# 多输出 bent 函数的优化设计

吴菊英[1], 韦永壮[2], 王选明[3]
(1. 空军工程大学, 陕西西安 710077; 2. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071;
3. 中国科科学院软件研究所 计算机科学重点实验室, 北京 100080)

摘 要: 本文运用密码函数输入变元的复合可逆变换, 对文[1, 2] 的多输出 bent 函数进行优化设计, 结果获得了更为丰富的新的多输出 bent 函数簇: (1) 有很大一部分不属于 Maiorana-McFarland 型 bent 函数; (2) 同样可以获得最大的代数次数和最大的输出维数; (3) 具有良好的构造计数等. 此外, 本文也说明了密码函数输入变元的复合可逆变换, 为构造具有良好密码学性质的函数, 提供了一种简洁、且易于实现的方法.

关键词: 多输出 bent 函数; 复合可逆变换; 可逆矩阵; 代数次数
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2005) 03-0521-03

## An Optimized Method for Multiple Output Bent Functions

WU Ju-ying[1], WEI Yong-zhuang[2], WANG Xuan-ming[3]
(1. *The Air Force Engineering University, Xi'an, Shaanxi 710077, China;*
2. *ISN National Key Lab., Xidian University, Xi'an, Shaanxi 710071, China;*
3. *Key Lab of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China*)

**Abstract:** Kaisa Nyberg and Takashi Satoh gave some methods for constructing multiple output bent functions in paper[1, 2] respectively, while these bent functions belong to Maiorana-McFarland bent functions. In this paper, an optimizing method for multiple output bent functions in paper[1, 2] is presented by using Cryptographic functions' input-variety compounding reversible transform. As a result, many new multiple output bent functions were obtained, and these functions have following properties: (1) they do not belong to Maiorana-McFarland bent functions; (2) they have highest algebraic degree and maximal number of output bits; (3) they also have good construction number. Moreover, it also means that compounding reversible transform is very useful for constructing good Cryptographic functions and the method is concise and easily implemented.

**Key words:** multiple-output bent functions; compounding reversible transform; reversible matrix; algebraic degree

## 1 引言

多输出布尔函数在流密码和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. 注意到, bent 函数具有抗差分攻击和抗最佳仿射逼近的能力[4], 因此自 1976 年 Rothaus[7] 首次提出后, 就受到广泛的关注, 且在密码核心部件设计中发挥重要作用: 如澳大利亚加密算法 HAVAL 中, 所运用的 5 个布尔函数均是由 bent 函数演化得来的[5]. 为此, 进一步研究多输出 bent 函数的构造对于密码部件的安全性设计是很有意义的.

关于多输出 bent 函数的构造, 目前公开的方法很少; 冯登国博士曾在其专著[4] 中指出, 构造多输出 bent 函数的有效方法仍是一个公开研究问题之一.

文献[1] kaisa Nyberg 基于 $m$ 序列中状态转移矩阵给出了多输出 bent 函数的一种构造方法, 然而这些 bent 函数均属于 Maiorana-McFarland 型 bent 函数(即 $f(x, y) = \varphi(x)y + g(x)$ 形式[1, 8]), 而 Maiorana-McFarland 型函数有着明显的缺陷[8];

文献[2] Takashi Satoh 基于置换方法, 给出了多输出 bent 函数的新的构造方法, 并且能使 bent 函数的代数次数和输出维数同时达到最大. 但是, 这些函数仍是属于 Maiorana-McFarland 型 bent 函数;

文献[3] 基于布尔函数的谱分解, 给出了 2 维 bent 函数的构造, 这些函数有些不属于 Maiorana-McFarland 型 bent 函数; 而对于更高维的非 Maiorana-McFarland 型多输出 bent 函数, 仍待进一步研究.

本文运用密码函数输入变元的复合可逆变换, 对文[1, 2] 的多输出 bent 函数进行优化设计, 结果获得了更为丰富的新的多输出 bent 函数簇: (1) 有很大一部分不属于 Maiorana-McFarland 型 bent 函数; (2) 同样可以获得最大的代数次数和最大的输出维数; (3) 具有良好的构造计数.

收稿日期: 2003-11-19; 修回日期: 2004-03-26
基金项目: ISN 国家重点实验室开放课题基金资助(No. 5—03); 国防科技重点实验室基金资助(No. 51436010201DZ0104)

## 2 基本定义及引理

定义 **1**[6] 设$f(x)$是 $n$ 元布尔函数, $a\in GF(2)^n$, 若 $f(x)+f(x+a)$是均衡函数, 则称函数$f(x)$在 $a$ 处满足扩散性准则, 若函数在每一个非零点处均满足扩散性准则, 则称这样的函数为 bent 函数.

定义 **2**[6] $(n, m)$函数 $F(x)=(F_1(x), F_2(x), \cdots, F_m(x))$称为$(n, m)$bent 函数, 如果对任意 $c=(c_1, c_2, \cdots, c_m)\in GF(2)^m$, $c\neq 0$, $\sum_{j=1}^{m}c_jF_j$ 均为 bent 函数.

引理 **1**[1] $n$ 元 Maiorana-McFarland 型函数 $f(x, y)=\varphi(x)y+g(x)$, 其中 $n$ 为偶数, $(x, y)\in GF(2)^n$; $x\in GF(2)^{n/2}$ 若 $\varphi(x)$为 $GF(2)^{n/2}$上的一个置换, 则$f(x, y)$为 bent 函数.

引理 **2**[9] $GF(2)$上的 $n$ 阶可逆方阵共有个 $\prod_{i=0}^{n-1}(2^n-2^i)$.

引理 **3**[6] 若 $n$ 元布尔函数$f(x)$是一 bent 函数, 则函数$f(x)$的输入变元经过复合可逆变化 $xA+b$, 仍得到一 bent 函数, 其中 $A$ 为一 $n$ 元可逆方阵; $x, b\in GF(2)^n$.

## 3 多数出 **bent** 函数的优化设计

### 3.1 **Kaisa Nyberg** 和 **Takashi Satoh** 构造多输出 **bent** 函数方法[1,2]:

(1)Kaisa Nyberg 的构造方法:

设$(n, m)$函数 $F(x, y)=(f_1(x, y), f_2(x, y), \cdots, f_m(x, y))$, 其中$f_i(x, y)=\pi_i(x)y+g_i(x)$ $(i=1, \cdots, m)$; $(x, y)\in GF(2)^n$; $x\in GF(2)^{n/2}$; $n$ 为偶数; $\pi_i$ 均为$GF(2)^{n/2}$上的置换. 若$\pi_i$的任意非零线性组合, 仍为 $GF(2)^{n/2}$上的置换, $(i=1, \cdots, m)$则$(n, m)$函数 $F(x, y)$为$(n, m)$bent 函数. 为了获得以上的置换$\pi_i$ $(i=1, \cdots, m)$, Kaisa Nyberg 采用 $n/2$ 长反馈移位寄存器, 生成一 $m$ 序列, 并取 $m$ 序列中不同的转移状态(状态转移矩阵)作为以上的置换簇. 这样就得到了一种构造$(n, m)$bent 函数的方法.

(2)Takashi Satoh 的构造方法:

设 $n$ 为偶数, $m=n/2$, $x=(x_1, x_2, \cdots, x_m)\in GF(2)^m$, $y=(y_1, y_2, \cdots, y_m)\in GF(2)^m$, $\alpha$ 为 $GF(2^{n/2})$的本原元; 则函数 $F(x, y)=(f_1(x, y), f_2(x, y), \cdots, f_m(x, y))$为$(n, m)$bent 函数, 且可以获得最大的代数次数和输出维数(均为 $m=n/2$), 其中$f_i(x, y)=[\varphi_i(x)]y+g_i(x)$; 这里 $\varphi_i(x)\triangleq\begin{cases}0, & x=0, \cdots, 0\\ \alpha^{dec(x)+i-1}, & x\neq(0, 0, \cdots, 0)\end{cases}$, $g_i(x)$是任意一个 $n/2$ 元布尔函数. (注: 对于任意 $x=(x_1, x_2, \cdots, x_m)\in GF(2)^m$, $dec(x)=2^{m-1}x_1+2^{m-2}x_2+\cdots+x_m$; 对于任意 $\beta\in GF(2)^m$, $[\beta]$表示元素 $\beta$ 的 $m$ 长比特向量). 这样 Takashi Satoh 给出了另一种构造$(n, m)$bent 函数的方法.

然而, 值得我们注意的是:

(1)Kaisa Nyberg 的构造方法是在 $GF(2)^{n/2}$上找置换簇; 而Takashi Satoh 的构造方法是在 $GF(2^{n/2})$ 上找置换簇. 前者采用 $m$ 序列中不同的转移状态作为置换簇 $\pi_i$ 的基础, 而后者采用 $GF(2^{n/2})$的本原元作为置换簇的基础, 实际上也可看作是 $m$ 序列的不同转移状态的另一种表示. 所以这两种构造置换的方法, 本质是一体的.

(2)此外, 我们也注意到这两种构造方法, 得到的函数均是 Maiorana-McFarland 型 bent 函数, 而这些函数明显的一个缺陷[8]是: $f(x, y)=\varphi(x)y+g(x)$ 中取定 $x$, 函数退化为线性函数, 同时函数的最大代数次数仅和 $g(x)$ 有关, 变元 $y$ 并不参与作用.

### 3.2 运用函数输入变元的复合可逆变换, 对文献[1, 2]的多输出 **bent** 函数进行优化

定理 **1** 若$(n, m)$函数 $F(x, y)=(f_1(x, y), f_2(x, y), \cdots, f_m(x, y))$为一个$(n, m)$bent 函数, 则 $G(x, y)=F[(x, y)A+b]$仍为$(n, m)$bent 函数, 其中 $A$ 为一 $n$ 元可逆方阵; $b\in GF(2)^n$.

证明: 由定义 2 可知对任意 $c=(c_1, c_2, \cdots, c_m)\in GF(2)^m$, $c\neq 0$, $\sum_{j=1}^{m}c_jf_j(x, y)$均为 bent 函数, 再由引理 3 的结论可知 $\sum_{j=1}^{m}c_jf_j(x, y)$的输入变元经过复合可逆变化$(x, y)A+b$, 仍得到一 bent 函数. 即 $G(x, y)=F[(x, y)A+b]$仍为$(n, m)$bent 函数.

推论 **1** 给定任意的一个$(n, m)$bent 函数, 其输入变元经过复合可逆变换 $xA+b$, 可得到 $2^n\sum_{i=0}^{n-1}(2^n-2^i)-1$ 个新的$(n, m)$bent 函数.

推论 **2** 若$(n, m)$bent 函数具有最大的输出维数(即 $m=n/2$)和最大的代数次数, 则其输入变元经过适当的复合可逆变换, 同样可获得最大的输出维数和最大的代数次数.

定理 **2** 函数$f(x, y)=xy+g(x)$为一个 $n$ 元 Maiorana-McFarland 型 bent 函数, 若函数$f(x, y)$满足以下条件之一: (1)若 $g(x)$的代数次数大于2, 且不含有二次项; (2)若 $g(x)$的代数次数大于 2, 且不含有某一变元 $x^*$; (3)若 $g(x)$的二次项中不含有某一变元 $x^*$; 则其输入变元经过适当的复合可逆变换, 可以获得非 Maiorana-McFarland 型 bent 函数.

证明: (1)取定可逆阵 $A=\begin{pmatrix}A_1 & A_2\\ B_1 & B_2\end{pmatrix}_{n\times n}$, 其中 $A_2$ 为全零阵, $A_1$, $B_2$ 均为 $n/2$ 阶单位阵, $B_1$ 为非零阵, 且其主对角线及以下的元素全为 0, 即 $B_1=\begin{pmatrix}0 & * & *\\ 0 & \ddots & *\\ 0 & 0 & 0\end{pmatrix}_{(n/2)\times(n/2)}$, 进一步的, 其输入变元经过复合可逆变换 $G(x, y)=f[(x, y)A]$, 由于 $g(x)$的代数次数大于 2, 且不含有二次项; 则总可写成形式: $f[(x, y)A]=\Phi(x)y+g_1(x)+g_2(y)$, 其中 $g_1(x)$, $g_2(y)$, 的代数次数都大于或等于 2, $\Phi(x)$为 $x$ 的一个变换; 不难知道 $G(x, y)$并不是 Maiorana-McFarland 型 bent 函数. (2)由于 $g(x)$的代数次数大于 2, 且不含有某一变元 $x^*$ (设为第 $i$ 个分量); 取(1)中的阵 $B_1$ 其第 $i$ 行 1 列的元素为 1, 其余的均为零则总可写成形式 $G(x, y)=\Phi(x)y+g_1(x)+g_2(y)$. 其中

$g_1(x)$, $g_2(y)$ 的代数次数都大于或等于 2, 即 $G(x, y)$ 为非 Maioranar McFarland 型 bent 函数. (3) 的证明方法和(2) 相同.

更一般的, 对于 $f(x, y) = \pi(x)y + g(x)$ Maioranar McFarland 型 bent 函数, 可采用类似的方法进行优化, 可以得到更为丰富的非 Maioranar McFarland 型 bent 函数.

推论 **3**　文献[1, 2]的 Maioranar McFarland 型$(n, m)$ bent 函数, 其分量函数经过复合可逆变换, 可以获得非 Maioranar McFarland 型$(n, m)$ bent 函数.

下面给出一个例子.

例　对 6 元 Maioranar McFarland 型$(6, 2)$ bent 函数优化, 其中 $F(x_1, x_2, x_3, y_1, y_2, y_3) = (f_1(x, y), f_2(x, y))$; $f_1(x, y) = x_1y_1 + x_2y_2 + x_3y_3 + x_1x_3$; $f_2(x, y) = (x_1 + x_3)y_1 + x_1y_2 + x_2y_3 + x_1x_2x_3$, 取定 $B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, 则 $f_1((x, y)A) = x_1y_1 + x_2y_2 + x_3y_3 + x_1x_3 + y_1y_3$; $f_2((x, y)A) = (x_1 + x_3 + x_1x_3)y_1 + x_1y_2 + x_2y_3 + x_1x_2x_3 + y_1y_3$, 即 $G(x, y) = F((x, y)A) = F((x, y)A)$ 为一个非 Maioranar McFarland 型$(6, 2)$ bent 函数.

由此, 我们得到了多输出 bent 函数的一种实用优化方法.

## 4　总结

本文运用密码函数输入变元的复合可逆变换, 对文献[1, 2] 的多输出 bent 函数进行优化设计, 结果获得了更为丰富的新的多输出 bent 函数簇: (1) 有很大一部分不属于 Maioranar McFarland 型 bent 函数; (2) 也可以同时获得最大的代数次数和最大的输出维数; (3) 具有良好的构造计数等. 此外, 本文也说明了对密码函数输入变元的复合可逆变换, 为构造具有良好密码学性质的函数, 提供了一种简洁、且易于实现的优化方法.

参考文献:


[1] KNyberg. Perfect Nonlinear S-boxes[A]. In Advances in Cryptology Eurocrypt' 91[C]. Berlin: Springer-Verlag, 1992. 378- 383.

[2] T Satoh, T Iwata and Kaoru K. On Cryptographically Secure Victoria Boolean functions. Proc of Asiacrypt' 99, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1999. (1716): 20- 28.

[3] 张文英, 滕吉红, 李世取. 布尔函数的谱分解式及其在 k 维 bent 函数构造中的应用[A]. 第三届中国信息和通信安全学术安全会议论文集-CCICS' 2003[C]. 北京: 北京科学出版社, 2003. 290 - 296.

[4] 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.

[5] Zheng Y L, J Pieprzyk, J Seberry. HAVAL A One Way Hashing Algorithm with Variable Length Output [A]. Advances in Cryptology AUSCRYPT' 92[C]. Australia, 1993, (718): 280- 291.

[6] 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, 3, 16- 62.

[7] O S Rothaus. On Bent Functions[J]. Journal of Combine theory, 1976, (20): 300- 305.

[8] C Carlet. A Larger Class of Cryptographic Boolean Functions Via a Study of the Maioranar McFarland Construction [A]. CRYPTO2002 [C]. Berlin, 2002. 549- 564.

[9] 曾祥勇, 张焕国, 王丽娜. AES S 盒的设计分析[A]. 第三届中国信息和通信安全学术安全会议论文集 CCICS' 2003[C]. 北京: 科学出版社, 2003. 186- 193.


作者简介:


吴菊英　女, 1964 年 3 月出生于陕西乾县, 1986 年 7 月西北大学获得理学学士学位, 现为中国人民解放军空军工程大学, 讲师, 主要研究领域: 代数与编码密码学.



韦永壮　男, 1976 年 12 月出生于广西田阳县, 2000 年 7 月广西民族大学获得理学学士, 现为西安电子科技大学密码学专业 2001 级硕士研究生, 主要研究方向: 密码函数安全性设计、分组密码、流密码.