拟Bent函数是很有意义的，它具有很强的抵抗最佳仿射逼近攻击

(BAA)的能力.

3 一类具有相关免疫性的多输出一阶拟 *Bent* 函数的构造

定理2 设$f(X)$是按引理4的方法所构造的多输出一阶拟Bent函数,则它具有m级l阶相关免疫性的充要条件是对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$,矩阵$E_{i_1}\oplus E_{i_2}\oplus\cdots\oplus E_{i_j}$的任意行向量中1的个数均大于$l$.

证明 由引理2知,$f(x)$是m级l阶相关免疫的充要条件是对任意的$v=(v_1,v_2)\in F_2^n$,$1\leqslant W_H(v)\leqslant l$,其中$v_1\in F_2^{k-1}$,$v_2\in F_2^k$及$u\in F_2^m$,$1\leqslant W_H(u)\leqslant m$,有$S_{(f)}(u,v)=S_{(u\cdot f)}(v_1,v_2)=0$再由引理3可得,$S_{(u\cdot f)}(v_1,v_2)=0$当且仅当对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$,$v_2\notin \mathrm{Im}(\pi_{i_1}\oplus\pi_{i_2}\oplus\cdots\oplus\pi_{i_j})$,当且仅当对任意的$1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_j\leqslant m$,矩阵$E_{i_1}\oplus E_{i_2}\oplus\cdots\oplus E_{i_j}$中任意行向量中1的个数均大于$l$.

参考文献:

[1] Rothaus O S. On Bent Functions [J]. Journal of Combinatorial Theory: Series A, 1976, 20: 300 - 305.

[2] 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.

[3] 李世取,刘文芬,滕吉红. k 阶拟 Bent 函数的性质及其应用[C]//谢仁宏. 第7届全国青年通信学术会议论文集. 北京:电子工业出版社,2001:939 -943.

[4] ZHENG Y L, ZHANG X M. On plateau functions [J]. IEEE Transactions on Information Theory, 2001, 47(3): 1215 - 1223.

[5] 滕吉红,李世取,刘文芬. k 阶拟 Bent 函数在密码设计和通信中的应用[J]. 通信学报,2003,24(12):58 - 66.

[6] 滕吉红,张文英,李世取,等. 一类 k 阶拟 Bent 函数密码性质的矩阵特征[J]. 计算机学报,2004,27(4):543 -547.

[7] 张习勇,韩文报. 拟 Bent 函数的性质和构造[J]. 数学学报,2004,47(6):1175 - 1184.

[8] 何军,张建中. 一类 k 阶拟 Bent 函数的构造[J]. 陕西师范大学学报:自然科学版,2005,33(3):18 - 20.

[9] 胡斌金,晨辉,冯春海. Plateaued 函数的密码学性质[J]. 电子与信息学报,2008,30(3):660 - 664.

[10] 胡斌金,晨辉,史建红. 多输出 Plateaued 函数的密码学性质[J]. 电子与信息学报,2009,31(6):1433 - 1437.

[11] 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,2000:95 - 132.

[12] 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.

[13] Pieprzyk J, Finkelstein C. Towards Effective Nonlinear Cryptosystem Design[C]//IEEE Proceedings, Part E: Computers and Digital Techniques. 1998, 135: 325 - 335.

[14] 刘志高,张福泰,徐倩. 一类多输出半 bent 函数的构造及其密码学性质[J]. 南京师范大学学报:工程技术版,2006,6(1):38 - 42.

The constructions of two classes of 1-order multi-output quasi-Bent functions

LIU Zhi-gao

(Maanshan Technical College, Ma'anshan 243031, China)

Abstract: Based on the characteristic matrix of mapping, two methods to construct 1-order multi-output quasi-Bent functions are presented. One class of 1-order multi-output quasi-Bent functions with balance is constructed. Another class of 1-order multi-output quasi-Bent functions with correlation-immunity is also constructed.

Key words: quasi-Bent function; multi-output quasi- Bent function; walsh cyclic-spectrum

本文编辑:龚晓宁