多输出 Plateaued 函数的密码学性质

胡 斌 金晨辉 史建红
(解放军信息工程大学电子技术学院 郑州 450004)

摘 要：该文对多输出 Plateaued 函数的一些密码学性质进行了研究，以多输出函数的特征函数为工具，建立了多输出 Plateaued 函数的差分转移概率与其 Walsh 谱及阶数之间的关系。给出了多输出 Plateaued 函数的 Walsh 谱值在一定条件下的分布情形，指出 (n,m,r) 多输出 Plateaued 函数的在其输出分量函数的任意非零线性组合函数均为非平衡函数时，其输入变量个数 n 、输出变量个数 m 与其阶数 r 之间的关系满足 $m \le n - r/2$ 。

关键词： 密码学；Bent 函数；部分 Bent 函数；Plateaued 函数；多输出 Plateaued 函数
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)06-1433-05

Cryptographic Properties of Multi-output Plateaued Functions

Hu Bin Jin Chen-hui Shi Jian-hong
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper discusses the cryptographic properties of Multi-output plateaued functions, the relationship among difference, Walsh spectra and the order of Multi-output plateaued functions is established. The Walsh spectra distribution of Multi-output plateaued functions is given under certain conditions. Pointed that when any nonzero linear combination of the coordinate functions of the (n,m,r) multi-output plateaued functions are not balanced, the relationship among the number n of input variables, number m of output variables and the order r satisfy $m \le n - r/2$.

Key words: Cryptography; Bent functions; Partially Bent functions; Plateaued functions; Multi-output Plateaued functions

1 引言

在密码函数的设计中，我们总是希望其能满足多个非线性准则，但是有的非线性准则之间存在着一定的制约关系，因此要设计出兼顾各种性质的非线性密码函数有一定的难度。如密码函数的非线性度是一个重要的非线性准则，非线性度达到最大的函数是 Bent 函数，Bent 函数对任意的非零向量均满足扩散性准则。但 Bent 函数又有其明显的弱点，如它不是平衡的，不满足相关免疫性，只能是偶数维函数，而且所有非仿射的部分Bent函数都可以通过Bent函数来构造[1]等。为弥补 Bent 函数的这一不足，1992 年 Carlet 提出了部分 Bent 函数[2]，Bent 函数是部分 Bent 函数的子集。部分 Bent 函数也具有很高的非线性度，而且可以具有平衡性、相关免疫性和一定的扩散性。但是，除了为 Bent 函数的那部分外，部分 Bent 函数都有非零的线性结构，而这是通常是在密码学上不希望具有的一个性质。Chee 等通过将一个 Bent 函数和一个与其仿射等价的另一个 Bent 函数进行链接而得到一类新的函数，即半 Bent 函数，但其只能是奇数维的，实用性受到很大限制[3,4]。2001 年，Zheng 等在文献[5]中提出了 Plateaued 函数，该函数是包含 Bent 函数和部分 Bent 函数的更大函数类。它具有很好的非线性度，可以满足相关免疫性、平衡性。而且可以不具有非零的线性结构，是一类密码学性质优良的密码函数，在密码学上有重要的应用。文献[5]对 Plateaued 函数的一些密码学性质进行了初步的研究，如非线性度、代数次数、线性维数等，得出了一些重要结论，文献[6]进一步对 Plateaued 函数的密码学性质进行了研究，给出了一些新的结果。

在密码设计中，很多情况下需要考虑多输出函数的情形，如分组密码的 S 盒设计、序列密码的前馈函数设计中就经常用到多输出函数。文献[7]中给出了多输出 Plateaued 函数的概念，并给出了两种简单的构造方法，但未对其密码学性质进行研究，文献[5]和文献[6]也主要是对布尔 Plateaued 函数的性质进行了分析研究。Plateaued 函数作为一类重要的密码函数，研究多输出 Plateaued 函数的密码学性质有重要意义。本文对多输出 Plateaued 函数的密码学性质进行了深入研究，以多输出函数的特征函数为工具，建立了其差分性质与其 Walsh 谱及阶数间的关系。给出了其谱值在一定条件下的具体分布情形，并给出了 r 阶多输出 Plateaued 函数的输入变量、输出变量与其阶数之间的关系，为密码设计中使用多输出 Plateaued 函数奠定了理论基础。

2 基本定义

n 个变元的布尔函数 $f(x)$ 是从 F_2^n 到 F_2 的一个函数或映

2008-05-30 收到，2008-12-31 改回

射，记为 $f(x):F_2^n \to F_2$。

定义 1[8] 设 $x=(x_1,x_2,\cdots,x_n)$，$w=(w_1,w_2,\cdots,w_n)\in F_2^n$，$x$ 和 w 的点积定义为 $w\cdot x = w_1x_1+w_2x_2+\cdots+w_nx_n$，$n$ 个变元的布尔函数 $f(x)$ 的循环 Walsh 谱定义为

$$S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+w\cdot x} \tag{1}$$

定义 2[8] 设 m,n 均为正整数，$m\le n$，$f_i(x)$ 为 $F_2^n\to F_2$ 上的布尔函数，$i=1,2,\cdots,m$，则称 $F(x)=(f_1(x),f_2(x),\cdots,f_m(x))$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出布尔函数。

以下如不特别说明，将 n 元 m 输出布尔函数简称为 n 元 m 输出函数，且 $m\le n$，以下的多输出函数均指上述所定义的 n 元 m 输出函数。

定义 3[5] 设 $f(x):F_2^n\to F_2$，如果存在一个偶数 r，使得 $\#\{w\in F_2^n \mid S_{(f)}(w)\ne 0\}=2^r$，且对任意的 $w\in F_2^n$，$S_{(f)}(w)=0$或$\pm 2^{-(r/2)}$，则称 $f(x)$ 为 r 阶 Plateaued 函数，其中 $\#\{A\}$ 表示集合 A 的计数。

定义 4 设 $F(x)=(f_1(x),f_2(x),\cdots,f_m(x))$ 为 $F_2^n\to F_2^m$ 上的多输出函数，如果对任意非 0 的 $c=(c_1,\cdots,c_n)\in F_2^n$，$f(x)=\sum_{i=1}^m c_if_i(x)$ 均是 r 阶 Plateaued 函数，则称 $F(x)$ 为 $F_2^n\to F_2^m$ 上的 r 阶多输出 Plateaued 函数，或称为 (n,m,r) 多输出 Plateaued 函数。

由文献[9]和文献[10]中所给出的多输出 Bent 函数和多输出部分 Bent 函数的定义可知，多输出 Bent 函数和多输出部分 Bent 函数均是多输出 Plateaued 函数的子集。

定义 5[8] 设 $f(x)$ 为 n 元 m 输出布尔函数，$u\in F_2^m$，$v\in F_2^n$，称 $S_{(f)}(u,v)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{u\cdot f(x)+v\cdot x}$ 为 $f(x)$ 在点 (u,v) 处的 Walsh 谱值。

由定义 5 可知，$f(x)$ 为 (n,m,r) 多输出 Plateaued 函数等价于对任意非 0 的 $u\in F_2^m, v\in F_2^n$，有 $S_{(f)}(u,v)=\pm 2^{-(r/2)}$ 或 0。

定义 6[8] 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，如果对任意的 $a\in F_2^m$，有 $P(f(x)=a)=1/2^m$，即 $\#\{x\in F_2^n, f(x)=a\}=2^{n-m}$，则称 $f(x)$ 为 $F_2^n\to F_2^m$ 上的多输出平衡函数。

3 多输出 Plateaued 函数的密码学性质

多输出布尔函数是分组密码的设计中经常使用的函数，其核心部分 S 盒通常就是多输出函数，对于分组密码的变换环节而言，差分性质是重要的一种性质，下面分析 (n,m,r) 多输出 Plateaued 函数的差分性质与其 Walsh 谱之间的关系。

定义 7 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，对任意的 $\alpha\in F_2^n,\beta\in F_2^m$，称

$$p_f(\alpha\to\beta)=\frac{1}{2^n}\#\{x\in F_2^n : f(x+\alpha)+f(x)=\beta\} \tag{2}$$

为 $f(x)$ 在点 (α,β) 处的差分转移概率。

为讨论 (n,m,r) 多输出 Plateaued 函数的差分转移概率，下面引入多输出函数的特征函数及其谱值的概念。

定义 8 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，设 $\xi_f:F_2^n\times F_2^m\to F_2$，则称

$$\xi_f(x,y)=\begin{cases}1, & y=f(x)\\ 0, & y\ne f(x)\end{cases} \tag{3}$$

为多输出函数 $f(x)$ 的特征函数。

$f(x)$ 的差分转移概率可通过其特征函数表示，我们有以下结论。

定理 1 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，$\xi_f(x,y)$ 为 $f(x)$ 的特征函数，则对任意的 $\alpha\in F_2^n,\beta\in F_2^m$，有：

$$p_f(\alpha\to\beta)=\frac{1}{2^n}\sum_x\sum_y\xi_f(x+\alpha,y+\beta)\xi_f(x,y) \tag{4}$$

证明 由差分转移概率的定义可知，

$$\begin{aligned}p_f(\alpha\to\beta)&=\frac{1}{2^n}\#\{x\in F_2^n : f(x+\alpha)+f(x)=\beta\}\\&=\frac{1}{2^n}\sum_y\#\{x\in F_2^n : f(x+\alpha)=\beta+y, \text{且} f(x)=y\}\end{aligned} \tag{5}$$

由于 $f(x)=y$ 等价于 $\xi_f(x,y)=1$，$f(x+\alpha)=\beta+y$ 等价于 $\xi_f(x+\alpha,\beta+y)=1$，于是对于 $x\in F_2^n$，$f(x+\alpha)=\beta+y$, 且$f(x)=y \Leftrightarrow \xi_f(x+\alpha,y+\beta)\xi_f(x,y)=1$，因此可得：

$$\begin{aligned}p_f(\alpha\to\beta)=\frac{1}{2^n}\sum_y\#\{x\in F_2^n : f(x+\alpha)=\beta+y,\\ \text{且} f(x)=y\}=\frac{1}{2^n}\sum_x\sum_y\xi_f(x+\alpha,y+\beta)\xi_f(x,y)\end{aligned}$$

证毕

定理 1 给出了差分转移概率和特征函数之间的关系，我们可进一步给出差分转移概率与函数的 Walsh 谱值之间的关系。为此我们先给出特征函数的线性谱的定义。

定义 9 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，$\xi_f(x,y)$ 为 $f(x)$ 的特征函数，则对任意的 $\alpha\in F_2^n,\beta\in F_2^m$，称

$$S_{\xi_f}(\alpha,\beta)=\frac{1}{2^{n+m}}\sum_x\sum_y\xi_f(x,y)(-1)^{\alpha\cdot x+\beta\cdot y} \tag{6}$$

为 $\xi_f(x,y)$ 在点 (α,β) 处的线性 Walsh 谱。

由特征函数 $\xi_f(x,y)$ 在点 (α,β) 处的线性 Walsh 谱的定义，可得以下结论。

定理 2 设 $f(x)$ 为 $F_2^n\to F_2^m$ 上的 n 元 m 输出函数，$\xi_f(x,y)$ 为 $f(x)$ 的特征函数，$S_{\xi_f}(\alpha,\beta)$ 为 $\xi_f(x,y)$ 在点 (α,β) 处的线性 Walsh 谱，则对任意的 $\alpha\in F_2^n,\beta\in F_2^m$，有：

$$\begin{aligned}&\sum_x\sum_y S_{\xi_f}^2(x,y)(-1)^{\alpha\cdot x+\beta\cdot y}\\&=\frac{1}{2^{n+m}}\sum_u\sum_v\xi_f(u+\alpha,v+\beta)\xi_f(u,v)\end{aligned} \tag{7}$$

证明

$$\begin{aligned}
&\sum_x\sum_y S_{\xi_f}^2(x,y)(-1)^{\alpha\cdot x+\beta\cdot y}\\
&=\sum_x\sum_y\frac{1}{2^{n+m}}\sum_a\sum_b\xi_f(a,b)(-1)^{\alpha\cdot x+b\cdot y}\\
&\quad\cdot\frac{1}{2^{n+m}}\sum_u\sum_v\xi_f(u,v)(-1)^{u\cdot x+v\cdot y}(-1)^{\alpha\cdot x+\beta\cdot y}\\
&=\frac{1}{2^{2n+2m}}\sum_a\sum_b\sum_u\sum_v\xi_f(a,b)\xi_f(u,v)\\
&\quad\cdot\sum_x\sum_y(-1)^{(u+a+\alpha)\cdot x+(v+b+\beta)\cdot y}\\
&=\frac{1}{2^{2n+2m}}\sum_a\sum_b\sum_u\sum_v\xi_f(a,b)\xi_f(u,v)\\
&\quad\cdot\sum_x(-1)^{(u+a+\alpha)\cdot x}\sum_y(-1)^{(v+b+\beta)\cdot y}\\
&=\frac{1}{2^{2n+2m}}\sum_u\sum_v\xi_f(u,v)\sum_a\sum_b\xi_f(a,b)\\
&\quad\cdot\sum_x(-1)^{(u+a+\alpha)\cdot x}\sum_y(-1)^{(v+b+\beta)\cdot y}\\
&=\frac{1}{2^{n+m}}\sum_u\sum_v\xi_f(u+\alpha,v+\beta)\xi_f(u,v)
\end{aligned}$$

证毕

对于 (n,m,r) 多输出Plateaued函数，记 $\Im_{\beta f}=\{\alpha\in F_2^n, S_{(f)}(\beta,\alpha)\neq 0\}$，由此可以得到 (n,m,r) 多输出 Plateaued 函数的差分转移概率与 $\Im_{\beta f}$ 的关系。

定理 3 设 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，则对任意的 $\alpha\in F_2^n,\beta\in F_2^m$，有

$$p_f(\alpha\to\beta)=\frac{1}{2^{m+r}}\sum_{y\in F_2^m}\sum_{x\in\Im_{yf}}(-1)^{\alpha\cdot x+\beta\cdot y}\tag{8}$$

证明 由定理 1 及定理 2 可得：

$$\begin{aligned}
p_f(\alpha\to\beta)&=\frac{1}{2^n}\sum_x\sum_y\xi_f(x+\alpha,y+\beta)\xi_f(x,y)\\
&=2^m\sum_x\sum_y S_{\xi_f}^2(x,y)(-1)^{\alpha\cdot x+\beta\cdot y}
\end{aligned}$$

对于 $\alpha\in F_2^n,\beta\in F_2^m$，有

$$\begin{aligned}
S_{(f)}(\beta,\alpha)&=\frac{1}{2^n}\sum_x(-1)^{\beta\cdot f(x)+\alpha\cdot x}=\frac{1}{2^n}\sum_x\sum_y\xi_f(x,y)(-1)^{\beta\cdot y+\alpha\cdot x}\\
&=2^m S_{\xi_f}(\alpha,\beta)
\end{aligned}$$

于是由 $f(x)$ 为 (n,m,r) 多输出Plateaued函数及定理2可得：

$$\begin{aligned}
p_f(\alpha\to\beta)&=2^m\sum_x\sum_y S_{\xi_f}^2(x,y)(-1)^{\alpha\cdot x+\beta\cdot y}\\
&=\frac{1}{2^m}\sum_x\sum_y S_{(f)}^2(y,x)(-1)^{\alpha\cdot x+\beta\cdot y}\\
&=\frac{1}{2^{m+r}}\sum_{y\in F_2^m}\sum_{x\in\Im_{yf}}(-1)^{\alpha\cdot x+\beta\cdot y}
\end{aligned}$$

证毕

对于 (n,m,r) 多输出 Plateaued 函数，还可以给出其谱值的一些性质。

定理 4 设 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，对任意固定的 $\alpha\in F_2^m$，若 $\alpha\cdot f(0)$ 为 0，则当 β 遍历 F_2^n 时，在所有 2^n 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取值为 $2^{-(r/2)}$ 的有 $2^{r-1}+2^{r/2-1}$ 个，取值为 $-2^{-(r/2)}$ 的有 $2^{r-1}-2^{r/2-1}$ 个，取值为 0 的有 2^n-2^r 个。若 $\alpha\cdot f(0)$ 为 1，则当 β 遍历 F_2^n 时，在所有 2^n 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取值为 $2^{-(r/2)}$ 的有 $2^{r-1}-2^{r/2-1}$ 个，取值为 $-2^{-(r/2)}$ 的有 $2^{r-1}+2^{r/2-1}$ 个，取值为 0 的有 2^n-2^r 个。

证明 对于任意的 $\alpha\in F_2^m$，有：

$$\begin{aligned}
\sum_{\beta\in F_2^n}S_{(f)}(\alpha,\beta)&=\frac{1}{2^n}\sum_{\beta\in F_2^n}\sum_{x\in F_2^n}(-1)^{\alpha\cdot f(x)+\beta\cdot x}\\
&=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{\alpha\cdot f(x)}\sum_{\beta\in F_2^n}(-1)^{\beta\cdot x}=(-1)^{\alpha\cdot f(0)}
\end{aligned}$$

故对于任意的 $\alpha\in F_2^m$，当 $\alpha\cdot f(0)$ 为 0 时，有 $\sum_{\beta\in F_2^n}S_{(f)}(\alpha,\beta)=1$，由于 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，$S_{(f)}(\alpha,\beta)$ 只取 0 或 $\pm2^{-(r/2)}$ 这 3 个值，于是对于任意固定的 $\alpha\in F_2^m$，当 β 遍历 F_2^n 时，在所有 2^n 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取值为 $2^{-(r/2)}$ 的有 $2^{r-1}+2^{r/2-1}$ 个，取值为 $-2^{-(r/2)}$ 的有 $2^{r-1}-2^{r/2-1}$ 个，取值为 0 的有 2^n-2^r 个。

反之，若 $\alpha\cdot f(0)$ 为 1 时，有 $\sum_{\beta\in F_2^n}S_{(f)}(\alpha,\beta)=-1$，于是当 β 遍历 F_2^n 时，在所有 2^n 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取值为 $2^{-(r/2)}$ 的有 $2^{r-1}-2^{r/2-1}$ 个，取值为 $-2^{-(r/2)}$ 的有 $2^{r-1}+2^{r/2-1}$ 个，取值为 0 的有 2^n-2^r 个。　　证毕

定理 5 设 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，记 $\ker_f=\{x\in F_2^n: f(x)=0\}$，则有：

(1)若 $\ker_f$ 构成一线性子空间，则对任意非 0 的 $\beta\in F_2^n$，当 α 遍历 F_2^m 时，在所有 2^m 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取 $2^{-(r/2)}$ 与 $-2^{-(r/2)}$ 的个数相等。

(2)若集合 $\ker_f$ 中的元素个数为奇数，则有 $n-m\le r/2$。

证明 对于任意的 $\beta\in F_2^n,\beta\neq 0$，有

$$\begin{aligned}
\sum_{\alpha\in F_2^m}S_{(f)}(\alpha,\beta)&=\frac{1}{2^n}\sum_{\alpha\in F_2^m}\sum_{x\in F_2^n}(-1)^{\alpha\cdot f(x)+\beta\cdot x}=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{\beta\cdot x}\\
&\quad\cdot\sum_{\alpha\in F_2^m}(-1)^{\alpha\cdot f(x)}=2^{m-n}\sum_{x\in\ker_f}(-1)^{\beta\cdot x}
\end{aligned}$$

(1)对于任意给定的 $\beta\in F_2^n,\beta\neq 0$，当 $\ker_f$ 构成一线性子空间时，有 $\sum_{\alpha\in F_2^m}S_{(f)}(\alpha,\beta)=0$，由于 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，$S_{(f)}(\alpha,\beta)$ 只取 0 或 $\pm2^{-(r/2)}$ 这三个值，于是当 α 遍历 F_2^m 时，在所有 2^m 个 $S_{(f)}(\alpha,\beta)$ 的取值中，取 $2^{-(r/2)}$ 与 $-2^{-(r/2)}$ 的个数相等。

(2)对于任意固定的 $\beta\in F_2^n$，$\sum_{\alpha\in F_2^m}S_{(f)}(\alpha,\beta)=2^{m-n}\cdot\sum_{x\in\ker_f}(-1)^{\beta\cdot x}=k\cdot2^{-(r/2)}$，当集合 $\ker_f$ 中的元素个数为奇数时，则 2^{m-n} 必定为 $2^{-(r/2)}$ 的倍数，故此时有 $n-m\le r/2$。

证毕

众所周知，对于 (n,m) 多输出 Bent 函数，一定有 n 为偶数，且 $m \le n/2$。那么，对于 (n,m,r) 多输出 Plateaued 函数， n 与 m 之间是否也存在着特定的关系呢？定理 5 中的第 2 个结论从一个角度给出了 (n,m,r) 多输出 Plateaued 函数中 n,m,r 之间的关系。下面给出 (n,m,r) 多输出 Plateaued 函数中 n,m,r 之间在函数不平衡时存在的特定关系。

对于 $F_2^n \to F_2^m$ 上的多输出平衡函数，有以下结论。

定理 6[8] 设 $f(x)$ 为 $F_2^n \to F_2^m$ 上的 n 元 m 输出函数，则 $f(x)$ 是平衡多输出函数的充分必要条件是对于任意的 $c \in F_2^m, c \ne 0$， $c \cdot f(x)$ 是平衡的布尔函数。

下面给出 (n,m,r) 多输出 Plateaued 函数中 n,m,r 之间的关系。

定理 7 设 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，且对于任意非零的 $u \in F_2^m$， $u \cdot f(x)$ 均是不平衡函数，则有：$m \le n - r/2$。

证明 设 $a_y = \#\{x \in F_2^n, f(x) = y\}, y \in F_2^m$， $u \in F_2^m$， $u \ne 0$，考查 $u \cdot f(x)$ 在 0 点的 Walsh 谱值，有

$$2^n S_{(f)}(u,0) = \sum_{x \in F_2^n} (-1)^{u \cdot f(x)} = \sum_{y \in F_2^m} a_y (-1)^{u \cdot y} \tag{9}$$

两边对非 0 的 u 求和，可得

$$\sum_{y \in F_2^m} a_y \sum_{u \ne 0} (-1)^{u \cdot y} = 2^n \sum_{u \ne 0} S_{(f)}(u,0) \tag{10}$$

即

$$a_0 \sum_{u \ne 0} (-1)^{u \cdot 0} + \sum_{y \in F_2^m, y \ne 0} a_y \left(\sum_{u \in F_2^m} (-1)^{u \cdot y} - (-1)^{0 \cdot y} \right) = 2^n \sum_{u \ne 0} S_{(f)}(u,0) \tag{11}$$

于是可得

$$a_0 \cdot (2^m - 1) - \sum_{y \in F_2^m, y \ne 0} a_y = 2^n \sum_{u \ne 0} S_{(f)}(u,0) \tag{12}$$

即

$$a_0 \cdot 2^m - 2^n = 2^n \sum_{u \ne 0} S_{(f)}(u,0) \tag{13}$$

由于 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，且对于任意非零的 $u \in F_2^m$， $u \cdot f(x)$ 均是不平衡函数，由定理 6 可知，有 $S_{(f)}(u,0) = \pm 2^{-(r/2)}$。又显然 $\sum_{u \ne 0} S_{(f)}(u,0)$ 必定为 $2^{-(r/2)}$ 的倍数，不妨设 $\sum_{u \ne 0} S_{(f)}(u,0) = k \cdot 2^{-(r/2)}$。由于非 0 的 u 的个数为 $2^m - 1$， 即 $S_{(f)}(u,0)$ 取 $2^{-(r/2)}$ 与 $-2^{-(r/2)}$ 的个数之和为 $2^m - 1$，为奇数，故二者之差也必定为奇数，即 k 为奇数。于是由式(13)可得：

$$a_0 \cdot 2^m = k \cdot 2^{n - \frac{r}{2}} + 2^n \tag{14}$$

因此有： $2^m \mid (k \cdot 2^{(n-r/2)} + 2^n)$， 显然 $2^m \mid 2^n$， 因此可得：$2^m \mid k \cdot 2^{(n-r/2)}$，由于 k 为奇数，故 $2^m \mid 2^{(n-r/2)}$，所以 $m \le n - r/2$。 证毕

由定理 5 和定理 7 易知以下推论。

推论 1 设 $f(x)$ 为 (n,m,r) 多输出 Plateaued 函数，记 $\ker_f = \{x \in F_2^n : f(x) = 0\}$， 若 $f(x)$ 是不平衡函数且集合 $\ker_f$ 中的元素个数为奇数，则有： $m = n - r/2$。

对于 (n,m,r) 多输出 Plateaued 函数 $f(x)$， 当 $f(x)$ 为非线性函数时，其至少在 2 个以上点的谱值不为 0，又由于 r 必定为偶数，故有 $r \ge 2$， 此时有 $m \le n - 1$， 这说明任意的置换不可能是多输出 Plateaued 函数，任意的 $F_2^n \to F_2^n$ 上的函数也不可能是多输出 Plateaued 函数。对于 $m < n$ 的 (n,m,r) 多输出 Plateaued 函数 $f(x)$， 当其为平衡函数时，n,m,r 之间的具体关系如何，还有待于进一步研究。

4 结束语

本文对多输出 Plateaued 函数的一些密码学性质进行了深入分析与研究，以多输出函数的特征函数为工具，建立了其差分性质与其 Walsh 谱及阶数间的关系。给出了其谱值在一定条件下的具体分布情形，并给出了 r 阶多输出 Plateaued 函数的输入变量、输出变量与其阶数之间的关系。为密码设计中使用多输出 Plateaued 函数奠定了理论基础。多输出 Plateaued 函数的构造理论与方法研究是多输出 Plateaued 函数研究的另外一个重要内容，文献[7]中给出了两种简单的构造方法，深入研究多输出 Plateaued 函数的构造理论方法是很有意义的问题，值得进一步研究和探讨。

参 考 文 献

[1] Li Shi Qi and Zhao Ya Qun. The relation between partially-Bent and Bent functions. Proceedings of CCICS'99, Beijing, 1999: 196–201.

[2] Carlet C. Partially bent functions, Advance in Cryptology-Crytpo'93 Berlin: Springer-Verlag, 1993: 77–101.

[3] Charpin P, Pasalic E, and Tavernier C. On Bent and semi-bent quadratic boolean functions. *IEEE Trans. on Information Theory*, 2005, 51(12): 4286–4298.

[4] 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. 南京师范大学学报, 2006, 6(1): 38–42.
Liu Zhi-gao, Zhang Fu-tai, and Xu Qian. The constructions and cryptographic properties of a type of multi-output semi-bent functions. *Journal of NanJin Normal University*, 2006, 6(1): 38–42.

[5] Zheng Y and Zhang X M. On Plateaued functions. *IEEE Trans. on Information Theory*, 2001, 47(3): 1215–1223.

[6] 胡斌, 金晨辉, 冯春海. Plateaued函数的密码学性质. 电子与信息学报, 2008, 30(3): 660–664.
Hu Bin, Jin Chen-hui, and Feng Chun-hai. The cryptographic properties of Plateaued functions. *Journal of Electronics & Information Technology*, 2008, 30(3): 660–664.

[7] Zhang Wei-guo and Xiao Guo-zhen. On constructions of multi-output plateaued functions. *Chinese Jorunal of Electronics*, 2005, 15(1): 169–171.

[8] 冯登国. 频谱理论及其在密码学中的应用. 北京: 科学出版社, 2000: 39–132.
Feng Deng-guo. The Spectrum Theory and Its Application in Cryptography. Beijing, Science Press, 2000: 39–132.

[9] 鞠桂枝, 赵亚群. 多输出部分 Bent 函数的几种构造方法. 通信学报, 2005, 26(5): 138–141.
Ju Gui-zhi and Zhao Ya-qun. Constructions of multi-output partially Bent functions. *Journal on Communications*, 2005, 26(5): 138–141.

[10] 赵亚群, 鞠桂枝. 多输出 Bent 函数有关性质的研究. 郑州大学学报(理学版), 2005, 27(1): 45–48.
Zhao Ya-qun and Ju Gui-zhi. The properties of multi-output Bent functions. *Journal of Zhengzhou University*, 2005, 27(1): 45–48.

[11] Carlet C. On an improved correlation analysis of stream ciphers using Muti-output boolean functions and the related generalized notion of nonlinearity, http://eprint.iacr.org, 2007/207. pdf, 2007.

胡　斌： 男，1971 年生，副教授，研究方向为密码学与信息安全.
金晨辉： 男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.
史建红： 男，1976 年生，讲师，研究方向为密码学与信息安全.