布尔函数的扩展代数免疫度

熊晓雯*①　屈龙江①②　李　超①
①(国防科技大学数学与系统科学系　长沙　410073)
②(东南大学移动通信国家重点实验室　南京　210096)

摘　要：该文研究了布尔函数的扩展代数免疫度，首先给出了布尔函数的扩展代数免疫度与其代数免疫度相等的一个充分必要条件；然后讨论了两类具有最大代数免疫度的布尔函数的扩展代数免疫度，给出了其扩展代数免疫度也达到最大值的充分必要条件；最后基于代数补元素的思想，给出了布尔函数零化子结构的一种新刻画。

关键词：密码学；布尔函数；零化子；代数攻击；代数免疫度
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2011)02-0284-05
DOI: 10.3724/SP.J.1146.2010.00470

On Axtended Algebraic Immunity of Boolean Functions

Xiong Xiao-wen①　Qu Long-jiang①②　Li Chao①
①(*Department of Mathematics and System Science*, *National University of Defence Technology*, *Changsha* 410073, *China*)
②(*National Mobile Communications Research Laboratory*, *Southeast University*, *Nanjing* 210096, *China*)

Abstract: Extend algebraic immunity of Boolean functions are investigated in this paper. Firstly, a sufficient and necessary condition is presented that algebraic immunity of a Boolean function equals to its extended algebraic immunity. Secondly, it is proved that two classes of Boolean functions with maximum algebraic immunity also have optimal extended algebraic immunity. Finally, it is analyzed that the structure of the annihilators of Boolean functions with the algebraic complement.

Key words: Cryptography; Boolean functions; annihilators; Algebraic attacks; Algebraic immunity

1　引言

布尔函数作为序列密码、分组密码和 Hash 函数中的重要组件，其密码学性质的好坏直接关系到密码算法的安全性。2003 年以前，针对线性攻击、差分攻击、相关攻击等各种攻击方式，人们提出了多种布尔函数的密码学指标，如平衡性、非线性度、相关免疫度、弹性等等。2003 年，Armknecht，Courtois 等人[1,2]提出和发展了一种新的攻击方式——代数攻击，成功地攻击了许多流密码算法，受到了密码学界的高度关注。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)[3]。构造高代数免疫度尤其是最高代数免疫度布尔函数受到了人们的关注，已有许多报道[3–11]。

文献[4]在研究中注意到流密码算法中经常使用的 m 序列没有全零状态，因此若记 f 的补元素为 f^c，则 f 和 f^c 在零点以外的任一点的取值都相同，如果 $\mathrm{AI}(f^c)<\mathrm{AI}(f)$，那么用 f^c 替代 f 后再进行代数攻击会更有效，因为对于代数攻击，即使是两个布尔函数的代数免疫度之间仅仅相差 1 的改变，也可能会引起至关重要的变化。从而，在代数攻击中 $\mathrm{EAI}(f)$ 和 $\mathrm{AI}(f)$ 之间的不同是值得被研究的。因此，他们提出了扩展代数免疫度的概念，定义 f 的扩展代数免疫度 (Extended Algebraic Immunity，EAI) 为 $\mathrm{EAI}(f)=\min\{\mathrm{AI}(f),\mathrm{AI}(f^c)\}$。他们证明了 $0\le \mathrm{AI}(f)-\mathrm{EAI}(f)\le 1$，并指出 $\mathrm{AI}(f)-\mathrm{EAI}(f)=1$ 在很多情况下都成立。文献[12]进一步给出了布尔函数 f 和其代数补元素 f^c 的重量、零化子、Walsh 谱值和非线性度之间的关系，以及 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的一个充分条件。然而 EAI 还有许多亟需研究的地方，如目前并没有判断 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 成立的充分必要条件；还有人们也并不清楚许多代数免疫度达到最大的偶数元布尔函数的 EAI 是否也达到最大。

本文正是在此方向上进行的一些研究工作，内容包括：首先给出了 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的一个充分必要条件，据笔者所知，这是该问题的第 1 个充分必要条件；然后讨论了两类具有最大代数免疫度的布尔

2010-05-11 收到，2010-09-14 改回
国家自然科学基金(60803156)和移动通信国家重点实验室开放研究基金(W200807)资助课题
*通信作者：熊晓雯　winnie101206@126.com

函数的扩展代数免疫度，给出了其扩展代数免疫度也达到最大值的充分必要条件；最后基于代数补元素的思想，给出了布尔函数零化子结构的一种新刻画。

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

$$f(x_1,\cdots,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\le i<j\le n}a_{i,j}x_ix_j+\cdots+\sum_{1\le i_1<\cdots<i_d\le n}a_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}+\cdots+a_{1,\cdots,n}x_1x_2\cdots x_n$$

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 $\deg(f)$。代数次数小于等于 1 的布尔函数称为仿射函数。

n 元布尔函数 f 的支撑集定义为 $\mathrm{supp}(f)=\{x\in F_2^n|f(x)=1\}$。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。两个 n 元布尔函数 f 和 g 的 Hamming 距离定义为 $wt(f+g)$。

对给定的布尔函数 $f(x)\in\mathrm{B}_n$，$\alpha\in F_2^n$，令 $W_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus x\cdot\alpha}$，则 $W_f(\alpha)$ 称为函数 $f(x)$ 在点 α 的 Walsh 变换。布尔函数 f 的非线性度 $NL(f)$ 是 f 和所有仿射函数的最小汉明距离，即有

$$NL(f)=\min_{g\in\mathrm{B}_n,\deg g\le 1}d(f,g)=2^{n-1}-\frac{1}{2}\max_{\alpha\in F_2^n}|W_f(\alpha)|$$

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

$$\mathrm{AI}(f)=\min\{\deg(g)|0\ne g\in\mathrm{Ann}(f)\cup\mathrm{Ann}(1+f)\}=(f+1)\cup(f)\}$$

由 $f(1+f)=f+f^2=0$ 知，对每个 $0\ne f\in\mathrm{B}_n$，$\mathrm{AI}(f)\le\deg(f)$。另一方面，可以证明：如果 f 是一个 n 元布尔函数，那么 $\mathrm{AI}(f)\le\lceil n/2\rceil$[2,12]。

定义 1　设 $f\in\mathrm{B}_n$，f 的代数补元素定义为：由所有不在 f 的代数正规型中出现的单项式 $x_1^{u_1}\cdots x_n^{u_n},u_j\in\{0,1\}$ 所组成的函数，记为 f^c。

定义 2　设 $f\in\mathrm{B}_n$，其扩展代数免疫度定义为

$$\mathrm{EAI}(f)=\min\{\deg(g)|0\ne g\in\mathrm{AN}(f)\cup\mathrm{AN}(1+f)\cup\mathrm{AN}(f^c)\cup\mathrm{AN}(1+f^c)\}=\min\{\mathrm{AI}(f),\mathrm{AI}(f^c)\}$$

由 EAI 的定义不难推出，n 元布尔函数的 EAI 的最大值为 $\lceil n/2\rceil$。

定义 3　设 $f\in\mathrm{B}_n$，若 f 的代数正规型中的常数项是 0，那么称 f 为 0-CM，否则称为 1-CM。

性质 1[4]　设 $\Delta(x)=(1+x_1)\cdots(1+x_n)$，其中 $x=(x_1,\cdots,x_n)\in F_2^n$，那么有

(1) $\Delta(x)=1$ 当且仅当 $x=0$；

(2)若 $f(0)=0$，则 $\forall f(x)\in\mathrm{B}_n,f(x)\cdot\Delta(x)=0$；

(3)若 $f(0)=1$，则 $\forall f(x)\in\mathrm{B}_n,f(x)\cdot\Delta(x)=\Delta(x)$。

性质 2[4]　设 $f\in\mathrm{B}_n$，那么有

(1) $\forall x\in F_2^n,f^c(x)=f(x)+\Delta(x)$；

(2) $\forall 0\ne x\in F_2^n,f^c(x)=f(x)$。

由性质 2 易知，f 和 f^c 在任一非零点的取值都是相同的，只是在 $x=0$ 时的取值相差 1。

性质 3[4]　设 $f\in\mathrm{B}_n$，那么有

(1) $|\mathrm{AI}(f)-\mathrm{AI}(f^c)|\le 1$；

(2) $0\le\mathrm{AI}(f)-\mathrm{EAI}(f)\le 1$，且 $0\le\mathrm{AI}(f^c)-\mathrm{EAI}(f)\le 1$。

3　主要结果

3.1　$\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的充分必要条件

文献[4]虽然证明了 $0\le\mathrm{AI}(f)-\mathrm{EAI}(f)\le 1$，并指出 $\mathrm{AI}(f)-\mathrm{EAI}(f)=1$ 在很多情况下都成立，但并没有对 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 或者说对 $\mathrm{AI}(f)-\mathrm{EAI}(f)=1$ 的条件做进一步分析。文献[12]中虽然讨论了 $\mathrm{EAI}(f)$ 和 $\mathrm{AI}(f)$ 的关系，但只给出了 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的一个充分条件。本文对布尔函数的 EAI 和 AI 的取值进行了进一步的研究，首次给出了 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的一个充分必要条件。

引理 1[12]　设 $f\in\mathrm{B}_n$，那么有：(1)当 f 是 1-CM 时，$\mathrm{AN}(f^c)=\mathrm{AN}(f)\cup\mathrm{AN}(f)^c$；(2)当 f 是 0-CM 时，$\mathrm{AN}(f)=\mathrm{AN}(f^c)\cup\mathrm{AN}(f^c)^c$。

推论 1[12]　设 $f\in\mathrm{B}_n$，那么有：(1) 当 f 是 1-CM 时，$\mathrm{AN}(1+f)=\mathrm{AN}(1+f^c)\cup\mathrm{AN}(1+f^c)^c$；(2) 当 f 是 0-CM 时，$\mathrm{AN}(1+f^c)=\mathrm{AN}(1+f)\cup\mathrm{AN}(1+f)^c$。

定理 1　设 $f\in\mathrm{B}_n$，那么有

(1)当 f 为 0-CM 时，$\mathrm{EAI}(f)=\mathrm{AI}(f)$，当且仅当对任给的 $0\ne g\in\mathrm{AN}(1+f)$，都有 $\deg g^c\ge\mathrm{AI}(f)$；

(2)当 f 为 1-CM 时，$\mathrm{EAI}(f)=\mathrm{AI}(f)$，当且仅当对任给的 $0\ne g\in\mathrm{AN}(f)$，都有 $\deg g^c\ge\mathrm{AI}(f)$。

证明　只证明(1)，(2)类似可证。

首先证明充分性：若对任给的 $0\ne g\in\mathrm{AN}(1+f)$，都有 $\deg g^c\ge\mathrm{AI}(f)$，即 $\forall g\in\mathrm{AN}(1+f)^c$，有 $\deg(g)\ge\mathrm{AI}(f)$。那么由推论 1 可知，$\forall g\in\mathrm{AN}(1+f^c)$，有 $\deg(g)\ge\mathrm{AI}(f)$。当 f 为 0-CM 时，f^c 为 1-CM，$1+f$ 为 1-CM，$1+f^c$ 为 0-CM。注意到

$\forall x \in F_2^n$，有 $f^c(x) = f(x) + \Delta(x)$ 成立，那么若 $f^c g = 0$，则有 $(f + \Delta(x))g = fg + \Delta(x)g = 0$。由 f^c 为 1-CM 可知，当 $x = 0$ 时，$f^c(0) = 1$，那么此时必有 $g(0) = 0$，所以 $\Delta(x)g \equiv 0$，进而有 $fg = 0$。所以 $\forall g \in \mathrm{AN}(f^c)$，有 $\deg(g) \geq \mathrm{AI}(f)$。综合两方面有：$\forall g \in \mathrm{AN}(1 + f^c) \cup \mathrm{AN}(f^c), \deg(g) \geq \mathrm{AI}(f)$，故 $\mathrm{AI}(f^c) \geq \mathrm{AI}(f)$，进而有 $\mathrm{EAI}(f) = \mathrm{AI}(f)$，即充分性得证。

其次证明必要性若 $\mathrm{EAI}(f) = \mathrm{AI}(f)$，那么有 $\mathrm{AI}(f) \leq \mathrm{AI}(f^c)$，从而有 $\forall 0 \neq g \in \mathrm{AN}(f^c) \cup \mathrm{AN}(1 + f^c), \deg(g) \geq \mathrm{AI}(f)$，也就是有 $\forall g \in \mathrm{AN}(f) \cup \mathrm{AN}(1 + f), \deg(g^c) \geq \mathrm{AI}(f)$，那么必然有 $\forall g \in \mathrm{AN}(1 + f), \deg g^c \geq \mathrm{AI}(f)$，故必要性得证。 证毕

由定理 1 可以很容易地得到下面的推论。

推论 2 设 $f \in \mathrm{B}_n$，那么有

(1)当 f 为 0-CM 时，$\mathrm{EAI}(f) = \mathrm{AI}(f) - 1$，当且仅当存在 $g \in \mathrm{AN}(1 + f)$，使得 $\deg g^c < \mathrm{AI}(f)$；

(2)当 f 为 1-CM 时，$\mathrm{EAI}(f) = \mathrm{AI}(f) - 1$，当且仅当存在 $g \in \mathrm{AN}(f)$，使得 $\deg g^c < \mathrm{AI}(f)$。

3.2 两类具有最大 AI 的布尔函数的 EAI

为了能够更好地抵抗代数攻击，希望布尔函数的 AI 和 EAI 能够同时达到其最大值，但是由文献[12]可知，满足 $\mathrm{AI}(f) = \lceil n/2 \rceil$ 的奇数元的布尔函数，其 EAI 只能达到 $\lfloor n/2 \rfloor$，而对于偶数元的情况并没有给出相应的结果。下面讨论两类已知的满足 $\mathrm{AI}(f) = n/2$ 的布尔函数的 EAI，给出了其 EAI 也取到最大值的充分必要条件。

引理 2[12] 设 $f \in \mathrm{B}_n$，n 为偶数，$f(x_1, \cdots, x_n) = \begin{cases} 0, & wt(x_1, \cdots, x_n) < n/2 \\ 1, & wt(x_1, \cdots, x_n) > n/2 \\ b \in \{0,1\}, & wt(x_1, \cdots, x_n) = n/2 \end{cases}$，若 $b = 1$，那么 $\mathrm{EAI}(f) = n/2 - 1$。

定理 2 设 n 为偶数，那么布尔函数 $f(x_1, \cdots, x_n) = \begin{cases} 0, & wt(x_1, \cdots, x_n) < n/2 \\ 1, & wt(x_1, \cdots, x_n) > n/2 \\ b \in \{0,1\}, & wt(x_1, \cdots, x_n) = n/2 \end{cases}$ 达到最大扩展代数免疫度 $n/2$，当且仅当存在 $(x_1, \cdots, x_n) \in F_2^n$，使得 $wt(x_1, \cdots, x_n) = n/2$ 且 $f(x_1, \cdots, x_n) = 0$。

证明 首先文献[5]中已经证明 $\mathrm{AI}(f) = n/2$。由引理 2 易知必要性成立，下面证明充分性：若存在 $(x_1, \cdots, x_n)$，使得 $wt(x_1, \cdots, x_n) = n/2$ 且 $f(x_1, \cdots, x_n) = 0$，则有 $\mathrm{EAI}(f) = n/2$。

注意到 f 为 0-CM，故只需证明 $1 + f^c$ 没有次数小于 $n/2$ 的零化子。记

$$f_1 = 1 + f^c(x_1, \cdots, x_n) = \begin{cases} 0, & wt(x_1, \cdots, x_n) = 0 \\ 1, & 1 \leq wt(x_1, \cdots, x_n) < n/2 \\ 0, & wt(x_1, \cdots, x_n) > n/2 \\ b + 1 \in \{0,1\}, & wt(x_1, \cdots, x_n) = n/2 \end{cases}$$

假设存在 $g \in \mathrm{B}_n$，使得 $f_1 g = 0$，且 $\deg(g) < n/2$，那么当 $1 \leq wt(x_1, \cdots, x_n) < n/2$ 时，$g(x) = 0$。设 $d = n/2 - 1$，那么有

$$g(x_1, \cdots, x_n) = g_0 + \sum_{1 \leq i \leq n} g_i x_i + \sum_{1 \leq i < j \leq n} g_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 < i_2 < \cdots < i_d \leq n} g_{i_1 i_2 \cdots i_d} x_{i_1} x_{i_2} \cdots x_{i_d}$$

当 $wt(x_1, \cdots, x_n) = 1$ 时，$g(x) = 0 = g_0 + g_i \Rightarrow g_i = g_0$，$1 \leq i \leq n$；当 $wt(x_1, \cdots, x_n) = 2$ 时，$g(x) = 0 = g_0 + g_i + g_j + g_{ij} \Rightarrow g_{ij} = g_0, 1 \leq i < j \leq n$；$\cdots$；当 $wt(x_1, \cdots, x_n) = d$ 时，$g(x) = 0 = \sum_{\mathrm{supp}(I) \subseteq \mathrm{supp}(x)} g_I$ $\Rightarrow g_{i_1 i_2 \cdots i_d} = g_0, 1 \leq i_1 < i_2 < \cdots < i_d \leq n$。

那么

$$g(x_1, \cdots, x_n) = g_0 \left(1 + \sum_{1 \leq i \leq n} x_i + \sum_{1 \leq i < j \leq n} x_i x_j + \cdots + \sum_{1 \leq i_1 < i_2 < \cdots < i_d \leq n} x_{i_1} x_{i_2} \cdots x_{i_d} \right)$$

若 $g_0 = 1 \neq 0$，则

$$g(x_1, \cdots, x_n) = 1 + \sum_{1 \leq i \leq n} x_i + \sum_{1 \leq i < j \leq n} x_i x_j + \cdots + \sum_{1 \leq i_1 < i_2 < \cdots < i_d \leq n} x_{i_1} x_{i_2} \cdots x_{i_d}$$

当 $wt(x_1, \cdots, x_n) = n/2$ 时，$g(x) = \sum_{\mathrm{supp}(I) \subseteq \mathrm{supp}(x)} g_I = (2^{n/2} - 1) = 1 \neq 0$。

已知存在 $(x_1, \cdots, x_n)$，使得 $wt(x_1, \cdots, x_n) = n/2$ 且 $f(x_1, \cdots, x_n) = 0$，那么 $f_1(x_1, \cdots, x_n) = 1$，这与 $f_1 g = 0$ 矛盾，所以只能有 $g_0 = 0$，进而有 $g(x) = 0$。所以当 $\mathrm{AI}(f) = n/2$ 时，若 $(1 + f^c)g = 0$，那么必有 $g = 0$ 或 $\deg(g) \geq n/2$。即 $\forall g \in \mathrm{AN}(1 + f)$，都有 $\deg g^c \geq \mathrm{AI}(f)$，故由定理 1 可知 $\mathrm{EAI}(f) = n/2$，从而充分性得证。 证毕

定理 3 设 $n \geq 2$ 为一偶数，α 为 F_{2^n} 上的一个本原元，f 为 F_{2^n} 上支撑为 $\{0\} \cup \{\alpha^i | i = 0,1,\cdots,2^{n-1} - 2\}$ 的布尔函数，则 $\mathrm{EAI}(f) = n/2$。

证明 首先文献[8]中已经证明 $\mathrm{AI}(f) = n/2$。

注意到 f 为 1-CM，故只需证明 f^c 没有次数小于 $n/2$ 的零化子即可。

设 $g(x)$ 为任一代数次数至多为 $n/2 - 1$ 的布尔函数，设 $g(x) = \sum_{i=0}^{2^n - 1} g_i x^i, g_i \in F_{2^n}$，为其在域 F_{2^n} 中的单变量表示，其中若 i 的 2-重量 $wt(i) \geq n/2$，则

$g_i=0$，特别的有 $g_{2^n-1}=0$，那么 $g(x)=\sum_{i=0}^{2^n-2}g_ix^i$。注意到 $\mathrm{supp}(f^c)=\{\alpha^i|i=0,1,\cdots,2^{n-1}-2\}$，那么若 $f^cg=0$，则对任意的 $i=0,1,\cdots,2^{n-1}-2$，有 $g(\alpha^i)=0$，也就是说，向量 $(g_0,\cdots,g_{2^n-2})$ 为 F_{2^n} 上零点为 $1,\alpha,\cdots,\alpha^{2^{n-1}-2}$ 的 Reed-Solomon 码的一个码字。若 $g\neq 0$，那么由定义有

$$\begin{pmatrix} g(1)\\ g(\alpha)\\ g(\alpha^2)\\ \vdots\\ g(\alpha^{2^n-2}) \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1\\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(2^n-2)}\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ 1 & \alpha^{2^n-2} & \alpha^{2(2^n-2)} & \cdots & \alpha^{(2^n-2)(2^n-2)} \end{pmatrix}\times\begin{pmatrix} g_0\\ g_1\\ g_2\\ \vdots\\ g_{2^n-2} \end{pmatrix}$$

注意到对任意的 $0\le i,j\le 2^n-2$，若 $i=j$，则 $\sum_{k=0}^{2^n-2}\alpha^{(i-j)k}=1$；否则为 0。

进而有

$$\begin{pmatrix} g_0\\ g_1\\ g_2\\ \vdots\\ g_{2^n-2} \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1\\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(2^n-2)}\\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(2^n-2)}\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ 1 & \alpha^{-(2^n-2)} & \alpha^{-2(2^n-2)} & \cdots & \alpha^{-(2^n-2)(2^n-2)} \end{pmatrix}\times\begin{pmatrix} g(1)\\ g(\alpha)\\ g(\alpha^2)\\ \vdots\\ g(\alpha^{2^n-2}) \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 1 & \cdots & 1\\ \alpha^{-(2^{n-1}-1)} & \alpha^{-2^{n-1}} & \cdots & \alpha^{-(2^n-2)}\\ \vdots & \vdots & \cdots & \vdots\\ \alpha^{-(2^{n-1}-1)(2^n-2)} & \alpha^{-2^{n-1}(2^n-2)} & \cdots & \alpha^{-(2^n-2)(2^n-2)} \end{pmatrix}\times\begin{pmatrix} g(\alpha^{2^{n-1}-1})\\ g(\alpha^{2^{n-1}})\\ \vdots\\ g(\alpha^{2^n-2}) \end{pmatrix}$$

假设至少有 2^{n-1} 个 $g_i=0$，则 $g(\alpha^{2^{n-1}-1}),g(\alpha^{2^{n-1}}),\cdots,g(\alpha^{2^n-2})$ 满足一个系数矩阵为 2^n-1 阶 Vandermonde 矩阵的齐次线性方程组，其行列式非零，那么有 $g(\alpha^{2^{n-1}-1}),g(\alpha^{2^{n-1}}),\cdots,g(\alpha^{2^n-2})$ 全为零，因此 g 必须为 0，矛盾。所以向量 $(g_0,\cdots,g_{2^n-2})$ 的重量至少为 2^{n-1}。注意到若 $wt(g_0,\cdots,g_{2^n-2})=2^{n-1}$，则由 $\left|\{i|wt(i)\le\lceil n/2\rceil-1\}\right|\le 2^{n-1}$ 可知必有 n 为奇数，故 $wt(g_0,\cdots,g_{2^n-2})>2^{n-1}$。但这又与 $\deg(g)\le(n/2)-1$ 矛盾，故只能有 $g(x)=0$，那么 f^c 没有次数小于 $n/2$ 的零化子，所以 $\mathrm{EAI}(f)=n/2$。　　证毕

3.3 基于代数补思想的布尔函数零化子结构的新刻画

布尔函数的零化子在代数攻击中扮演着重要的角色，如果布尔函数 f 或 $1+f$ 存在较低次数的零化子，将在很大程度上提高代数攻击的效率，因此希望找到有效的算法来计算布尔函数的零化子，尤其是判定一个布尔函数是否存在较低次的零化子。分析布尔函数零化子的结构对寻找较低次的零化子很有益处。下面利用布尔函数 f 与其代数补元素 f^c 两者的零化子之间的关系，给出布尔函数零化子结构的一种新刻画。

设 $S\subseteq F_2^n$，定义 $f^s(x)=\begin{cases}f(x), & x\notin S\\ f(x)+1, & x\in S\end{cases}$。令 $\Delta_s(x)=\sum_{a=(a_1,\cdots,a_n)\in S}\prod_{i=1}^n(x_i+a_i+1)$，那么 $f^s(x)=f(x)+\Delta_s(x)$。

定理 4 设 $I=\{x\in F_2^n|wt(x)\le r,f(x)=0\},r=1,2,\cdots$，则 $\mathrm{AN}(f)=\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S$。

证明　一方面，若 $g\in\mathrm{AN}(f)$，则 $fg=0$，故当 $x\in\mathrm{supp}(f)$ 时，$g=0$。设 $S_0=\{x\in I|g(x)=1\}\subseteq I$，令 $\varphi(x)=g(x)^{S_0}$，于是 $\varphi(x)=\begin{cases}0, & x\in I\\ g(x), & x\notin I\end{cases}$，从而 $\varphi(x)f^I(x)=0$，那么 $\varphi(x)\in\mathrm{AN}(f^I)$，进而有 $g(x)\in\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S$，故 $\mathrm{AN}(f)\subseteq\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S$。

另一方面，若 $g\in\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S$，则存在 $S_0\subseteq I$，使得 $g\in(\mathrm{AN}(f^I))^{S_0}$，那么 $g^{S_0}\in\mathrm{AN}(f^I)$，进而有 $0=g^{S_0}f^I$。注意到 $(g^{S_0})^{S_0}=g$，$S_0\subseteq I$，且 $\forall x\in I,f(x)=0$，那么有 $gf=0$，进而有 $g\in\mathrm{AN}(f)$，故 $\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S\subseteq\mathrm{AN}(f)$。综合两方面有 $\mathrm{AN}(f)=\bigcup_{S\subseteq I}(\mathrm{AN}(f^I))^S$。　　证毕

定理 4 给出了 $\mathrm{AN}(f)$ 结构的一个新刻画，该刻画有助于求解 $\mathrm{AN}(f)$ 的全部元素。由定理 4 中集合 I 的定义易知，若 $x\in F_2^n$ 且 $wt(x)\le r$，则 $f^I(x)=1$，因此 $\mathrm{AN}(f^I)$ 比 $\mathrm{AN}(f)$ 容易计算。求出了 $\mathrm{AN}(f^I)$ 的元

素后，对于每一个 $S \subseteq I$，每一个函数 $g \in \mathrm{AN}(f^I)$，计算 $g^s(x) = g(x) + \Delta_s(x)$ 就给出了 $\mathrm{AN}(f)$ 的全部元素，然而注意到 I 的子集个数随 $|I|$ 指数增长，故 r 也不能取得过大。但是定理 4 目前并不能直接应用到低次零化子求解或代数免疫度的计算中，这是因为对任一子集 $S \subseteq I$，目前并没有刻画 $\mathrm{AN}(f^I)^S$ 中低次元素的有效方法，但一旦找到了刻画 $\mathrm{AN}(f^I)^S$ 中低次元素的有效方法，由于 $\mathrm{AN}(f^I)$ 比 $AN(f)$ 要容易计算，这很可能成为快速计算 AI 的一种新方法，这也是我们下一步的研究方向。

4 结束语

为了更好地抵抗代数攻击，人们推广了布尔函数代数免疫度概念，提出了 EAI 的概念。本文对布尔函数的 EAI 进行了进一步研究，得到了一些结果：利用 f 和 f^c 的零化子之间的关系首次给出了 $\mathrm{EAI}(f) = \mathrm{AI}(f)$ 的一个充分必要条件；讨论了两类已知满足 $\mathrm{AI}(f) = \lceil n/2 \rceil$ 的偶数元布尔函数的 EAI，给出了其 EAI 也取到最大值的充分必要条件；并基于代数补元素思想对布尔函数零化子的结构给出了一种新刻画。这些结果无论对于布尔函数 EAI 的分析，还是对于构造高 EAI 的布尔函数，都是很有意义的。但是仍有许多关于布尔函数 EAI 的问题需要解决，比如如何进一步提高本文给出的充分必要条件的有效性，能否给出 EAI 和抵抗快速代数攻击的关系等等。

参 考 文 献

[1] Armknecht F. Improving fast algebraic attacks, 2004, LNCS 3017: 65–82.

[2] Courtois N and Meier W. Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology-EUROCRYPT 2003, 2003, LNCS 2656: 345–359.

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

[4] Zhang Xiao-mo, Pieprzyk J, and Zheng Yu-liang. On algebraic immunity and annihilators, ICISC 2006, 2006, LNCS 4296: 65–80.

[5] Dalai D K. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Designs, Codes and Cryptography*, 2006, 40(1): 41–58.

[6] Du Yu-song and Pei Ding-yi. Construction of Boolean functions with maximum algebraic immunity and count of their annihilators at lowest degree. *Science in China*, 2010, 50(4): 780–787.

[7] Li Na and Qu Long-jiang, *et al*.. On the construction of Boolean functions with optimal algebraic immunity. *IEEE Transactions on Information Theory*, 2008, 54(3): 1330–1334.

[8] Carlet C and Feng K Q. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. ASIACRYPT 2008, 2008, LNCS 5350: 425–440.

[9] Carlet C, Dalai D K, Gupta K C, and Maitra S. Algebraic immunity for cryptographically significant Boolean functions：analysis and construction. *IEEE Transactions on Information Theory*, 2006, 52(7): 3105–3121.

[10] Qu L J, Feng K Q, Liu F, and Wang L. Construction symmetric Boolean functions with maximum algebraic immunity. *IEEE Transactions on Information Theory*, 2009, 55(5): 2406–2412.

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

[12] Wang Chun-peng and Chen Xiao-song. On extended algebraic immunity. *Designs, Codes and Cryptography*, 2010, 57(3): 271–281.

熊晓雯： 女，1985 年生，硕士生，研究方向为编码密码理论及其应用.

屈龙江： 男，1980 年生，博士，讲师，研究方向为编码密码理论及其应用.

李 超： 男，1966 年生，教授，研究方向为编码密码理论及其应用.