构造具有良好密码学性质的旋转对称布尔函数

熊晓雯* 魏爱国 张智军
(军事交通学院汽车指挥系 天津 300161)

摘 要：该文提出构造具有良好密码学性质的 2^m 元旋转对称布尔函数的新方法。该类函数是平衡的，具有最大代数免疫度、最优代数次数和高非线性度，是一类能够同时满足多种密码学指标的优良函数。

关键词：密码学；布尔函数；旋转对称；代数免疫度
中图分类号：TN918 **文献标识码**： A **文章编号**：1009-5896(2012)10-2358-05
DOI: 10.3724/SP.J.1146.2012.00329

Construction of Rotation Symmetric Boolean Functions with Good Cryptographic Properties

Xiong Xiao-wen Wei Ai-guo Zhang Zhi-jun
(*Automobile Transportation Command Department*, *Military Transportation University*, *Tianjin* 300161, *China*)

Abstract: In this paper, a new class of rotation symmetric Boolean functions with good cryptographic properties are constructed when the number of variables is 2^m. These constructed functions are balanced, and have maximum algebraic immunity, optimum algebraic degree and high nonlinearity. They are excellent functions which can satisfy many cryptographic indexes simultaneously.

Key words: Cryptography; Boolean functions; Rotation symmetry; Algebraic Immunity (AI)

1 引言

代数攻击作为一种新的攻击方式，自提出后就一直受到密码学界的高度关注[1]。代数攻击的提出与发展为布尔函数提供了一个新的密码学指标：代数免疫度(Algebraic Immunity, AI)[2,3]。构造高代数免疫度尤其是最大代数免疫度的布尔函数受到了人们的关注，涌现了许多方法[4–9]。除此之外，其它密码学性质，比如代数次数和非线性度等等，在构造布尔函数时也是需要考虑的因素。

旋转对称布尔函数(Rotation Symmetric Boolean Function, RSBF)是指在循环群 C_n 的作用下保持不变的一类函数[10]。目前，这类函数因其良好的密码学性质，受到了越来越多的关注[11–13]。文献[14]首先提出了一种构造具有最大代数免疫度的奇数元旋转对称布尔函数的理论性构造方法。基于类似的构造思想，文献[15]又提出了另一种构造方法。但是已有的构造方法并没有针对偶数元函数的，直到文献[16]给出了构造平衡的 2^m 元旋转对称布尔函数的方法，这类函数具有最大代数免疫度和高非线性度，但是其代数次数并没有讨论。

本文正是在此方向上进行的一些研究工作，提出了构造具有良好密码学性质的 2^m 元旋转对称布尔函数的新方法。该类函数是平衡的，具有最大代数免疫度、最优代数次数和高非线性度，是一类能够同时满足多种密码学指标的优良函数。文章的结构如下：第 2 节给出了关于布尔函数和旋转对称布尔函数的基本概念和相关性质，第 3 节提出了新的构造方法，第 4 节总结本文。

2 预备知识

设 F_2 是二元域，F_2^n 是 F_2 上的 n 维向量空间，一个 n 元布尔函数 f 是从 F_2^n 到 F_2 上的一个映射。n 元布尔函数全体记作 B_n。一个 n 元布尔函数 f 可以唯一地表示为

$$\begin{aligned} f(x_1,\cdots,x_n) = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1\le i<j\le n} a_{i,j} x_i x_j + \cdots \\ + \sum_{1\le i_1<\cdots<i_d\le n} a_{i_1,\cdots,i_d} x_{i_1}\cdots x_{i_d} + \cdots \\ + a_{1,\cdots,n} x_1 x_2 \cdots x_n \end{aligned} \tag{1}$$

其中 $a_0, a_i, a_{i,j}, \cdots, a_{1,\cdots,n} \in F_2$。$f$ 的这种表示形式称之为 f 的代数正规型(ANF)，其系数非零项所含有的最多变元个数称为代数次数，记为 $\deg(f)$。

F_2^n 中向量 $\boldsymbol{x} = [x_1, x_2, \cdots, x_n]$ 的支撑集定义为 $\mathrm{supp}(\boldsymbol{x}) = \{i \,|\, x_i = 1\}$，支撑集 $\mathrm{supp}(\boldsymbol{x})$ 中所含的元素个数称为 $\boldsymbol{x}$ 的 Hamming 重量，记为 $wt(\boldsymbol{x})$。n 元布尔函数 f 的支撑集定义为 $\mathrm{supp}(f) = \{\boldsymbol{x} \in F_2^n \,|\, f(\boldsymbol{x})$

2012-03-27 收到，2012-06-06 改回
*通信作者：熊晓雯 winnie101206@126.com

$=1\}$。支撑集 $\mathrm{supp}(f)$ 所含的元素个数称为 f 的 Hamming 重量，记为 $wt(f)$。若 $wt(f)=2^{n-1}$，则称 n 元布尔函数 f 是平衡的。对给定的布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{\alpha}\in F_2^n$，令 $W_f(\boldsymbol{\alpha})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{f(\boldsymbol{x})\oplus\boldsymbol{x}\cdot\boldsymbol{\alpha}}$，则 $W_f(\boldsymbol{\alpha})$ 称为函数 $f(\boldsymbol{x})$ 在点 $\boldsymbol{\alpha}$ 的 Walsh 变换。布尔函数 f 的非线性度 $NL(f)$ 定义为

$$NL(f)=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{\alpha}\in F_2^n}|W_f(\boldsymbol{\alpha})|$$

对 $f\in \mathrm{B}_n$，f 的零化子为集合 $AN(f)=\{g\in \mathrm{B}_n \mid f\cdot g=0\}$。那么 f 的代数免疫度定义为

$$\mathrm{AI}(f)=\min\{\deg(g)\mid 0\neq g\in AN(f)\cup AN(1+f)=(f+1)\cup(f)\} \tag{2}$$

可以证明：如果 f 是一个 n 元布尔函数，那么 $\mathrm{AI}(f)\le\lceil n/2\rceil$[1]。当 n 元布尔函数满足 $\mathrm{AI}(f)=\lceil n/2\rceil$ 时，我们就说该函数具有最大代数免疫度。

定义 1　设 $f\in \mathrm{B}_n,\boldsymbol{x}=[x_1,x_2,\cdots,x_n]\in F_2^n,1\le i\le n$，如果对任给的 $0\le k\le n-1$ 总有下式成立：$f(\rho_n^k(x_1,\cdots,x_n))=f(x_1,\cdots,x_n)$，其中

$$\rho_n^k(x_i)=\begin{cases}x_{i-k}, & i>k\\ x_{i+n-k}, & i\le k\end{cases}$$

那么就称 $f(x_1,x_2,\cdots,x_n)$ 为旋转对称布尔函数。

注意到，一个 n 元布尔函数有 2^n 个不同的输入值。定义

$$G_n(x_1,\cdots,x_n)=\{\rho_n^k(x_1,\cdots,x_n)\mid 0\le k\le n-1\} \tag{3}$$

也就是向量 $[x_1,\cdots,x_n]$ 在 ρ_n^k 变换下的轨道。显然不同的 G_n 构成了集合 F_2^n 的一个划分。如果 f 是一个旋转对称布尔函数，那么对于属于同一轨道的任意向量，f 在该点的 Walsh 变换谱值是相同的，也就是说，若 $\boldsymbol{v}\in G_n(\boldsymbol{u})$，则 $W_f(\boldsymbol{u})=W_f(\boldsymbol{v})$[13]。

次数为 i 的 Krawtchouk 多项式定义为 $K_i(k,n)=\sum_{j=0}^{i}(-1)^j\binom{k}{j}\binom{n-k}{i-j}$。取定一个 $\boldsymbol{w}$，使得 $wt(\boldsymbol{w})=k$，那么有 $\sum_{wt(\boldsymbol{x})=i}(-1)^{\boldsymbol{w}\cdot\boldsymbol{x}}=K_i(k,n)$。下面两个引理是关于 Krawtchouk 多项式 $K_i(k,n)$ 的一些已知的相关性质。

引理 1[4]　对于 Krawtchouk 多项式，有下面的性质：

(1) $\binom{n}{k}K_i(k,n)=\binom{n}{i}K_k(i,n)$；

(2)当 n 为偶数时，

$$K_i(n/2,n)=\begin{cases}0, & i\text{是奇数}\\ (-1)^{i/2}\binom{n/2}{i/2}, & i\text{是偶数}\end{cases} \tag{4}$$

(3) $K_0(k,n)=1,\ K_1(k,n)=n-2k$；

(4)对任意的 $0\le r\le n$ 和 $n,\ k\ge 1$，等式 $\sum_{i=0}^{r}K_i(k,n)=K_r(k-1,n-1)$ 总是成立的。

引理 2[4]　设 n 是偶数，那么对任意的 $1\le k\le n-2$，总有 $|K_{n/2-1}(k,n-1)|\le\frac{1}{n-1}\binom{n-1}{n/2}$ 成立。

3　构造具有良好密码学性质的旋转对称布尔函数

在这一节，我们要研究平衡的 2^m 元旋转对称布尔函数。记 $n=2^m$，对任给的 $\boldsymbol{u}\in F_2^n$，显然有 $|G_n(\boldsymbol{u})|$ 的值等于 2 的幂次。如果 $|G_n(\boldsymbol{u})|=2^i$，那么我们就称 $G_n(\boldsymbol{u})$ 是一个 2^i-轨道。记重量为 $n/2$ 的所有 2^i-轨道的集合为 Ω_i，且 $h_i=|\Omega_i|$，那么关于 h_i 有下面的一些结论。

引理 3[16]　当 $2\le i\le m$ 时，

$$h_i=\frac{1}{2^i}\left(\binom{2^i}{2^{i-1}}-\binom{2^{i-1}}{2^{i-2}}\right)$$

引理 4[16]　当 $i\ge 3$ 时，有 $4\mid h_i$ 成立。

若一个函数的次数小于 k，并且它在一个维数不小于 k 的平面上的某点取值为零，如果它不是这个平面上的一个向量，那么它就一定在整个平面上取值为零。Carlet 把上述思想应用在布尔函数 f 和 $f+1$ 的零化子上，于是得到了下面的结论。

引理 5[5]　设 k 是满足 $k\le\lceil n/2\rceil$ 的任意正整数，一个布尔函数 f 不存在代数次数严格小于 k 的非零零化子的充分条件是，存在一个平面序列 $(A_i)_{1\le i\le r}$，其中 A_i 的维数至少为 k，使得

$$\left.\begin{array}{l}\forall i\le r,\left|A_i\setminus\left[\bigcup_{i^*<i}A_{i^*}\bigcup\mathrm{supp}(f)\right]\right|\le 1\\ F_2^n\setminus\mathrm{supp}(f)\subseteq\bigcup_{i\le r}A_i\end{array}\right\} \tag{5}$$

这一节的主要目的就是利用引理 5 来构造具有最大代数免疫度、最优代数次数和较高非线性度的平衡的旋转对称布尔函数，下面就给出我们的构造。

构造方法 1

第 1 步　令 $n=2^m(m\ge 3)$；

第 2 步　构造集合 B,C,D 如下：$B=G_n(1,0,1,0,\cdots,1,0)$，$C=G_n(1,1,\cdots,1)$，$D$ 中的元素是由 Ω_3 中的一半元素，Ω_4 中的一半元素，$\cdots,\Omega_m$ 中的一半元素所构成的，并且满足对任取的 $\boldsymbol{x}\in D$，都有 $\overline{\boldsymbol{x}}\in D$（引理 3 确保了集合 D 的存在性）；

第 3 步　构造旋转对称布尔函数

$$f(\boldsymbol{x})=\begin{cases}0, & \boldsymbol{x}\in B\cup C\cup D\cup\{\boldsymbol{x}\mid wt(\boldsymbol{x})<n/2\}\\ 1, & \text{其它}\end{cases} \tag{6}$$

在证明 $\mathrm{AI}(f)=n/2$ 之前，需要引入如下的一些记号：$E=G_n(1,1,0,0,\cdots,1,1,0,0)$，$W^{n/2}=\{\boldsymbol{x}\in F_2^n \mid wt(\boldsymbol{x})=n/2\}$，$W^{>n/2}=\{\boldsymbol{x}\in F_2^n \mid wt(\boldsymbol{x})>n/2\}$，$W^{<n/2}=\{\boldsymbol{x}\in F_2^n \mid wt(\boldsymbol{x})<n/2\}$。令 $D_2=W^{n/2}\setminus[B\cup D\cup E]$，那么有 $|D_2|=|D|$。

定理 1 构造方法 1 中所构造的函数 f 是具有最大代数免疫度的平衡的旋转对称布尔函数。

证明 注意到 $|G_n(1,0,\cdots,1,0)|+|G_n(1,1,\cdots,1,1)|=3$，那么由引理 3 有

$$|B+C+D|=3+\frac{1}{2}\sum_{i=3}^{m}h_i\cdot 2^i=3+\frac{1}{2}\left[\binom{n}{n/2}-\binom{2^{3-1}}{2^{3-2}}\right]=\frac{1}{2}\binom{n}{n/2} \quad (7)$$

这也就说明了 f 是平衡的。

显然有 $\sum_{k=0}^{n/2}\binom{n}{k}=\sum_{i=n/2}^{n}\binom{n}{k}$，我们记这个值为 M。设 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_M$ 是由 F_2^n 中重量至少为 $n/2$ 的全部向量所组成的一个有顺序的集合，这个顺序就是指按重量的大小升序排列(重量相同的向量可以任意排列)。定义 $A_i=\{\boldsymbol{x}\in F_2^n \mid \mathrm{supp}(\boldsymbol{x})\subseteq\mathrm{supp}(\boldsymbol{a}_i)\}$，那么当 $1\le i\le\binom{n}{n/2}$ 时，有

$$\left.\begin{aligned}A_i\setminus\left[\bigcup_{i^*<i}A_{i^*}\bigcup\mathrm{supp}(f+1)\right]x=\{\boldsymbol{a}_i\},\ \boldsymbol{a}_i\notin B\cup D\\ A_i\setminus\left[\bigcup_{i^*<i}A_{i^*}\bigcup\mathrm{supp}(f+1)\right]=\varnothing,\qquad \boldsymbol{a}_i\in B\cup D\end{aligned}\right\} \quad (8)$$

当 $\binom{n}{n/2}<i<M$ 时，有 $A_i\setminus\left[\bigcup_{i^*<i}A_{i^*}\bigcup\mathrm{supp}(f+1)\right]=\{\boldsymbol{a}_i\}$；当 $i=M$ 时，有 $A_i\setminus\left[\bigcup_{i^*<i}A_{i^*}\bigcup\mathrm{supp}(f)\right]=\varnothing$。

于是由引理 5 可知，$f+1$ 没有次数小于 $n/2$ 的非零零化子。

类似地，设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_M$ 是由 F_2^n 中重量至多为 $n/2$ 的全部向量所组成的一个有顺序的集合，这个顺序就是指按重量的大小降序排列(重量相同的向量可以任意排列)。定义 $A_i'=\{\boldsymbol{x}\in F_2^n \mid \mathrm{supp}(\boldsymbol{b}_i)\subseteq\mathrm{supp}(\boldsymbol{x})\}$，设 $\boldsymbol{b}_1\in D_2\cup E$，那么有 $A_1'\setminus\mathrm{supp}(f)=(1,1,\cdots,1,1)$；当 $2\le i\le\binom{n}{n/2}$ 时，有

$$\left.\begin{aligned}A_i'\setminus\left[\bigcup_{i^*<i}A_{i^*}'\bigcup\mathrm{supp}(f)\right]=\varnothing,\quad \boldsymbol{b}_i\notin B\cup D\\ A_i'\setminus\left[\bigcup_{i^*<i}A_{i^*}'\bigcup\mathrm{supp}(f)\right]=\{\boldsymbol{b}_i\},\ \boldsymbol{b}_i\in B\cup D\end{aligned}\right\} \quad (9)$$

当 $\binom{n}{n/2}<i\le M$ 时，有 $A_i'\setminus\left[\bigcup_{i^*<i}A_{i^*}'\bigcup\mathrm{supp}(f)\right]=\{\boldsymbol{b}_i\}$。

于是由引理 5 可知，f 没有次数小于 $n/2$ 的非零零化子。

所以综合两方面有 $\mathrm{AI}(f)=n/2$，定理得证。

定理 2 构造方法 1 中所构造的函数 f 具有最优代数次数。

证明 设 $f(\boldsymbol{x})=f(x_1,\cdots,x_n)=\sum_{I\subseteq\{1,2,\cdots,n\}}a_I\cdot\prod_{i\in I}x_i$ 是 f 的代数正规型，那么易知对每个 I 有 $a_I=\sum_{\mathrm{supp}(\boldsymbol{x})\subseteq I}f(\boldsymbol{x})$。注意到 $a_I=1$，当且仅当 $|C_I\cap\mathrm{supp}(f)|=|C_I\cap W^{>n/2}\setminus C|+|C_I\cap W^{n/2}\setminus(B\cup D)|$ 是奇数，其中 $C_I=\{\boldsymbol{x}\mid\mathrm{supp}(\boldsymbol{x})\subseteq I\}$。当 $|I|=n-1$ 时，有

$$\begin{aligned}&|C_I\cap W^{>n/2}\setminus C|+|C_I\cap W^{n/2}\setminus(B\cup D)|\\&=|C_I\cap W^{>n/2}|+|C_I\cap W^{n/2}\setminus(B\cup D)|\\&=2^{n-2}-\binom{n-1}{n/2}+|C_I\cap W^{n/2}\setminus(B\cup D)|\end{aligned} \quad (10)$$

注意到若 $n=2^m$，则 $\binom{n-1}{n/2}=1\bmod 2$。那么对任意的 $\boldsymbol{x}\in W^{n/2}\setminus(B\cup D)$，有

$$|C_I\cap G_n(\boldsymbol{x})|=\frac{1}{2}|G_n(\boldsymbol{x})|=2^{i-1} \quad (11)$$

由引理 4 可知 $|C_I\cap W^{n/2}\setminus(B\cup D)|=0\bmod 2$，进而有 $|C_I\cap\mathrm{supp}(f)|=1\bmod 2$。那么有 $a_I=1$，所以 $\deg(f)\ge n-1$。因为 f 是平衡的，所以 $\deg(f)\ne n$，因而 $\deg(f)=n-1$，即 f 具有最优代数次数，定理得证。

在研究 f 的非线性度之前，我们首先给出下面的一个引理。

引理 6 设 D 和 D_2 是上面所定义的集合，记

$$\left|\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}\right|+\left|\sum_{\boldsymbol{x}\in D\cup D_2}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\right| \quad (12)$$

为 Q，那么有 $|Q|\le\binom{n}{n/2}-6$。

证明 设 $D^0=\{\boldsymbol{x}\in D\mid\boldsymbol{x}\cdot\boldsymbol{u}=0\}$，$D^1=\{\boldsymbol{x}\in D\mid\boldsymbol{x}\cdot\boldsymbol{u}=1\}$，$D_2^0=\{\boldsymbol{x}\in D_2\mid\boldsymbol{x}\cdot\boldsymbol{u}=0\}$，$D_2^1=\{\boldsymbol{x}\in D_2\mid\boldsymbol{x}\cdot\boldsymbol{u}=1\}$。那么有 $\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}=|D^0|-|D^1|$，$\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}=|D_2^1|-|D_2^0|$ 和 $\sum_{\boldsymbol{x}\in D\cup D_2}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}=|D^0|-|D^1|-|D_2^1|+|D_2^0|$。不妨设 $|D^0|\ge|D^1|$，$|D_2^1|\ge|D_2^0|$。因为 $\binom{n}{n/2}=|D^0|+|D^1|+|D_2^1|+|D_2^0|+6$，所以有

$$\binom{n}{n/2}-|Q|=\begin{cases}3|D^1|+|D_2^1|+|D_2^0|-|D^0|+6,\\ \quad |D^0|-|D^1|\geq |D_2^1|-|D_2^0|\\ 3|D_2^0|+|D^0|+|D^1|-|D_2^1|+6,\\ \quad |D^0|-|D^1|<|D_2^1|-|D_2^0|\end{cases} \tag{13}$$

注意到 $3|D^1|+|D_2^1|+|D_2^0|-|D^0|\geq |D_2|-|D|=0$，且 $3|D_2^0|+|D^0|+|D^1|-|D_2^1|\geq |D|-|D_2|=0$，所以定理得证。

定理 3　构造方法 1 中所构造的函数 f 的非线性度为 $NL(f)=2^{n-1}-\binom{n-1}{n/2}+1$。

证明　首先我们来研究函数 f 的 Walsh 变换，它有一些与 Krawtchouk 多项式相关的非常好的组合性质。对任意的 $\boldsymbol{u}\in F_2^n$，有

$$\begin{aligned}W_f(\boldsymbol{u})=&\sum_{\boldsymbol{x}\in B}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in E}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}\\&+\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in W^{<n/2}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\\&+\sum_{\boldsymbol{x}\in W^{>n/2}}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+2\sum_{\boldsymbol{x}\in C}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\end{aligned} \tag{14}$$

注意到 $(-1)^{\overline{\boldsymbol{x}}\cdot\boldsymbol{u}}=(-1)^{wt(\boldsymbol{u})}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}$。如果 $wt(\boldsymbol{u})$ 是奇数，那么由引理 1 可知

$$\begin{aligned}W_f(\boldsymbol{u})&=2\sum_{\boldsymbol{x}\in C}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+2\sum_{\boldsymbol{x}\in W^{<n/2}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\\&=-2+2\sum_{i=0}^{n/2-1}K_i(wt(\boldsymbol{u}),n)\\&=-2+2K_{n/2-1}(wt(\boldsymbol{u})-1,n-1)\end{aligned} \tag{15}$$

如果 $wt(\boldsymbol{u})$ 是偶数，那么有

$$\begin{aligned}W_f(\boldsymbol{u})=&\sum_{\boldsymbol{x}\in B}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\\&+\sum_{\boldsymbol{x}\in E}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+2\end{aligned} \tag{16}$$

下面我们分 4 种情况来证明。

当 $wt(\boldsymbol{u})=0$ 时，因为 f 是平衡的，所以 $W_f(\boldsymbol{u})=0$。

当 $wt(\boldsymbol{u})=1$ 时，由引理 1 有

$$\begin{aligned}W_f(\boldsymbol{u})&=-2+2K_{n/2-1}(0,n-1)\\&=-2+2\binom{n-1}{n/2-1}K_0(n/2-1,n-1)\\&=-2+2\binom{n-1}{n/2-1}K_0(n/2,n)\\&=-2+2\binom{n-1}{n/2}\end{aligned} \tag{17}$$

当 $3\leq wt(\boldsymbol{u})\leq n-1$ 且 $wt(\boldsymbol{u})$ 是奇数时，由引理 2 有

$$\begin{aligned}W_f(\boldsymbol{u})&\leq -2+|2K_{n/2-1}(wt(\boldsymbol{u})-1,n-1)|\\&\leq -2+\frac{2}{n-1}\binom{n-1}{n/2}\end{aligned} \tag{18}$$

当 $2\leq wt(\boldsymbol{u})\leq n$ 且 $wt(\boldsymbol{u})$ 是偶数时，由引理 6 有

$$\begin{aligned}|W_f(\boldsymbol{u})|=&\Bigg|\sum_{\boldsymbol{x}\in B}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\\&+\sum_{\boldsymbol{x}\in E}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}+2\Bigg|\\\leq&\left|\sum_{\boldsymbol{x}\in D}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}+\sum_{\boldsymbol{x}\in D_2}(-1)^{1+\boldsymbol{x}\cdot\boldsymbol{u}}\right|+8\\\leq&\binom{n}{n/2}-6-\left|\sum_{\boldsymbol{x}\in D\cup D_2}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\right|+8\\\leq&\binom{n}{n/2}-6-\left|\sum_{\boldsymbol{x}\in W^{n/2}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}-6\right|+8\\\leq&\binom{n}{n/2}-\left|\sum_{\boldsymbol{x}\in W^{n/2}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}\right|+8\end{aligned} \tag{19}$$

因为 $\sum_{\boldsymbol{x}\in W^{n/2}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}=K_{n/2}(wt(\boldsymbol{u}),n)$，所以由引理 1 可知

$$|W_f(\boldsymbol{u})|\leq\binom{n}{n/2}-\binom{n}{n/2}\binom{n/2}{wt(\boldsymbol{u})/2}\Big/\binom{n}{wt(\boldsymbol{u})}+8 \tag{20}$$

注意到 $\binom{n}{n/2}=2\binom{n-1}{n/2}$，所以当 $wt(\boldsymbol{u})=1$ 时，$|W_f(\boldsymbol{u})|$ 的取值最大，即 $|W_f(\boldsymbol{u})|\leq -2+2\binom{n-1}{n/2}$。

再由非线性度的定义，即知定理得证。

4　结束语

本文给出了一种构造平衡的 2^m 元旋转对称布尔函数的新方法，该方法构造出的函数具有最大代数免疫度，最优代数次数和高非线性度。然而把这种构造方法扩展到普通的 n 元函数上还是比较困难的，这是因为对于普通的 n，存在着不同的轨道(事实上，对于某些其它的变元个数，我们能够得到一些具有最大代数免疫度的平衡的旋转对称布尔函数，但是这些函数的非线性度和代数次数并不理想)。所以我们下一步的主要工作是针对普通的 n 元函数，构造具有良好密码学性质的平衡的旋转对称布尔函数。此外，目前仍存在许多其它问题需要研究，比如说如何构造能够抵御快速代数攻击的具有良好密码学性质的旋转对称布尔函数等等。

参 考 文 献

[1] Courtois N and Meier M. Algebraic attacks on stream ciphers with linear feedback[C]. Cryptology-EUROCRYPT 2003, 2003, LNCS 2656: 345–359.

[2] Dalai D K, Gupta K C, and Maitra S. Results on algebraic immunity for cryptographically significant Boolean functions[C]. INDOCRYPT 2004, 2004, LNCS 3348: 92–106.

[3] Meier W, Pasalic E, and Carlet C. Algebraic attacks and decomposition of Boolean functions[C]. Cryptology-EUROCRYPT 2004, 2004, LNCS 3027: 474–491.

[4] Carlet C and Zeng X Y. Further properties of several classes of Boolean functions with optimum algebraic immunity[J]. *Designs, Codes and Cryptography*, 2009, 52(3): 303–338.

[5] Carlet C. A method of construction of balanced functions with optimum algebraic immunity[C]. Proceedings of the First International Workshop on Coding and Cryptography, Fujian, 2007: 25–43.

[6] Li Y, Yang M, and Kan H B. Constructing and counting Boolean functions on even variables with maximum algebraic immunity[J]. *IEICE Transactions on Fundamentals*, 2010, 93-A(3): 640–643.

[7] Rizomiliotis P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation [J]. *IEEE Transactions on Information Theory*, 2010, 56(8): 4014–4024.

[8] Tu Z R and Deng Y P. A class of 1-resilient function with high nonlinearity and algebraic immunity[R]. Cryptography ePrint Archive, Report 2010, 2010/179.

[9] Wang Q, Peng J, Kan H, *et al.*. Constructions of cryptographically significant Boolean functions using primitive polynomials[J]. *IEEE Transactions on Information Theory*, 2010, 56(6): 3048–3053.

[10] Stanica P and Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties[J]. *Electronic Notes in Discrete Mathematics*, 2003, 15(5): 139–145.

[11] Dalai D K, Maitra S, and Sarkar S. Results on rotation symmetric bent functions[J]. *Discrete Mathematics*, 2006, 309(8): 2398–2409.

[12] Maximov A, Hell M, and Maitra S. Plateaued rotation symmetric boolean runctions on odd number of variables[C]. First Workshop on Boolean Functions: Cryptography and Applications, University of Rouen and Havre, 2005: 83–104.

[13] Stanica P, Maitra S, and Clark J. Results on rotation symmetric bent and correlation immune Boolean functions[C]. FSE 2004, 2004, LNCS 3017: 161–177.

[14] Sarkar S and Maitra S. Construction of rotation symmetric Boolean functions with maximum algebraic immunity on odd number of variables[J]. *Computation Systems*, 2009, 12(3): 267–284.

[15] Fu S J, Li C, Matsuura K, *et al.*. Construction of rotation symmetric Boolean functions with maximum algebraic immunity[C]. CANS 2009, 2009, LNCS 5888: 402–412.

[16] Fu S J, Qu L J, Li C, *et al.*. Banlanced rotation symmetric Boolean function with maximum algebraic immunity[J]. *IET Information Security*, 2011, 5(2): 93–99.

熊晓雯： 女，1985 年生，硕士，助教，研究方向为信息安全.

魏爱国： 男，1966 年生，博士，教授，主要研究方向为运输保障模拟仿真.

张智军： 男，1977 年生，硕士，讲师，研究方向为车辆管理.