布尔函数的代数厚度

周 宇[1], 汪小芬[1], 罗彦锋[2], 肖国镇[1]
(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室, 陕西西安 710071;
2. 兰州大学 数学与统计学院, 甘肃兰州 730000)

摘 要: 基于布尔函数的代数次数和代数厚度, 给出了布尔函数和其分解函数的代数厚度的关系, 利用递归和反证法导出了 n 元布尔函数代数厚度的上界是 2^{n-1}, 这个上界回答了"是否存在代数厚度大于 2^{n-1} 的 n 元布尔函数"这个公开问题. 在此基础上改进了 n 元 k ($2 \leqslant k \leqslant (n-1)/2$) 次基本对称布尔函数的代数厚度的上界, 同时也得到了布尔函数的代数厚度的一些性质.

关键词: 布尔函数; 代数正规型; 代数厚度; 基本对称布尔函数
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2009) 07-1412-04

Algebraic Thickness of Boolean Functions

ZHOU Yu[1], WANG Xiao-fen[1], LUO Yan-feng[2], XIAO Guo-zhen[1]
(1. *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China;*
2. *School of Mathematics and Statistics, Lanzhou University, Lanzhou, Gansu 730000, China*)

Abstract: Based on the algebraic degree and the algebraic thickness of Boolean functions, the relationship of algebraic thickness between a Boolean function and their decomposing Boolean functions is given, and the upper bound on the algebraic thickness of Boolean functions with n variables is 2^{n-1} by the recurrence method and the reduction to absurdity. The upper bound answers the open problem: "whether there exists a Boolean function with n variables whose algebraic thickness is strictly greater than 2^{n-1}". At the end of this paper, according to this fact an upper bound on algebraic thickness of elementary symmetric Boolean functions of n variables with algebraic degree k ($2 \leqslant k \leqslant (n-1)/2$) is improved, and some properties on algebraic thickness of Boolean functions are derived.

Key words: Boolean functions; algebraic normal form; algebraic thickness; elementary symmetric Boolean functions

1 引言

布尔函数在科学技术的许多领域有重要的应用, 如通信和密码学等方面. 在流密码和分组密码中除了研究布尔函数的非线性度外, 还得考虑另外的两个指标: 代数次数和代数正规型中单项式(非零的系数)的个数, Knudsen 和 Lai 分别提出针对分组密码的高阶差分攻击[1,2]依靠的就是布尔函数的最大代数次数. 而由非线性布尔函数组合的多个线性反馈移位寄存器(LFSR)生成的序列中, 其线性复杂度是由这个布尔函数代数正规型中单项式的个数和代数次数来决定的, 所以文献[3]指出在线性反馈移位寄存器(LFSR)的非线性布尔函数选取中, 必须考虑高的代数次数和多的单项式. 在密码攻击中使用的布尔函数常常用仿射等价的布尔函数来代替, 这意味着代数正规型中单项式的个数在仿射变换下可能会改变. 所以 Carlet 提出代数厚度[4-6](Algebraic Thickness)概念, 用来衡量一个布尔函数在仿射变换下其代数正规型中单项式的个数多少, 在利用组合理论的基础上研究了代数厚度满足一定条件的布尔函数的个数界, 提出了关于任意元布尔函数代数厚度的公开问题, 但并未对一般布尔函数的代数厚度进行讨论.

本文中针对一般布尔函数, 研究了代数厚度的一些性质, 给出了布尔函数与其分解函数的代数厚度之间的关系, 由此解决了 Carlet 提出的对于任意布尔函数代数厚度的公开问题, 进而改进了基本对称布尔函数给的代数厚度上界, 同时得到布尔函数的代数厚度的一些性质.

2 预备知识

一个 n 元布尔函数 $f(x) = f(x_1, x_2, \cdots, x_n)$ 是指 F_2^n 到 F_2 的一个映射. 设 B_n 是所有这样的 n 元布尔函数组成的集合. 对任意一个 n 元布尔函数 $f(x)$ 都可以用一个多元多项式表示:

收稿日期: 2008-04-20; 修回日期: 2009-01-10
基金项目: 国家自然科学基金(No. 60773003, 60503010, 60603010); 中国科学院研究生院信息安全国家重点实验室开放课题(No. 03-06); 陕西省自然科学基金(No. 2006F19); 陕西省自然科学基础计划基金(No. SJ08-ZT14)

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{u \in F_2^n} a^u \left(\prod_{i=1}^{n} x_i^{u_i} \right) = \bigoplus_{u \in F_2^n} a^u x^u$$

$$= a_0 \oplus \sum_{1 \leqslant i \leqslant n} a_i x_i \oplus \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\cdots n} x_{12\cdots n}$$

其中 $a_0, a_i, a_{ij}, \cdots, a_{12\cdots n} \in F_2$, $\oplus$表示在 F_2, F_2^n 和 B_n 上的加法, 称这个多元多项式为 $f(x)$ 的代数正规型(ANF). 而 $f(x)$ 的代数次数 $\deg(f)$ 是指代数正规型中具有非零系数的拥有变量数 x_i 最多项的变量数. 若 $\deg(f) \leqslant 1$, 称 $f(x)$ 为仿射函数, 记为 $A(n)$, 若还满足无常数项, 称 $f(x)$ 为线性函数, 记为 $L(n)$. 对一般的 n 元布尔函数 $f(x)$, 可将其函数值按 x 的字典序从小到大排成一个向量: $[f(0), f(1), \cdots, f(2^n - 1)]$, 此时称这个向量中 1 的个数为 $f(x)$ 的汉明重量, 记为 $wt(f)$. 同样对任意一个向量 $\alpha \in F_2^n$, $wt(\alpha)$ 表示 α 中的 1 的个数. 若 $wt(f) = 2^{n-1}$, 则称 $f(x)$ 是平衡函数.

定义 **1**[4~6]　设 $f(x) \in B_n$, Ω_n 表示 F_2 上所有 $n \times n$ 非奇异矩阵的集合, $\tau(x) = xB \oplus b$, 其中 $B \in \Omega_n$, $b \in F_2^n$, $f(x)$ 的代数厚度(Algebraic Thickness)定义为 $f(\tau(x))$ 的代数正规型中具有非零系数单项式的最小个数, 记为 $T(f)$.

定义 1 中的 $\tau(x) = xB \oplus b$ 也称为仿射变换. 在定义 1 的基础上可知对任意的布尔函数

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{u \in F_2^n} a^u \left(\prod_{i=1}^{n} x_i^{u_i} \right) = \bigoplus_{u \in F_2^n} a^u x^u$$

$T(f)$ 是 $f(\tau(x))$ 的代数正规型中具有非零系数单项式的最小个数, 等价于

$$f(\tau(x)) = f(l_1(x_1), l_2(x_2), \cdots, l_n(x_n))$$

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

其中 $l_i(x_i)(1 \leqslant i \leqslant n)$ 是仿射函数且其线性部分是线性独立的.

为了得到主要结论, 需要以下定义作为基础.

定义 **2**　设 $F_f(x)$ 是 F_2^n 到 $Z^+ \cup \{0\}$ 的一个映射, $f(x) \in B_n$. $F_f(x)$ 定义为如下形式:

$$F_f(x) = a_0 + \sum_{1 \leqslant i \leqslant n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \cdots + a_{12\cdots n} x_{12\cdots n}$$

其中"+"为 $Z^+ \cup \{0\}$ 上加法, Z^+ 为正整数.

从定义 2 可知, $F_f(x)$ 完全由 $f(x)$ 决定, 例如若 $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1 \oplus x_2$, 则 $F_f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1 + x_2$.

Carlet 在文献[4]中的得到代数厚度满足一定条件的布尔函数的个数界, 即, 对每一个 $\lambda < 1/2$, $|\{f(x) \in B_n \mid T(f) \geqslant \lambda 2^n\}| \geqslant 1 - 2^{2^n H(\lambda) - 2^n + n^2 + n}$, 其中 $H(\lambda)$ 是熵函数. 进而在文献[6]中得到几乎所有 n 元布尔函数其代数厚度大于等于 $\lambda 2^n$. 所以在文献[4~6]中提出这样一个公开问题:"是否存在 $T(f) > 2^{n-1}$ 的 n 元布尔函数 $f(x)$?", 在本文中将给出此问题的答案.

3　一般布尔函数的代数厚度

为了得到一般布尔函数的代数厚度的上界, 首先, 在定义 2 的基础上, 可以给出任意布尔函数的代数厚度的普遍上界. 为了论述方便, 下文中统一用 $\bar{1}$ 和 $\vec{1}$ 分别表示 F_2^n 和 F_2^{n-1} 上全 1 向量, 也就是, $\bar{1} = (1, 1, \cdots, 1) \in F_2^n$, $\vec{1} = (1, 1, \cdots, 1) \in F_2^{n-1}$.

性质 **1**　设 $f(x) \in B_n$, 则 $T(f) \leqslant F_f(\bar{1})$.

证明　由定义 2 可知, 当变量 $x = \bar{1}$ 时, $F_f(\bar{1})$ 为 $f(x)$ 的代数正规型中单项式的个数, 而由定义 1 可知在变换 $\tau(x) = xB \oplus b$ 下, 只需取 $B = I$(I 为 F_2^n 上单位阵), $b = \bar{0}$($\bar{0} = (0, 0, \cdots, 0)$ 为 F_2^n 上全零向量), 这时 $T(f)$ 应该不大于 $f(\tau(x))$ 中单项式的个数, 所以一定有 $T(f) \leqslant F_f(\bar{1})$.

性质 1 表明任何一个布尔函数 $f(x)$ 的代数厚度小于等于其变量全取 1 时的 $F_f(\bar{1})$ 值.

性质 **2**　设 $f(x), g(x) \in B_n$. 若存在 $B \in \Omega_n$, $b \in F_2^n$ 使得 $f(x) = g(xB \oplus b)$, 则 $T(f) = T(g)$.

性质 2 反映了若布尔函数互为仿射等价, 则它们的代数厚度是一样的, 这也就说可以从仿射等价角度对布尔函数的代数厚度做划分: 仿射等价的布尔函数可作为一类. 在文献[7]中可知, 所有的 6 元布尔函数有 150357 个等价类, 而文献[8]中给出了所有的 4 元 Bent 函数有 28 个等价类, 这些等价类的个数远远小于 6 元和 4 元布尔函数的总数, 所以布尔函数代数厚度的研究可以转化为布尔函数仿射等价类的研究.

而对于 n 元线性布尔函数同样有以下结论.

性质 **3**　若 $f(x) \in L(n)$ 且 $\deg(f) = 1$, 则 $T(f) = 1$.

证明　由于 $f(x)$ 是 n 元线性函数且其代数次数为 1, 所以其代数正规型可写为 $f(x) = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$, $a = (a_1, a_2, \cdots, a_n) \in F_2^n$ 且 $wt(a) = k$, $1 \leqslant k \leqslant n$. 为了方便, 我们不妨设 a 的前 k 个分量为 1, 其余 $n - k$ 个分量为 0, 此时 $f(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_k$. 设 $\tau(x) = xB \oplus b = (x_1, x_1 \oplus x_2, x_2 \oplus x_3, \cdots, x_{k-1} \oplus x_k, x_{k+1}, \cdots, x_n) \oplus (0, 0, \cdots, 0)$, 可知 $l_1(x) = x_1$, $l_i(x) = x_{i-1} \oplus x_i (2 \leqslant i \leqslant k)$, $l_j(x) = x_j (k+1 \leqslant j \leqslant n)$, 所以 $l_1(x), l_2(x), \cdots, l_n(x)$ 是线性无关的, 所以对任意的 $k (1 \leqslant k \leqslant n)$, 有 $f(\tau(x)) = x_1 \oplus x_1 \oplus x_2 \oplus x_2 \oplus x_3 \oplus \cdots \oplus x_{k-1} \oplus x_k = x_k$, 即 $T(f) \leqslant 1$. 但由于 B 为非奇异矩阵, 所以 $f(\tau(x))$ 至少有一个单项式, 即 $T(f) \geqslant 1$. 因此 $T(f) = 1$.

进而根据性质 3 可知对任意仿射函数 $f(x) \in A(n)$ 有 $T(f) = 0$ 或者 1.

性质 **4**　若 $f(x) \in B_n$ 且 $T(f) > k$, 则 $\deg(f) > l(l$

为集合$\{j\in Z^+\cup\{0\}\mid \sum_{i=0}^{j}C_n^i\leqslant k\}$中的最大值).

证明 只需注意到 n 元布尔函数$f(x)$的代数次数仅为 i 的单项式有$C_n^i(0\leqslant i\leqslant n)$个, 所以当 $T(f)>k$ 时, 要使得$f(x)$的单项式的个数最少为 $k+1$, 即, $\deg(f)>l$, 其中 l 为集合$\{j\in Z^+\cup\{0\}\mid \sum_{i=0}^{j}C_n^i\leqslant k\}$中的最大值.

性质 4 给出了布尔函数的代数厚度与代数次数的关系. 在性质 1 和 2 的基础上, 对一般的布尔函数可以给出其分解函数与原函数的代数厚度之间的关系.

定理 1 设$f(x)=x_nf_1(x_1,x_2,\cdots,x_{n-1})\oplus f_2(x_1,x_2,\cdots,x_{n-1})\in B_n$, 则 $T(f)\leqslant 2\max\{T(f_1),T(f_2)\}$.

证明 不妨取 $B=\begin{pmatrix}B_0 & 0_{(n-1)\times 1}\\ 0_{1\times(n-1)} & 1\end{pmatrix}_{n\times n}$, $b=(b_1,\cdots,b_{n-1},0)\in F_2^n$, 其中 B_0 为 F_2 上$(n-1)\times(n-1)$阶非奇异矩阵, $0_{(n-1)\times 1}$和$0_{1\times(n-1)}$分别为长度为 $n-1$ 的全零列向量和行向量. 为了方便我们记 $x'=(x_1,x_2,\cdots,x_{n-1})\in F_2^{n-1}$, $b'=(b_1,\cdots,b_{n-1})\in F_2^{n-1}$, 这时就有

$$f(xB\oplus b)=x_nf_1(x'B_0\oplus b')\oplus f_2(x'B_0\oplus b').$$

令 $x=\bar{1}=(\overrightarrow{1},1)$, $g_1(x')=f_1(x'B_0\oplus b')$, $g_2(x')=f_2(x'B_0\oplus b')$, 根据性质 1, 对任意的 $B_0\in\Omega_{n-1}$, $b'\in F_2^{n-1}$ 有

$$\begin{aligned}T(f)&\leqslant F_f(\bar{1}B\oplus b)\\&=F_{f_1}(\overrightarrow{1}B_0\oplus b')+F_{f_2}(\overrightarrow{1}B_0\oplus b')\\&=F_{g_1}(\overrightarrow{1})+F_{g_2}(\overrightarrow{1})\leqslant 2\max\{F_{g_1}(\overrightarrow{1}),F_{g_2}(\overrightarrow{1})\}.\end{aligned}$$

再由性质 2 可知存在 $B'_0\in\Omega_{n-1}$, $b'_0\in F_2^{n-1}$ 使得 $T(g_1)=F_{g_1}(\overrightarrow{1})=T(f_1)$, $T(g_2)=F_{g_2}(\overrightarrow{1})=T(f_2)$, 所以, $T(f)\leqslant 2\max\{T(f_1),T(f_2)\}$.

定理 1 表明了分解函数和原函数的代数厚度的关系, 通过这个可以从分解函数的代数厚度角度去衡量原函数的代数厚度. 由于对于任意的$f(x)\in B_n$ 一定满足$T(f)\leqslant 2^n$, 进而对于文献[4~6]中的公开问题就有如下推论:

推论 1 设$f(x)=x_nf_1(x_1,x_2,\cdots,x_{n-1})\oplus f_2(x_1,x_2,\cdots,x_{n-1})\in B_n$. 若 $T(f)>2^{n-1}$, 则

$$2^{n-2}<\max\{T(f_1),T(f_2)\}\leqslant 2^{n-1}.$$

推论 1 表明, 对任意一个布尔函数$f(x)\in B_n$ 来说, 如果 $T(f)>2^{n-1}$, 则一定存在其 $n-1$ 元的分解函数f^{n-1}满足$T(f^{n-1})>2^{n-2}$; 同样如果考虑 $n-1$ 元布尔函数f^{n-1}, 利用推论 1 得知存在它的 $n-2$ 元分解函数f^{n-2}满足 $T(f^{n-2})>2^{n-3}$; 反复运用推论 1 就可以得到一系列布尔函数:

$$f=f^n,f^{n-1},f^{n-2},\cdots,f^2,f^1$$

其中$f^i\in B_i(1\leqslant i\leqslant n)$且 $T(f^i)>2^{i-1}$. 但是性质 3 表明对于任意的一元布尔函数来说其代数厚度为 0 或者 1, 即, $T(f^1)\leqslant 1$, 而不是 $T(f^1)>2^{1-1}=1$, 暗示了假设对任意的 n 元布尔函数$f(x)$满足 $T(f)>2^{n-1}$是错误的, 所以就回答了文献[4~6]公开问题:

定理 2 设$f(x)\in B_n$, 则 $T(f)\leqslant 2^{n-1}$.

由定理 2 可看出, 对于任意一个布尔函数$f(x)\in B_n$ 来说, 都有 $T(f)\leqslant 2^{n-1}$, 即, 不存在满足 $T(f)>2^{n-1}$ 的 n 元布尔函数$f(x)$.

下面将给出一些布尔函数代数厚度的性质.

性质 5 设$f(x)\in B_n$.

(1)若 $\deg(f)=n$, 则 $T(f)\geqslant 1$;

(2)若 $wt(f)=1$, 则 $T(f)=1$.

证明(1)根据代数厚度的定义, $\tau(x)=xB\oplus b$ 中 B 是可逆矩阵, 注意到 $\deg(f)=n$, 所以经过 $\tau(x)$ 变换后, $f(x)$的次数仍为 n, 即含有 $x_1x_2\cdots x_n$ 这一项, 所以 $T(f)\geqslant 1$;

(2)若 n 元布尔函数$f(x)$满足 $wt(f)=1$, 则$f(x)$的小项表示[9]为

$$f(x)=(x_1\oplus c_1)(x_2\oplus c_2)\cdots(x_n\oplus c_n),$$

其中 $c=(c_1,c_2,\cdots,c_n)\in F_2^n$, 由于 $\deg(f)=n$, 根据(1)可知 $T(f)\geqslant 1$. 若取 B 为 F_2 上单位阵, $b=c$, 则 $\tau(x)=xB\oplus b=(x_1\oplus c_1,x_2\oplus c_2,\cdots,x_n\oplus c_n)$, 所以$f(\tau(x))=x_1x_2\cdots x_n$, 即 $T(f)\leqslant 1$. 即, $T(f)=1$.

最后给出基本对称布尔函数代数厚度的上界. 称 n 元 k 次布尔函数$f^k(x)$为基本对称布尔函数:

$$f^k(x)=\bigoplus_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_k},\ 1\leqslant k\leqslant n.$$

由性质 1 可知对任意的 $k(1\leqslant k\leqslant n)$都有 $T(f^k)\leqslant C_n^k$, 而在定义 1 中表明非奇异矩阵 B 对代数正规型中单项式的系数有直接影响. 由于 $k=1$, n 分别对应次数为 1 和 n 的线性布尔函数和汉明重量为 1 的布尔函数, 在性质 3 和性质 5 中已给出了回答, 所以下面我们仅考虑 $k(2\leqslant k\leqslant(n-1)/2)$次的基本对称布尔函数的代数厚度的上界.

定理 3 设$2\leqslant k\leqslant(n-1)/2$, $f^k(x)\in B_n$, 则 $T(f^k)\leqslant C_{n-1}^k+2C_{n-2}^{k-2}$.

证明 不妨记$y_1=(x_1,x_2,\cdots,x_{n-1})\in F_2^{n-1}$, $y_2=(x_2,\cdots,x_{n-1})\in F_2^{n-2}$, 由于$f^k(x)$可表示成$f^k(x)=x_nf_1^{k-1}(y_1)\oplus f_2^k(y_1)$, 其中$f_1^{k-1}(y_1)$和$f_2^k(y_1)$分别为 $n-1$ 元的 $k-1$ 次和 k 次基本对称布尔函数, 所以当 $2\leqslant k\leqslant(n-1)/2$ 时为了使$f^k(x)$的每一个 k 次单项式经 $\tau(x)$ 变换后产生较少的低次项. 可以在 $\tau(x)=xB\oplus b$ 中取$B=\begin{pmatrix}A & a\\ 0_{1\times n-1} & 1\end{pmatrix}$, $b=(0,0,\cdots,0)\in F_2^n$, 其中 A 为

F_2 上的$(n-1)\times(n-1)$阶单位阵, $a^{\mathrm{T}}=(1,0,\cdots,0)\in F_2^{n-1}$, $0_{1\times n-1}$为 $n-1$ 维的零向量. 这时 $l_n(x)=x_1\oplus x_n$, $l_i(x)=x_i(1\leqslant i\leqslant n-1)$, 所以此时$f^k(\tau(x))=$

$=(x_1\oplus x_n)f_1^{k-1}(y_1A)\oplus f_2^k(y_1A)$

$=x_nf_1^{k-1}(y_1)\oplus x_1f_1^{k-1}(y_1)\oplus f_2^k(y_1)$

$=x_nf_1^{k-1}(y_1)\oplus x_1[x_1f_3^{k-2}(y_2)\oplus f_4^{k-1}(y_2)]\oplus f_2^k(y_1)$

$=x_nf_1^{k-1}(y_1)\oplus x_1f_3^{k-2}(y_2)\oplus x_1f_4^{k-1}(y_2)\oplus f_2^k(y_1)$

其中$f_3^{k-2}(y_2)$和$f_4^{k-1}(y_2)$分别是 $n-2$ 元的 $k-2$ 次和 $k-1$ 次基本对称布尔函数. 由基本对称布尔函数的定义可知: $x_nf_1^{k-1}(y_1)$ 的代数正规型中有 C_{n-1}^{k-1} 个单项式, $x_1f_3^{k-2}(y_2)$ 的代数正规型中有 C_{n-2}^{k-2} 个单项式; $x_1f_4^{k-1}(y_2)$的代数正规型中有 C_{n-2}^{k-1} 个单项式; $f_2^k(y_1)$的代数正规型中有 C_{n-1}^k 个单项式. 但在 F_2 上变量次数相同的两个单项式相加可以抵消, 由于 $x_1f_4^{k-1}(y_2)$和$f_2^k(y_1)$都为 $x_1, x_2, \cdots, x_{n-1}$变元的 k 次布尔函数, 所以$f^k(\tau(x))$的代数正规型中至多有 $C_{n-1}^{k-1}+C_{n-2}^{k-2}+C_{n-1}^k-C_{n-2}^{k-1}=C_{n-1}^k+2C_{n-2}^{k-2}$个单项式, 所以

$$T(f^k)\leqslant C_{n-1}^k+2C_{n-2}^{k-2}.$$

从定理 5 可知, 当 $2\leqslant k\leqslant(n-1)/2$ 时, $T(f^k)\leqslant C_{n-1}^k+2C_{n-2}^{k-2}\leqslant C_n^k$. 可见定理 3 改进了性质 1 中对 n 元基本对称布尔函数的代数厚度的上界.

4　结束语

在文中讨论了布尔函数的代数厚度的一些性质, 给出了布尔函数和其分解函数的代数厚度的关系, 进而回答了 Carlet 关于代数厚度上界的公开问题, 同时得到了布尔函数的代数厚度的一些性质, 最后改进了基本对称布尔函数的代数厚度的上界. 这些结果可用于设计流密码和分组密码.

参考文献:

[1] L R Knudsen. Truncated and higher order differentials[A]. Fast Software encryption, Second International Workshop[C]. Lecture Notes in Computer Science, Springer-Verlag, vol. 1008, 1995. 196-211.

[2] X Lai. Higher order derivatives and differential cryptanalysis [A]. Proc. Symposium on Communication, Coding and Cryptography[C]. In honor of J L Massey on the occasion of his 60'th birthday, 1994.

[3] A Menezes, P van Oorschot, S Vanstone. Handbook of Applied Cryptography[M]. Boca Taton, FL: CRC Press on Discrete Mathematics and Its Applications, 1996.

[4] C Carlet. On cryptographic complexity of Boolean functions [A]. in Proc. 6th Conf Finite Fields with Applications to Coding Theory, Cryptography and Related Areas [C]. G L Mullen, H Stichtenoth, H Tapis-Recillas, Eds. Springer, 2002. 53-69.

[5] C Carlet. On the algebraic thickness and nonnormality of Boolean functions[A]. in Proc. 2003 IEEE Information Theory Workshop[C]. Paris, France, 2003. 147-150.

[6] C Carlet. On the degree, nonlinearity, algebraic thickness and nonnormality of Boolean functions, with developments on symmetric functions[J]. IEEE Transactions on Information Theory, 2004, 50(9): 2178-2185.

[7] J Maiorana. A classification of the cosets of the Reed-Muller code R(1, 6)[J]. Mathematics of Computation, 1991, 57: 403-414.

[8] 王隽, 李世取. Bent 函数的一般构造法[J]. 高校应用数学学报(A), 1999, 14A(4): 473-479.
Wang Jun, Li Shi-qu. A general construction of bent functions [J]. Applied mathematics(A), Journal of Chinese universities. 1999, 14A(4): 473-479. (in Chinese)

[9] 张文英, 武传坤, 于静之. 密码学中布尔函数的零化子[J]. 电子学报, 2006, 34(1): 51-54.
Zhang Wen-ying, Wu Chuan-kun, Yu Jing-zhi. On the annihilators of cryptographic Boolean functions[J]. Acta Electronica Sinica, 2006, 34(1): 51-54. (in Chinese)

作者简介:

周　宇　男, 1980 年 2 月出生于甘肃庆阳, 2003 年毕业于兰州大学数学与统计学院, 获理学学士学位. 2006 年毕业于兰州大学数学与统计学院, 获理学硕士学位, 2006 年 9 月至今在西安电子科技大学攻读博士学位. 目前主要研究方向为密码学, 信息安全与信息论.
E-mail: zhouyu.zhy@tom.com

汪小芬　女, 1982 年 1 月出生于浙江江山, 现在就读于西安电子科技大学攻读博士学位. 主要研究信息安全.
E-mail: wangxuedou@sina.com

罗彦锋　男, 1964 年 7 月出生于河南临颍县, 现为兰州大学数学与统计学院教授, 博士生导师. 目前研究方向为代数与密码学, 半群.

肖国镇　男, 1934 年 9 月出生于吉林四平, 现为西安电子科技大学教授, 博士生导师. 目前研究方向为密码, 编码与信息论.