具有偶数个变元的高非线性度平衡布尔函数的构造

张卫国[1,2],肖国镇[1,2]
(1.西安电子科技大学 ISN 国家重点实验室,陕西西安 710071; 2.保密通信重点实验室,四川成都 610041)

摘 要: 通过修改 Maiorana-McFarland 型 bent 函数,构造出具有偶数个变元的高非线性度平衡布尔函数.并对具有偶数个变元的平衡布尔函数的非线性度上界提出一个猜想.

关键词: 密码学; 布尔函数; 平衡; 非线性度
中图分类号: TN918.1; TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 03-0727-02

Construction of Balanced Boolean Functions with High Nonlinearity on Even Number Variables

ZHANG Wei-guo[1,2], XIAO Guo-zhen[1,2]
(1. *ISN Laboratory, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan* 610041, *China*)

Abstract: A technique for constructing highly nonlinear balanced functions is described. It is shown that a balanced Boolean function with high nonlinearity on even number of variables can be obtained via modifying Maiorana-McFarland type bent functions. A conjecture about the upper bound of the nonlinearity of a balanced Boolean function on even number variables is given.

Key words: cryptography; Boolean function; balance; nonlinearity

1 引言和预备知识

众所周知,Bent 函数的非线性度达到最优,但却不是平衡布尔函数[1].具有高非线性度的平衡布尔函数的构造是密码学和序列设计中的重要课题[2,3].

设 F_2 表示具有两个元素的有限域. n 元布尔函数是从 F_2^n 到 F_2 的映射.用 B_n 表示 n 元布尔函数的集合.用 $\oplus$ 表示 F_2 上的加法.设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$, $f(\boldsymbol{x})\in B_n$ 通常用其代数正规型表示:

$$f(x)=\bigoplus_{u\in F_2^n}\lambda_u\left(\prod_{i=1}^{n}x_i^{u_i}\right)$$

其中 $\lambda_u\in F_2$, $u=(u_1,\cdots,u_n)$. $f(\boldsymbol{x})$ 的代数次数,用 $\deg(f)$ 表示,是使 $\lambda_u\neq 0$ 的 u 的最大汉明重量 $wt(u)$.向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ 和 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 在 F_2^n 上的点乘运算定义为:

$$\boldsymbol{a}\cdot\boldsymbol{x}=a_1x_1\oplus a_2x_2\oplus\cdots\oplus a_nx_n.$$

$f(\boldsymbol{x})$ 在 ω 点的 Walsh 变换用 $W_f(\omega)$ 表示,计算如下:

$$W_f(\omega)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus\boldsymbol{a}\cdot\boldsymbol{x}}.$$

若 $f(x)$ 真值表输出列中 0 和 1 的个数相同,即 $W_f(0)=0$,则称 $f(\boldsymbol{x})$ 是平衡的. $f(\boldsymbol{x})$ 的非线性度 N_f 可由以下公式计算: $N_f=2^{n-1}-1/2\cdot\max\limits_{\omega\in F_2^n}|W_f(\omega)|$.

2 构造及性质分析

Maiorana-McFarland 类 n 元 Bent 函数是通过毗连 $2^{n/2}$ 个不同的 $n/2$ 元线性函数得到[4].下面我们通过修改 Maiorana-McFarland 类 Bent 函数,构造高非线性度的平衡布尔函数.

设 $\boldsymbol{a},\boldsymbol{b}\in F_2^n$.符号 a^b 定义为

$$a^b=\begin{cases}1, & \boldsymbol{a}=\boldsymbol{b}\\ 0, & \boldsymbol{a}\neq\boldsymbol{b}\end{cases}$$

构造:设正整数 $n\geqslant 8$ 且 $n\equiv 0\pmod 4$, ϕ 是从 $F_2^{n/2}$ 到 $F_2^{n/2}$ 的双射.向量 $\boldsymbol{\delta}\in F_2^{n/2}$ 满足 $\phi(\boldsymbol{\delta})=(\theta_1,\cdots,\theta_{n/2})\neq\boldsymbol{0}$,其中 $wt((\theta_1,\cdots,\theta_{n/4+1}))\equiv 0\pmod 2$, $(\theta_{n/4+2},\cdots,\theta_{n/2})=\boldsymbol{0}$.设 Ψ 是任意从 $F_2^{n/4}$ 到 $F_2^{n/4}$ 的双射.对 $(\boldsymbol{y},\boldsymbol{x})\in F_2^{n/2}\times F_2^{n/2}$,其中 $\boldsymbol{x}=(x_1,x_2,\cdots,x_{n/2})$,构造函数 $f\in B_n$:

$$f(\boldsymbol{y},\boldsymbol{x})=\bigoplus_{b\in F_2^{n/2}}y^b\cdot g_b(\boldsymbol{x})$$

其中

收稿日期:2010-03-03;修回日期:2010-11-10
基金项目:国家自然科学基金(No.61003299);保密通信重点实验室项目(No.9140C1103031002);111 计划 (No. B08038);中央高校基本科研业务费专项资金项目

$$g_b(\boldsymbol{x}) = \begin{cases} \phi(\boldsymbol{b})\cdot\boldsymbol{x}, & \boldsymbol{b}\notin\{\boldsymbol{\delta},\phi^{-1}(0)\} \\ \phi(\boldsymbol{\delta})\cdot\boldsymbol{x} + x_1x_2\cdots x_{n/4+1}, & \boldsymbol{b}=\boldsymbol{\delta} \\ \Psi((x_1x_2\cdots x_{n/4}))\cdot(x_{n/4+1}x_{n/4+2}\cdots x_{n/2}), & \boldsymbol{b}=\phi^{-1}(0) \end{cases}$$

定理　由上述构造方案得到的布尔函数 $f\in B_n$ 具有以下性质：

(1) f 是平衡的；

(2) $N_f = 2^{n-1} - 2^{n/2-1} - 2^{n/4}$；

(3) $\deg(f) = 3n/4 + 1$.

证明　当 $\boldsymbol{b}\notin\{\boldsymbol{\delta},\phi^{-1}(0)\}$ 时，有

$$W_{g_b}(\alpha) = \begin{cases} 2^{n/2}, & \alpha = \phi(\boldsymbol{b}) \\ 0, & \alpha \neq \phi(\boldsymbol{b}) \end{cases}$$

当 $\boldsymbol{b}=\boldsymbol{\delta}$ 时，设 $\alpha = (\alpha_1,\alpha_2,\cdots,\alpha_{n/2})$，有

$$W_{g_b}(\alpha) = \begin{cases} 2^{n/2} - 2^{n/4}, & \alpha = \phi(\boldsymbol{\delta}) \\ \pm 2^{n/4}, & (\alpha_1,\cdots,\alpha_{n/4+1}) \neq (\theta_1,\cdots,\theta_{n/4+1}), \\ & (\alpha_{n/4+2},\cdots,\alpha_{n/2}) = (\theta_{n/4+2},\cdots,\theta_{n/2}) \\ 0, & (\alpha_{n/4+2},\cdots,\alpha_{n/2}) = (\theta_{n/4+2},\cdots,\theta_{n/2}) \end{cases}$$

且有　$W_{g_b}(0) = (-1)^{wt(\phi(\boldsymbol{\delta}))+1}\cdot 2^{n/4} = -2^{n/4}$.

当 $\boldsymbol{b} = \phi^{-1}(0)$ 时，

$$W_{g_b}(\alpha) = \pm 2^{n/4}$$

且有　$W_{g_b}(0) = 2^{n/4}$.

对任意 $(\beta,\alpha)\in F_2^{n/2}\times F_2^{n/2}$，有如下关系：

$$\begin{aligned} W_f(\beta,\alpha) &= \sum_{(y,x)\in F_2^n} (-1)^{f(\boldsymbol{y},\boldsymbol{x}) + (\beta,\alpha)\cdot(\boldsymbol{y},\boldsymbol{x})} \\ &= \sum_{b\in F_2^{n/2}} (-1)^{\beta\cdot\boldsymbol{b}} \sum_{x\in F_2^{n/2}} (-1)^{g_b(\boldsymbol{x}) + \boldsymbol{\alpha}\cdot\boldsymbol{x}} \\ &= \sum_{\boldsymbol{b}\in F_2^{n/2}} (-1)^{\beta\cdot b} W_{g_b}(\alpha) \end{aligned}$$

易得　$W_f(0) = \sum_{\boldsymbol{b}\in F_2^{n/2}} W_{g_b}(0) = 0$.

进一步可得，当 $\alpha = \phi(\boldsymbol{\delta})$，

$$W_f(\beta,\alpha) \in \{2^{n/2}, 2^{n/2} - 2^{n/4+1}\};$$

当 $(\alpha_1,\cdots,\alpha_{n/4+1}) \neq (\theta_1,\cdots,\theta_{n/4+1})$，$(\alpha_{n/4+2},\cdots,\alpha_{n/2}) = (\theta_{n/4+2},\cdots,\theta_{n/2})$，

$$W_f(\beta,\alpha) \in \{0, \pm 2^{n/2}, \pm 2^{n/4+1}, \pm(2^{n/2} + 2^{n/4+1}), \pm(2^{n/2} - 2^{n/4+1})\};$$

当 $(\alpha_{n/4+2},\cdots,\alpha_{n/2}) \neq (\theta_{n/4+2},\cdots,\theta_{n/2})$，

$$W_f(\beta,\alpha) \in \{\pm(2^{n/2} + 2^{n/4+1}), \pm(2^{n/2} - 2^{n/4+1})\}.$$

显然，

$$\max_{(\beta,\alpha)\in F_2^n} |W_f(\beta,\alpha)| = 2^{n/2} + 2^{n/4+1}.$$

可得 $N_f = 2^{n-1} - 2^{n/2-1} - 2^{n/4}$.

设 $\boldsymbol{y} = (y_1,y_2,\cdots,y_{n/2})$. 显然 $y_1y_2\cdots y_{n/2}x_1x_2\cdots x_{n/4+1}$ 必定出现在 f 的代数正规型中，且不会有更高次项出现. 可得　$\deg(f) = 3n/4 + 1$.

另外要说明：(1) 当 $n = 8$ 时，可以构造出非线性度是 116，代数次数是 7 的 8 元平衡布尔函数；(2) 可以对文中的方法进行简单修改使代数次数达到最优.

3　结束语

关于具有偶数个变元的高非线性度平衡布尔函数的构造，目前最好的结果是 Seberry 等人[5]给出的，他们构造的函数也是通过修改 Maiorana-McFarland 类 bent 函数得到的，这种方法得到的函数具有潜在的密码学弱点，工程实践中应谨慎使用.

平衡布尔函数的非线性度的紧上界至今仍是公开的难题. 我们提出如下猜想：当 n 为不小于 12 的偶数时，n 元平衡布尔函数 f 的非线性度上界是

$$N_f \leqslant 2^{n-1} - 2^{n/2-1} - 2^{\lfloor n/4\rfloor - 1}$$

参考文献

[1] Rothaus O S. On 'bent' functions[J]. Journal of Combinatorial Theory, Series A, 1976, 20(3): 300 – 305.

[2] Golomb S W, Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar[M]. Cambridge, U K: Cambridge University Press, 2005.

[3] Zhang W G, Xiao G Z. Constructions of almost optimal resilient Boolean functions on large even number of variables[J]. IEEE Transactions on Information Theory, 2009, 55(12): 5822 – 5831.

[4] Dillon J F. Elementary Hadamard Difference Set[D]. Maryland: University of Maryland, College Park, 1974.

[5] Seberry J, Zhang X M, Zheng Y. Nonlinearly balanced Boolean functions and their propagation characteristics[A]. Advances in Cryptology-CRYPTO' 93, Lecture Notes in Computer Science[C]. Berlin, Germany: Springer-Verlag, 1994. 49 – 60.

作者简介

张卫国　男，山东人，博士，副教授，研究方向为对称密码学中的布尔函数.

E-mail: weiguozhang@vip.qq.com

肖国镇　男，吉林人，教授，博士生导师，研究方向为信息论，编码理论和密码学.