多维超 Bent 函数的构造

张文英　武传坤
(中国科学院软件研究所信息安全国家重点实验室　北京 100080)
(中国科学院研究生院　北京　100039)

摘　要：有限域 $F_{p^{2m}}$ 上的超Bent函数是与F_p上所有m序列的距离都达到最大的函数，该文研究了 $F_{2^{2m}}$ 上超Bent函数与$\mathrm{GF}^{2m}(2)$上Bent函数之间的关系，对一类超Bent函数的性质作了深入细致的刻画，给出了有限域 $F_{p^{2m}}$ 上多维超Bent函数的两种构造方法.

关键词：密码学；Bent 函数；超 Bent 函数；多维超 Bent 函数
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2007)01-0197-04

The Construction of Multi Out-put Hyper Bent Functions

Zhang Wen-ying　Wu Chuan-kun
(*State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)
(*Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract: Hyper Bent functions achieve the maximal minimum distance to all the m sequences. In this paper, the relationship between the hyper Bent function on $F_{2^{2m}}$ and the Bent function on $\mathrm{GF}^{2m}(2)$ is studied and two methods for constructing vectorial hyper Bent functions on $F_{p^{2m}}$ are proposed as well.

Key words: Cryptography; Bent function; Hyper Bent function; Multi–dimension hyper Bent function

1　引言

有限域上超Bent函数[1]的概念是由龚光等学者在 2001 年欧密会上提出的，超Bent函数不仅像Bent函数那样能抵抗线性密码分析和差分密码分析，而且用任意的置换单项式去逼近它也都无济于事。文献[2]的实验结果表明，美国数据加密标准DES的S盒中所用到的函数与各置换单项式的距离接近相等，这说明超Bent函数在密码中的确有着重要的应用。最近Carlet又把超Bent函数用于循环码的研究中[3]。

该文将特征为 2 的有限域上超Bent函数的概念推广到特征为p的有限域上，研究了 $F_{2^{2m}}$ 上超Bent函数与$\mathrm{GF}^{2m}(2)$上Bent函数之间的关系，对一类超Bent函数的性质作了深入细致的研究，给出了利用素域F_p上m维向量空间上任意一个置换构造有限域 $F_{p^{2m}}$ 上的m维超Bent函数的方法。由于素域上m维向量空间上的置换比比皆是，所以这种构造容易实现。

2　$F_{2^{2m}}$ 上Bent函数与$\mathrm{GF}^{2m}(2)$上Bent之间的关系

定义 1　设p是素数，m是正整数，u是p次本原单位根，F是有p^{2m}个元素的有限域，即 $F=F_{p^{2m}}$，$K=Z/(p)$，$f:F\to K$。如果对任意给定的 $\gcd(p^{2m}-1,c)=1$ 及所有的 $w\in F$，其扩展Chrestenston循环谱 $S_{(f)}(w,c)$ 的模都为 p^{-m}，即

$$\left|S_{(f)}(w,c)\right|=p^{-2m}\left|\sum_{x\in K}u^{f(x)-\mathrm{Tr}(wx^c)}\right|=p^{-m} \qquad (1)$$

则称 $f(x)$为超 Bent 函数。

2005-03-22 收到，2005-08-23 改回
国家自然科学基金(90304007)资助课题

特别地，在定义 1 中若将 p 取为 2，就得到龚光等在文献[2]中所给出的超 Bent 函数。

由超 Bent 函数的定义不难证明若 $f(x)$ 是超 Bent 函数，则 $f(\alpha^k x)$, $0\le k\le p^{2m-2}$ 也是超 Bent 函数，即超 Bent 函数具有仿射不变性。

下面给出与 $F_{2^{2m}}$ 相对应的GF(2)的 $2m$维向量空间$\mathrm{GF}^{2m}(2)$上Bent函数的定义。

定义 2[4]　设 f:$\mathrm{GF}^{2m}(2)\to\mathrm{GF}(2)$，如果对任意给定的 $w\in\mathrm{GF}^{2m}(2)$，都有：$S_{(f)}(w)=\sum_{x\in\mathrm{GF}^{2m}(2)}(-1)^{f(x)+w\cdot x}=\pm 2^{-m}$，则称$f(x)$为Bent函数。

引理 1[5]　设F是有限域K的有限扩张，同时也将其视为K上的向量空间。则从F到K的所有线性变换恰好是所有迹函数 $L_\beta(x)=\mathrm{Tr}(\beta x)$，$\beta\in F$ 的全体，且 $L_{\beta_1}\ne L_{\beta 2}$ 当且仅当 $\beta_1\ne\beta_2$。因此 $L_\beta(x)$，$\beta\in F$ 与向量空间 $F=K^n$ 上的线性函数 $w\cdot x$, $w\in K^n$ 一一对应。即对于任意的 $\beta\in F$，都有 $w_\beta\in K^n$，使得对于任意的 $x\in F=K^n$ 都有 $L_\beta(cx)=w_\beta\cdot x$。

引理 2[6]　设$w\in F_{2^n}\backslash\{0\}$，$f(x)=x^c$是一个置换，则 $\deg(\mathrm{Tr}(wx^c))=W_H(c)$。其中$\deg(\cdot)$表示函数$\mathrm{Tr}(wx^c)$的代数次数，$W_H(c)$表示$c$的汉明重量。

定理 3　设 n 为偶数，有限域 F_{2^n} 上的一个超 Bent 函数与 $\mathrm{GF}^n(2)$ 上的一个 Bent 函数唯一对应。

证明　由引理 1 知道，$\{\mathrm{Tr}(\beta x),\ x\in F_{2^n}\mid\beta\in F_{2^n}\}$ 恰好是向量空间 $\mathrm{GF}^n(2)$ 上所有线性函数 $\{w\cdot x, x\in\mathrm{GF}^n(2), w\in\mathrm{GF}^n(2)\}$ 的全体，又由引理 2 知当c取遍与 2^n-1 互素的

自然数时，$\{\mathrm{Tr}(wx^c), x\in F: w\in F\}$ 还包含一些非线性函数，从而

$$\{\mathrm{Tr}(wx^c), x\in F: w\in F, \gcd(p^n-1,c)=1\}$$
$$\supset \{wx, x\in K^n: w\in K^n\} \quad (2)$$

因超 Bent 函数与式(2)左侧集合中的函数距离都相等，自然与式(2)右侧集合中的函数距离也都相等，故超 Bent 函数要求的条件比 Bent 函数强，超 Bent 函数一定是 Bent 函数。

由于目前对 $\mathrm{GF}^n(2)$ 上 Bent 函数的研究有了比较丰富的结果，由定理 3，有限域 F_{2^n} 上的一个超 Bent 函数与 $\mathrm{GF}^n(2)$ 上的一个 Bent 函数唯一对应，所以可以在已知的 Bent 函数中寻找超 Bent 函数，这也是超 Bent 函数的构造方法之一，运用这种方法，我们就找到了 F_{2^4} 上所有超 Bent 函数(共 56 个)，参见附录。(**注：**附录中每个函数取反后仍然是超 Bent 函数)

3 有限域上超 Bent 函数的构造

3.1 有限域上超 Bent 函数的构造定理

文献[7，8]中给出了如下广义 Bent 函数的构造法，作者在研究中发现这类函数不仅是广义 Bent 函数，还是超 Bent 函数。

定理 2 设p是一个素数，α 是 $F=F_{p^{2m}}$ 中的本原元，$F_{p^m}=\{1,\alpha^{p^m+1},(\alpha^{p^m+1})^2,\cdots,(\alpha^{p^m+1})^{p^m-1}\}$ 是 F_{p^n} 的子域，那么 $H_0=F_{p^m}^{\bullet}=F_{p^m}\setminus\{0\}$ 的陪集 $H_i=\alpha^i F_{p^m}^{\bullet}\subset F$，$i=0,1,\cdots,p^m$ 两两不同，且 $\bigcup_{i=0}^{p^m}H_i=F\setminus\{0\}$，将除了$H_0$之外的其他所有陪集所作成的集合 $\{H_1,H_2,\cdots,H_{p^m}\}$ 任意平均分成p组，每组中有 p^{m-1} 个 H_i，将每组中所有陪集的并集按照顺序分别记为 $A_0,A_1,\cdots,A_{p-1}$，即

$$A_0=H_{s1}\cup H_{s2}\cup\cdots\cup H_{sp^{m-1}}$$
$$A_1=H_{sp^{m-1}+1}\cup H_{sp^{m-1}+2}\cup\cdots\cup H_{s2p^{m-1}}$$
$$\vdots$$
$$A_{p-1}=H_{sp^m-p^{m-1}+1}\cup H_{sp^m-p^{m-1}+2}\cup\cdots\cup H_{sp^m}$$

其中 $s1,s2,\cdots,sp^m$ 是 $1,\cdots,p^m$ 的一个全排列。那么函数

$$f:\ F_{p^n}\to F_p,\ f(x)=\begin{cases}0, & x\in H_0\cup A_0\\ k, & x\in A_k, k=1,2,\cdots,p-1\end{cases} \quad (3)$$

是 F_{p^n} 上的超 Bent 函数。

定理 2 的证明类似于文献[1]中定理 1，略。

定理 2 所给出的方法在表面上看来十分复杂，既要把 F 分成陪集，又要把各陪集进行分类。深入分析一下它的构造思路，就容易理解了：分成陪集的目的就是要把 F_{p^n} 分成若干个不相交的集合，将这些陪集平均分成 p 组，给每组分别赋予不同的函数值便构造了 F_{p^n} 上的一个超 Bent 函数。特别地，当 p=2 时，就是让 $f(0)$，$f(F_{2^m}^{\bullet})$ 的值固定为 0，而 $f(\alpha F_{2^m}^{\bullet}),\cdots,f(\alpha^{2^m}F_{2^m}^{\bullet})$ 的值一半取 0，一半取 1。

下面是两个根据定理 2 所构造的超 Bent 函数的例子。

例 1 $n=4,m=2,p=2$ 时，$F_{16}=\{0,1,\alpha,\cdots,\alpha^{14}\}$，生成多项式为 $x^4+x+1=0$，α 是 F_{16} 上的本原元，则 $F_4=\{0,1,\alpha^5,\alpha^{10}\}$，$\alpha^5$ 是其生成元。令

$$H_0=F_4^{\bullet}=\{1,\alpha^5,\alpha^{10}\}$$
$$H_1=\alpha F_4^{\bullet}=\{\alpha,\alpha^6,\alpha^{11}\}$$
$$H_2=\alpha^2F_4^{\bullet}=\{\alpha^2,\alpha^7,\alpha^{12}\}$$
$$H_3=\alpha^3F_4^{\bullet}=\{\alpha^3,\alpha^8,\alpha^{13}\}$$
$$H_4=\alpha^4F_4^{\bullet}=\{\alpha^4,\alpha^9,\alpha^{14}\}$$

将陪集 H_1,H_2,H_3,H_4 分成 2 组：$A_0=H_1\cup H_2$，$A_1=H_3\cup H_4$。

如下定义函数

$$f:F_{16}\to F_2,\quad f(x)=\begin{cases}0, & x\in\{0\}\cup H_0\cup A_0\\ 1, & x\in A_1\end{cases} \quad (4)$$

则f满足定理 2 的条件，所以f是F_{16}上的超Bent函数。

若转化为布尔函数，则 $f(x)=x_1x_2+x_1x_3+x_3x_4\ +x_4$。易见它是$\mathrm{GF}^4(2)$上的Bent函数。

例 2 $F=F_9=\{0,1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^7\}$，生成多项式为$x^2+x+2=0$，$F_3^{\bullet}=F_3\setminus\{0\}=\{1,\alpha^4\}$，$H_0=F_3^{\bullet}$，$H_1=\alpha F_3^{\bullet}$，$H_2=\alpha^2F_3^{\bullet}$，$H_3=\alpha^3F_3^{\bullet}$。定义函数 $f:F_9\to F_3$，使得：$f(0)=f(H_0)=0$，$f(H_1)=0$，$f(H_2)=1$，$f(H_3)=2$。则f满足定理 2 的条件，是F_9上的超Bent函数。具体地，$f(\alpha^2)=f(\alpha^6)=1$，$f(\alpha^3)=f(\alpha^7)=2$，$f$在$F$中其他各点处函数值为 0。经计算得其多项式表示为 $f(x_1,x_2)=x_1x_2$，$(x_1,x_2)\in F_3^2$。

3.2 定理 2 中所构造函数的取值分布

下面来考察定理 2 中超 Bent 函数 f 的取值分布：首先函数值为 0 的点的个数为

$$|\{x\in F_{p^n}: f(x)=0\}|=1+|H_0|+|A_0|$$
$$=(1+p^{m-1})(p^m-1)+1$$

其次，函数值为 k 的点的个数为

$$|A_k|=p^{m-1}(p^m-1),\ k=1,\ \cdots,p-1$$

3.3 定理 2 中所构造函数值序列的周期性

定理 2 将有限域 F_{p^n} 中的元素划分成 p^m+1 个陪集，所定义的 f 在每个陪集内部所有元素的函数值都相同。因为各陪集形如 $H_k=\alpha^kF_{p^m}^{\bullet}=\alpha^k\{1,\ \alpha^{p^m+1},\alpha^{2(p^m+1)},\cdots,\alpha^{(p^m-2)(p^m+1)}\}$，保证了凡是相差 α 的 p^m+1 的整数倍方幂的元素必落在同一个陪集 H_i，$0\le i\le p^m$ 中，从而它们在映射f下的像相等，可见若将函数值按照自变量x的根表示中 α 的升幂排列，那么，函数值序列具有周期性，且其周期至多是p^m+1。因为必定存在两个序号相邻的陪集的像不同，即$f(H_i)=f(H_{i+1})$，若不然，则函数变成常值函数。即有某 H_i 中的最后一个元素 $\alpha^{i+(p^m-2)(p^m+1)}$ 的像与其后面的连续 p^m-1 个元素的像都不相同，故函数的周期不小于p^m，因而函数值序列的周期是p^m+1。

4 有限域上多维超 Bent 函数的构造

定义 3 每个分量以及各分量的所有非零线性组合都是超 Bent 函数的多输出函数称为多维超 Bent 函数，m 个输出

时称为 m 维超 Bent 函数。

本节分别运用有限域上 Bent 函数与相应的素域的向量空间上 Bent 函数之间的关系和定理 2 给出了多维超 Bent 函数的两种构造方法：

4.1　从多维 Bent 函数中寻找多维超 Bent 函数

因有限域 $F_{2^{2m}}$ 上的一个超Bent函数与$\mathrm{GF}^{2m}(2)$上的一个Bent函数唯一对应。$F_{2^{2m}}$ 上一组多维超Bent函数与$\mathrm{GF}^{2m}(2)$上多维Bent函数相对应，由于目前我们已经掌握了Bent函数的一些构造方法，并且对于变元个数较少的Bent函数的结构已经清楚，所以可在已知的多维Bent函数中寻找多维超Bent函数。用此方法，我们找到了F_{16}上所有二维超Bent函数，其中 $(x_1x_3+x_2x_4+x_3x_4+x_2+x_3,\ x_1x_2+x_1x_4\ \ +x_2x_3+x_2)$ 便是一例。

4.2　依据定理 2 构造多维超 Bent 函数

定理 3　设 f_i 和 φ_{f_i} 如定理 2 定义，则 $(f_1(x),f_2(x),\cdots,f_m(x)),\ x\in F_{p^m}$ 是 m 维超 Bent 函数的充分必要条件是 $(\varphi_{f_1},\varphi_{f_2},\cdots,\varphi_{f_m})$ 是 Z_p^m 上的置换，这种形式的 m 维超 Bent 函数共 $p^m!$ 个。

证明　函数f是形如定理 2 中所构造的超Bent函数的充要条件是f在同一集 A_i，i=0, 1,$\cdots$, $p-1$ 内各点处的函数值相等，且对不同的i，f取不同的值。这里A_i是把陪集集合$\{H_1, H_2,\cdots, H_p^m\}$中元素$p$“等分”后，取各等份中陪集的并集而得。也就是说若记 $\varphi_f(H_i)$ 为 $H_i, i=1,2,\cdots,p^m$ 中元素共同的像，则f是超Bent函数当且仅当

$$\varphi_f:\{H_1,H_2,\cdots,H_{p^m}\}\to F_p, H_i\mapsto f(x), x\in H_i \qquad (5)$$

是一个平衡函数。于是构造一个这种形式的超Bent函数的问题就等价于构造定义域内有p^m个元素的一个p值平衡逻辑函数 φ_f 的问题。为了构造各分量都形如定理 2 中f的多维超Bent函数，只须保证各分量相应的按照式(5)所定义的函数 φ_{f_i} 的任意非 0 线性组合都平衡即可，于是构造m维超Bent函数的问题便被转化为构造一个 F_{p^m} 到其自身的平衡逻辑函数的问题。一般地，若想构造有限域 F_{p^n} 上的$k(\ k\le m=n/2\ )$维向量广义Bent函数 $(f_1,f_2,\cdots,f_k)$，$k\le m$，只须构造一组具有均匀分布的向量逻辑函数 $(\varphi_1,\varphi_2,\cdots,\varphi_k)$，再令 $\varphi_{f_1}=\varphi_1$，$\varphi_{f_2}=\varphi_2,\cdots,\varphi_{f_k}=\varphi_k$，最后按照式(5)中的法则所求得的 $(f_1,f_2,\cdots,f_k)$ 就是有限域 F_{p^n} 上$k(\ k\le m=n/2\ )$维向量广义Bent函数。因 Z_p^m 上共$p^m!$个置换，所以这种形式的m维超Bent函数共有 $p^m!$ 个。

下面是构造多维超 Bent 函数的两个例子：

例 3　设 $H_i, i=0,1,2,3,4$ 同例 1，定义 $f_1,f_2:F_{16}\to F_2$

i	f_1	f_2
1	0	0
2	0	1
3	1	0
4	1	1

此表最左侧一栏表示陪集的序号，中间一栏表示各H_i，i=1，2，3，4 中元素在映射f_1下共同的像，右侧一栏表示各H_i中元素在映射f_2下共同的像，由于这是GF(2)上二维向量空间中元素的一个排列，所以此两列的任意非 0 线性和都平衡。再定义f_1和f_2在 0 点及H_0内各点处的函数值为 0，则f_1、f_2、f_1+f_2都满足定理 2 的条件，因而它们都是超Bent函数，故得F_{16}上二维超Bent函数 $(f_1,\ f_2)$。若转化为布尔函数，则有 $f_1(x)=x_1x_2+x_1x_3+x_3x_4+x_4\quad,\quad f_2(x)=x_1x_4+x_2x_4+x_2x_3+x_3+x_4$，易见$(f_1,\ f_2)$是$\mathrm{GF}^4(2)$上二维Bent函数。

例 4　$F_{81}=\{0,1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{79}\}$，生成多项式为 $x^4+x^3+x^2+2x+2=0$，则 $F_9^\bullet=F_9\setminus\{0\}=\{1,\alpha^{10},\alpha^{20},\alpha^{30},\cdots,\alpha^{70}\}$，$H_0=F_9$，$H_1=\alpha F_9^\bullet$，$H_2=\alpha^2F_9^\bullet$，$H_3=\ \alpha^3F_9^\bullet$，$\cdots$，$H_9=\alpha^9F_9^\bullet$。如下定义函数$f_1$，$f_2$：

i	f_1	f_2
1	0	0
2	0	1
3	0	2
4	1	0
5	1	1
6	1	2
7	2	0
8	2	1
9	2	2

上述表格的意义同例 3。因为此表的右侧两列是 F_3^2 中元素的全排列，再定义 f_1 和 f_2 在 0 点及 H_0 内各点处的函数值为 0，则f_2、f_1+f_2、f_1+$2f_2$都满足定理 2 的条件，因而它们都是超Bent函数，所以 (f_1,f_2) 是F_{81}上的 2 维超Bent函数。设 $x=(x_1,x_2,x_3,x_4)\in F_3^4$，则 (f_1,f_2) 的多项式表示分别为：

$$\begin{aligned}f_1(x)=&2x_1^2+2x_1x_2+x_1x_3+2x_1x_4+2x_2x_3+x_2x_4+x_3x_4\\&+x_1^2x_3^2+x_1^2x_4^2+2x_2^2+x_3^2x_4^2x_3^2+2x_1^2x_2x_3+x_1^2x_2x_4\\&+2x_1^2x_3x_4+x_2^2x_3x_4+x_2x_3^2x_4+x_1x_3x_4^2+x_2x_3x_4^2\\&+2x_1x_2x_3x_4\\f_2(x)=&2x_1x_2+x_1x_4+2x_2x_3+2x_3x_4+x_3^2+2x_4^2+x_1^2x_4^2\\&+2x_3^2x_4^2+2x_1^2x_2x_3+2x_1^2x_2x_4+x_1^2x_3x_4+x_1x_2^2x_3\\&+2x_2^2x_3x_4+x_1x_2x_3^2+x_2x_3^2x_4+x_1x_2x_4^2+2x_1x_3x_4^2\\&+x_2x_3x_4^2\end{aligned}$$

4.3　定理 3 中所构造的多维超 Bent 函数维数的上界：

定义 4[8]　设 $f(x):Z_p^n\to Z_p$，$x\in Z_p^n$ 是 p 值逻辑函数，若存在 Z_p^m 上的 p 值逻辑函数 $g(y)$，使得对任意的 $w\in Z_p^n$，都有 $S_{(f)}(w)=p^{-\frac{n}{2}}u^{g(w)}$，则称 $f(x)$ 为正则的。

计算表明根据定理 2、定理 3 所构造的函数的 Chrestenston 循环谱形如 $p^{-m}u^k, k\in Z_p$，故这类函数是正则的广义 Bent 函数，由文献[8]中的定理 3.2 知如此构造的 $2m$ 元多维广义 Bent 函数的维数不超过 m，又关于 m 个变元平衡的多维逻辑函数维数可达到 m(m 元置换就是这样一个例子)，所以定理 3 所构造多维广义 Bent 函数的维数达到了最

高。

5 结束语

本文将特征为 2 的有限域上超Bent函数的概念推广到特征为p的有限域上，研究了 F_{2^n} 上超Bent函数与$\mathrm{GF}^{2m}(2)$上Bent函数之间的关系，给出了有限域 $F_{p^{2m}}$ 上的m维超Bent函数的两种构造方法。需要指出的是通过对我们从 4 元布尔Bent函数所找到的F_{16}上的超Bent函数的研究，我们发现还有 18 个函数(例如假设F_{16}的生成多项式是x^4+x+1，若按照F_{16}上本原元的升幂排列，函数真值表是 0 0 0 0 0 0 0 1 0 1 1 0 0 1 1 0 1 的函数)不在Kaisa和龚光等所给的超Bent函数之列，所以他们所给出的构造法并不是完全构造法。因此寻找更多超Bent函数，给出超Bent函数新的构造法是一个值得研究的课题。通过上机搜索我们发现F_{64}上不存在代数次数为 2 的超Bent函数，即F_{64}上超Bent函数的代数次数都是 3，我们所得到的F_{81}上大量的超Bent函数的代数次数也都为 4。所以有限域上超Bent函数的代数次数的取值规律也是一个值得研究的问题。

附录 F_{16}上的所有超Bent函数

$f_1(x)$	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	1	
$f_2(x)$	0	0	0	0	0	1	0	1	1	0	0	1	1	0	1	0	
$f_3(x)$	0	0	0	0	1	0	1	1	0	0	1	1	0	1	0	0	
$f_4(x)$	0	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	(*)
$f_5(x)$	0	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	(*)
$f_6(x)$	0	0	0	1	0	1	1	0	0	1	1	0	1	0	0	0	
$f_7(x)$	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	(*)
$f_8(x)$	0	0	0	1	1	0	1	0	0	0	0	0	1	0	1	1	
$f_9(x)$	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	1	
$f_{10}(x)$	0	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	(*)
$f_{11}(x)$	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	(*)
$f_{12}(x)$	0	0	1	0	1	1	0	0	1	1	0	1	0	0	0	0	
$f_{13}(x)$	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	(*)
$f_{14}(x)$	0	0	1	1	0	0	1	1	0	1	0	0	0	0	0	1	
$f_{15}(x)$	0	0	1	1	0	1	0	0	0	0	0	1	0	1	1	0	
$f_{16}(x)$	0	1	0	0	0	0	0	1	0	1	1	0	0	1	1	0	
$f_{17}(x)$	0	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	(*)
$f_{18}(x)$	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	(*)
$f_{19}(x)$	0	1	0	0	1	1	0	1	0	0	0	0	0	1	0	1	
$f_{20}(x)$	0	1	0	1	0	0	0	0	0	1	0	1	1	0	0	1	
$f_{21}(x)$	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	(*)
$f_{22}(x)$	0	1	0	1	1	0	0	1	1	0	1	0	0	0	0	0	
$f_{23}(x)$	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	(*)
$f_{24}(x)$	0	1	1	0	0	1	1	0	1	0	0	0	0	0	1	0	
$f_{25}(x)$	0	1	1	0	1	0	0	0	0	0	1	0	1	1	0	0	
$f_{26}(x)$	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	
$f_{27}(x)$	0	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	
$f_{28}(x)$	0	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	

注 1 $f(0)=0$，其它各点处函数值系按照F_{16}中元素的根表示中α 的升幂顺序排列。

注 2 带(*)者是周期为 5 的超 Bent 函数。

参 考 文 献

[1] Youssef A M and Gong G. Hyper Bent functions. Eurocrypt'2001, Innsbruck, Austria, May 2001. LNCS2045: 406–419.

[2] Gong G and Golomb S W. Tranform Domain Analysis of DES. *IEEE Trans. on Information Theroy.* 1999, 45(6): 2065–2073.

[3] Clarlet C and Caborit P. Hyper-Bent functions and cyclic codes. IEEE International Symposium on Information Theory 2004, Chicago, USA, June: 499–515.

[4] Rothous O S. On Bent functions. *Journal of Combinatorial Theory*, 1976, 20(A): 300–305.

[5] Lidl R and Niederreiter H. Finite Fields. 2nd ed, Cambridge, England: Cambridge University Press, 1997: 56–57.

[6] 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: 194–195.

[7] Dillion J F. Elementary hadamard difference sets. [Ph.D. Thesis], University of Maryland, 1974.

[8] Nyberg K. Perfect nonlinear S-boxes. Advances in Cryptology-Eurocrypt'91, Brighton, UK, April 1991, LNCS 547: 378–383.

张文英： 女，1970 年生，博士，副教授，中国科学院软件研究所在站博士后，主要研究方向为密码学.

武传坤： 男，1964 年生，研究员，博士生导师，主要研究方向为密码学和网络安全，也包括安全电子商务等.