doi:10.3969/j.issn.1000-436x.2014.z2.024

对称布尔函数的扩展代数免疫度

伍高飞[1]，刘雪峰[1]，田叶[1]，张玉清[1,2]

(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. 中国科学院大学 国家计算机网络入侵防范中心，北京 101408)

摘 要：构造具有最优代数免疫度的布尔函数在流密码中有重要作用，基于布尔函数的单变量多项式表示，构造了一类达到最大扩展代数免疫度的布尔函数。以前的一些函数是这类函数的特例。利用对称布尔函数的基本性质，分析了具有最大代数免疫度的对称布尔函数的扩展代数免疫度。得出结论：共有 $2^{\lfloor \mathrm{lb}(n/2)\rfloor+2}$ 个达到最大扩展代数免疫度的 n （ n 是偶数）元对称布尔函数。

关键词：密码学；布尔函数；对称布尔函数；代数免疫度；零化子；扩展代数免疫度

中图分类号：TN918 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0179-05

Extended algebraic immunity of symmetric Boolean function

WU Gao-fei[1], LIU Xue-feng[1], TIAN Ye[1], ZHANG Yu-qing[1,2]

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China)

Abstract: Boolean functions with optimal algebraic immunity play an important role in stream ciphers. Based on the univariate polynomial representation of Boolean functions, a construction of Boolean functions with maximum extended algebraic immunity (EAI) is proposed, some previous results are special cases of our construction. The EAI of symmetric Boolean functions which have maximum algebraic immunity (AI) are analyzed by using the properties of symmetric Boolean functions. The result shows that there are only $2^{\lfloor \mathrm{lb}(n/2)\rfloor+2}$ n-variable (n even) symmetric Boolean functions achieve maximum EAI.

Key words: cryptography; Boolean functions; symmetric Boolean functions; algebraic immunity; annihilators; extended algebraic immunity

1 引言

布尔函数的密码学性质的好坏直接影响到流密码的安全性。目前，针对相关攻击，差分攻击，线性攻击等攻击方式，提出了抵抗相应攻击的密码学指标：相关免疫性、平衡性、非线性度等。2003 年，Courtois 等[1]提出一种新的流密码分析方法——代数攻击，它的基本思想是建立初始密钥和输出密钥流比特之间的代数方程，通过线性化方法求解该超定的多变元非线性方程组以得到初始密钥。如果布尔函数具有次数低的零化子，将会极大的提高代数攻击的效率。针对这种新的攻击，人们对布尔函数的设计提出了新的指标：代数免疫度(AI, algebraic immunity)[2]。Meier 等[2]证明了 n 元布尔函数的最大代数免疫度是 $\lceil n/2 \rceil$，达到此上界的布尔函数称为具有最大 AI 的函数。到目前为止，已经构造出很多具有最大 AI 的布尔函数[3~8]。

高的代数免疫度只是抵抗代数攻击的必要条件，但并不一定能有效的抵抗代数攻击[9]。扩展代数免疫度(EAI, extended algebraic immunity)的概念是由 Zhang 等[10]提出。他们注意到如果将布尔函数 f 换成其代数补元素 f^c（定义 2.1），而且 f^c 具有低次数的零化子，那么代数攻击的效率将会大大提高。文献[10]分析了 EAI 和 AI 之间的关系，指出

收稿日期：2014-07-23
基金项目：国家自然科学基金资助项目（61272481, 61402352）
Foundation Item: The National Natural Science Foundation of China (61272481, 61402352)

$\mathrm{AI}(f)-\mathrm{EAI}(f)\leqslant 1$，而且在大部分情况下有 $\mathrm{AI}(f)-\mathrm{EAI}(f)=1$。2010 年，Wang 等[11]进一步分析了布尔函数 f 及其代数补元素 f^c 的汉明重量，非线性度和 Walsh 谱值之间的关系，并给出了一个 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的充分条件。最近，Xiong 等[12]给出了一个 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的充分必要条件，并分析了两类具有最大 AI 的布尔函数的 EAI。

文献[3]指出，即使 2 个布尔函数的代数免疫度仅相差 1，对代数攻击的效率影响很大。因此，EAI 和 AI 之间的关系值得研究。目前，针对 EAI 的研究并不多，还有很多问题亟待解决，例如，如何构造具有最大 EAI 的布尔函数，如何更直观地刻画 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的充分必要条件，已知的具有最大 AI 的布尔函数的 EAI 表现等。

首先，基于布尔函数的单变量多项式表示，构造了一类具有最大 EAI 的布尔函数，指出文献[12]和定理 3 是定理 1 的特例；然后，分析了具有最大 AI 的对称函数的 EAI，并给出了所有的达到最大 EAI 的对称布尔函数。结果表明，在 $(2wt(n)+1)2^{\lfloor \mathrm{lb}(n/2)\rfloor+1}$ 个具有最大 AI 的 n（n 是偶数）元对称布尔函数中，有 $2^{\lfloor \mathrm{lb}(n/2)\rfloor+2}$ 个函数满足 $\mathrm{EAI}(f)=\mathrm{AI}(f)=n/2$。在这 $2^{\lfloor \mathrm{lb}(n/2)\rfloor+2}$ 个具有最大 EAI 的对称函数中，有 $2^{\lfloor \mathrm{lb}(n/2)\rfloor+1}$ 个对称函数具有性质 $\mathrm{EAI}(f^r)=n/2$，其中 $f^r(x)=f(x_1\oplus 1,x_2\oplus 1,\cdots,x_n\oplus 1)$。

2 预备知识

一个 n 元布尔函数 f 是从 $F_2^n\to F_2$ 的一个映射。B_n 表示全体 n 元布尔函数的集合。任一 n 元布尔函数 $f(x)$ 均可化为如下形式的多项式

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

其中，“$\oplus$”表示 F_2 上的加，$\lambda_u\in F_2$，$u=(u_1,u_2,\cdots,u_n)\in F_2^n$。称上式为函数 $f(x)$ 的代数标准型或者代数正规型（ANF）。定义函数 $f(x)$ 的代数次数为 $\max\{wt(u)\mid\lambda_u\neq 0\}$，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 元布尔函数的支撑集定义为：$\mathrm{supp}(f)=\{x\mid f(x)=1,x\in F_2^n\}$。函数 f 的 Hamming 重量 $wt(f)$ 等于其支撑集的元素个数。如果 $wt(f)=2^{n-1}$，则函数 f 为平衡的。2 个 n 元布尔函数 f 和 g 之间的 Hamming 距离为 $wt(f\oplus g)$。n 元布尔函数 f 的非线性度 $nl(f)$ 是函数 f 与所有的 n 元仿射函数之间的 Hamming 距离的最小值。布尔函数的非线性度可以用其 Walsh 谱值来刻画。给定 $f(x)\in B_n$，$\alpha\in F_2^n$，函数 $f(x)$ 其点 α 处的 Walsh 谱值定义为

$$W_f(\alpha)=\sum_{x\in F_2^n}(-1)^{f(x)+\alpha x}$$

则 $f(x)$ 的非线性度可以表示为

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

令 $f(x),g(x)\in B_n$，如果 $f\times g=0$，称 g 是 f 的零化子。函数 f 所有零化子的集合记作

$$Ann(f)=\{g\in B_n[x]\mid f\times g=0,g\neq 0\}$$

函数 f 的代数免疫度定义为：$\mathrm{AI}(f)=\min\{d\mid d=\deg(g),\ g\in Ann(f)\cup Ann(f\oplus 1)\}$[1]。

定义 1[10] 给定 $f(x)\in B_n$，$x=(x_1,x_2,\cdots,x_n)\in F_2^n$，定义函数 $f(x)$ 的代数补元素为 $f^c(x)=f(x)\oplus\Delta(x)$，其中，$\Delta(x)=(1\oplus x_1)(1\oplus x_2)\cdots(1\oplus x_n)$。

由于 $f^c(x)$ 和 $f(x)$ 只在零点函数值不同，所以 $|nl(f)-nl(f^c)|\leqslant 1$。因此，$f^c(x)$ 和 $f(x)$ 在抵抗线性攻击方面表现相当，故着重考虑它们抵抗代数攻击的能力。

定义 2[10] 给定 $f(x)\in B_n$，定义函数 $f(x)$ 的扩展代数免疫度(EAI)如下：$\mathrm{EAI}(f)=\min\{\mathrm{AI}(f),\mathrm{AI}(f^c)\}$。

由于奇变元布尔函数不可能达到最大 EAI[11]，故着重考虑偶变元布尔函数的 EAI。

文献[11]证明了 EAI 具有以下一些性质。

引理 1[11] 给定 $f(x)\in B_n$，n 是偶数，$n=2k$，且 $\mathrm{AI}(f)=n/2$，则有：

1) 如果 $f(0)=0$，且 $wt(f)=\sum_{i=0}^{n/2}\binom{n}{k}$，则 $\mathrm{EAI}(f)=k-1$；

2) 如果 $f(0)=1$，且 $wt(f)=\sum_{i=0}^{n/2-1}\binom{n}{k}$，则 $\mathrm{EAI}(f)=k-1$。

3 主要结果

3.1 一类具有最大 EAI 的布尔函数

最近，基于函数的单变量多项式表示，人们构造了很多具有最大 AI 的布尔函数[4]。任一函数 $f:F_{2^n}\to F_{2^n}$ 都可以唯一的表示成一个多项式 $\oplus_{i=0}^{2^n-1}a_ix^i$，其中 $a_i\in F_{2^n}$，众所周知，f 是布尔函数

当且仅当 $f(x)=(f(x))^2 \bmod (x^{2^n}-x)$，也即 $a_0,a_{2^n-1}\in F_2, \forall 1\leqslant i\leqslant 2^n-2, a_{2i \bmod (2^n-1)}=a_i^2$。

定理 1　设 n 是偶数，令 $n=2k\geqslant 4$，$f(x)\in B_n$，α 是域 F_{2^n} 上的一个本原元。如果函数 $f(x)$ 满足 $\mathrm{supp}(f(x))\supseteq\{\alpha^j,\alpha^{j+1},\cdots,\alpha^{j+D-1}\}$ 和 $\mathrm{supp}(f(x)\oplus 1)\supseteq\{\alpha^j,\alpha^{j+1},\cdots,\alpha^{j+D-1}\}$，那么 $f(x)$ 具有最大 EAI，其中 $D=\sum_{i=0}^{k-1}\binom{n}{i}$。

证明　函数 $f(x)$ 具有最大 AI 的证明在文献[4]中已给出，为了完整性，给出证明如下。设 $g(x)\in B_n$ 是函数 $f(x)$ 的零化子，且 $\deg(g)<k$，$g(x)$ 可以表示为

$$g(x)=\oplus_{i=0}^{2^n-1}a_i x^i, a_i=0, \forall wt(i)\geqslant k$$

不失一般性，假设 $\alpha_i\neq 0$ 当且仅当 $i\in\{i_1,i_2,\cdots,i_m\}$，其中，$m\leqslant D$。由于 $\mathrm{supp}(f(x))\supseteq\{\alpha^i,\alpha^{i+1},\cdots,\alpha^{i+D-1}\}$，所以对于任意 $x\in\{\alpha^i,\alpha^{i+1},\cdots,\alpha^{i+D-1}\}$，$g(x)=0$。用矩阵表示为 $\boldsymbol{B}\times\gamma=0$，其中 $\gamma=(a_{i_1},a_{i_2},\cdots,a_{i_m})$

$$\boldsymbol{B}=\begin{pmatrix}\alpha^{ii_1} & \alpha^{ii_2} & \cdots & \alpha^{ii_m}\\ \alpha^{(i+1)i_1} & \alpha^{(i+1)i_2} & \cdots & \alpha^{(i+1)i_m}\\ \cdots & \cdots & \cdots & \cdots\\ \alpha^{(i+D-1)i_1} & \alpha^{(i+D-1)i_2} & \cdots & \alpha^{(i+D-1)i_m}\end{pmatrix}$$

称矩阵 $\boldsymbol{B}$ 为 $\{\alpha^i,\alpha^{i+1},\cdots,\alpha^{i+D-1}\}$ 的相伴矩阵。设 $\boldsymbol{B'}=\boldsymbol{B}(1,2,\cdots,m)$，其中，$\boldsymbol{B}(1,2,\cdots,m)$ 表示矩阵 $\boldsymbol{B}$ 的前 m 行。因为 $\boldsymbol{B'}$ 是一个范德蒙矩阵，$\det(\boldsymbol{B'})\neq 0$。所以对于每个 $i\in\{i_1,i_2,\cdots,i_m\}$，$a_i=0$，故 $g(x)=0$。所以 $f(x)$ 不存在次数小于 k 的零化子。类似的，$f(x)\oplus 1$ 不存在次数小于 k 的零化子。综上，$\mathrm{AI}(f(x))=k=n/2$。由于 $\mathrm{supp}(f^c(x))\supseteq\{\alpha^j,\alpha^{j+1},\cdots,\alpha^{j+D-1}\}$ 且 $\mathrm{supp}(f^c(x)\oplus 1)\supseteq\{\alpha^j,\alpha^{j+1},\cdots,\alpha^{j+D-1}\}$，则由以上的证明可以看出 $\mathrm{AI}(f^c(x))=k=n/2$，于是，$\mathrm{EAI}(f)=n/2$，证毕。

注 1：定理 1 中函数的支撑集是由本原元 α 的连续幂次组成的。事实上，如果 $\mathrm{supp}(f(x))$ 和 $\mathrm{supp}(f(x)\oplus 1)$ 的相伴矩阵都是满秩的，则定理 1 依然成立。

注 2：文献[12]和定理 3 是定理 1 的特例。

文献[6]构造了两类具有最大 AI 的平衡布尔函数，文献[13]证明了文献[6]中构造的第一类函数和文献[4]中构造的函数是等价的。由定理 1，针对文献[6]中的第一类函数有如下推论。

推论 1　设 $p(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+1$ 是域 F_2 上的本原多项式，其伴随矩阵 $\boldsymbol{A}$ 为

$$\boldsymbol{A}=\begin{pmatrix}0 & 0 & \cdots & 0 & 1\\ 1 & 0 & \cdots & 0 & c_1\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & c_{n-1}\end{pmatrix}$$

定义函数 $f(x)\in B_n$，$\mathrm{supp}(f(x))\supseteq\{A^ib_1,A^{i+1}b_1,\cdots,A^{i+D-1}b_1\}$，函数 $f(x)\oplus 1$ 的支撑集 $\mathrm{supp}(f(x)\oplus 1)\supseteq\{A^jb_1,A^{j+1}b_1,\cdots,A^{j+D-1}b_1\}$，其中，$n=2k$，$D=\sum_{i=0}^{k-1}\binom{n}{i}$，$0\neq b_1\in F_2^n$。那么函数 $f(x)$ 具有最大 EAI。

3.2　对称布尔函数的扩展代数免疫度

对称布尔函数是指其函数值只取决于其自变量的 Hamming 重量的布尔函数。对称布尔函数由于其结构简单，易于硬件实现，所以一直是研究的热点。令 SB_n 为全体 n 元对称布尔函数的集合。给定一个对称布尔函数 $f(x)$，它可以由其特征向量

$$\boldsymbol{v}_f=(v_f(0),v_f(1),\cdots,v_f(n))\in F_2^{n+1}$$

表示，其中 $v_f(i)=f(x), wt(x)=i, x\in F_2^n$。

文献[14, 15]证明了对于奇数 $n\geqslant 3$，只有 $f(x)$ 和 $f(x)$+1　2 个 n 元对称布尔函数具有最大代数免疫度 $(n+1)/2$，其中

$$f(x)=\begin{cases}0, wt(x)\geqslant (n+1)/2\\ 1, wt(x)\geqslant (n-1)/2\end{cases}$$

由于奇变元布尔函数不可能达到最大 EAI，所以 $\mathrm{EAI}(f(x))=(n-1)/2$。因此，本节只考虑具有最大 AI 的偶元对称布尔函数的 EAI，并给出所有的达到最大 EAI 的对称布尔函数。

文献[16]构造出了所有的具有最大 AI 的偶元对称布尔函数。令 $n=2k\geqslant 4$，$k=(k_m,\cdots,k_1,k_0)_2$，$m=\lfloor \mathrm{lb}k \rfloor$，即 k_m=1。定义 $k(p)=(k_{p-1},\cdots,k_1,k_0)_2$，$1\leqslant p\leqslant m$，$k(0)=0$。把 $\{0,1,\cdots,n\}$ 分为 $m+2$ 个互不相交的集合 $A_0^k,\cdots,A_{m+1}^k$，即

$$\{0,1,\cdots,n\}=\prod_{i=0}^{m+1}A_i^k, A_i^k\cap A_j^k=\varnothing, 0\leqslant i<j\leqslant m+1$$

令 $A_0^k=\{k\}$，对于 $i\geqslant 1$，定义

$$A_i^k=\{x=(x_{m+1},\cdots,x_1,x_0)_2\mid (x_{i-1},\cdots,x_1,x_0)=(k_{i-1},\cdots,k_1,k_0), x_i\neq k_i, x\leqslant n\}$$

A_i^k 也可以表示为

$$A_i^k=\{k-2^i j+2^{i-1},k+2^i j-2^{i-1}\,|\,1\leqslant j\leqslant\left\lfloor\frac{k/2^{i-1}+1}{2}\right\rfloor\}$$

构造 1[16] 令 $I_k=\{p\,|\,k_p=1\}$，给定 $f\in SB_n$，任给 $m+2$ 个元素 $a_0,a_1,\cdots,a_{m+1}\in F_2$ 则 $\mathrm{AI}(f)=k$ 当且仅当 f 属于以下三类函数之一。

Class 1 令 $v_f(k)=a_0$。对于每一个 $1\leqslant t\leqslant m+1$，有 $v_f(i)=a_t=v_f(j)\oplus 1$，其中 $i,j\in A_t$，$i<k<j$。

Class 2 对于每一个 $1\leqslant t\leqslant m$，有 $v_f(i)=a_t=v_f(j)\oplus 1$，其中的 $i,j\in A_t$，$i<k<j$。此外，函数 f 还满足

$$v_f(k(m))\oplus 1=v_f(k)=a_0=v_f(n-k(m))\oplus 1。$$

Class 3 选择 $p\in I_k$，且 $p\neq m$。对于每一个 $1\leqslant t\leqslant m+1$，有 $v_f(i)=a_t=v_f(j)\oplus 1$，其中的 $i,j\in A_t$，$i<k<j$，且 $i\neq k(p),j\neq n-k(p)$。与第二类类似，函数 f 还满足

$$v_f(k(p))\oplus 1=v_f(k)=a_0=v_f(n-k(p))\oplus 1。$$

很容易看出以上三类对称布尔函数的个数分别是 2^{m+2}、2^{m+1} 和 $(wt(n)-1)2^{m+2}$。

定理 2 令 $n=2k\geqslant 4$，在所有 $(2wt(n)+1)2^{m+1}$ 个具有最大 AI 的对称布尔函数中，有 2^{m+2} 个函数具有最大 EAI。在这 2^{m+2} 个具有最大 EAI 的对称函数中，2^{m+1} 个函数具有性质：$\mathrm{EAI}(f^r)=k$，其中 $f^r(x)=f(x_1+1,x_2+1,\cdots,x_n+1)$。

证明 给定 $f\in SB_n$，则 f^r 和 $f^{rc}\in SB_n$，其中 $f^{rc}=(f^r)^c=f^r+\Delta(x)$。

在 Class 1 中，需要考虑 4 种情况。

1) $v_f(k)=1$ 和 $v_f(0)=0$，此种情况有 $wt(f)=2^{n-1}+\frac{1}{2}\binom{n}{k}$，则由引理 1 的第 1)条可知 $\mathrm{EAI}(f)=k-1$。

2) $v_f(k)=0$ 和 $v_f(0)=1$，类似第 1)种情况可知 $\mathrm{EAI}(f)=k-1$。

3) $v_f(k)=1$ 和 $v_f(0)=1$，容易得出 $v_f(0)=v_f(k)=v_f(n)+1$ 和 $v_{f^c}(0)=v_{f^c}(k)\oplus 1=v_{f^c}(n)$。如果 $k=2^m$，可以看出 $f^c\in$ Class 2；如果 $k\neq 2^m$，则 $f^c\in$ Class 3，所以 $\mathrm{AI}(f^c)=k$，故有 $\mathrm{EAI}(f)=k$。但是注意到 $v_{f^{rc}}(0)=v_{f^{rc}}(k)=v_{f^{rc}}(n)$，易知 f^{rc} 不属于构造 3.1 三类函数中的任何一类，故 $\mathrm{EAI}(f^r)=k-1<k$。

4) $v_f(k)=0$ 和 $v_f(0)=0$，类似于第 3)种情况，有 $\mathrm{AI}(f^c)=k$，$\mathrm{EAI}(f)=k$ 和 $\mathrm{EAI}(f^r)=k-1<k$。

综合以上 4 种情况可以得出结论：在 Class 1 的 2^{m+2} 个函数中，有 2^{m+1} 个函数具有最大 EAI，没有函数满足 $\mathrm{EAI}(f^r)=k=\mathrm{EAI}(f)$。

在 Class2 中，有 2 种情况需要考虑。

1) $k=2^m$ 由第二类函数的定义可知 $v_f(0)=v_f(k)\oplus 1=v_f(n)$，$v_{f^c}(0)\oplus 1=v_{f^c}(k)\oplus 1=v_{f^c}(n)$，可以看出 $f^c\in$ Class 1，$\mathrm{AI}(f^c)=k$，故 $\mathrm{EAI}(f)=k$。同时，容易看出 $\mathrm{EAI}(f^r)=k$。

2) $k\neq 2^m$ 此种情况下有 $v_f(k(m))\oplus 1=v_f(k)=v_f(n-k(m))\oplus 1$ 和 $v_f(0)=v_f(n)\oplus 1$，于是 $v_{f^c}(k(m))\oplus 1=v_{f^c}(k)=v_{f^c}(n-k(m))\oplus 1$，$v_{f^c}(0)=v_{f^c}(n)$。由于 $k\neq 2^m$，故 $k(m)\neq 0$，可以看出 f^{rc} 不属于构造 3.1 中的任何一类函数，故 $\mathrm{AI}(f^c)=k-1$，$\mathrm{EAI}(f)=k-1$。综合来看，Class 2 中的函数满足 $\mathrm{EAI}(f)=k$ 当且仅当 $k=2^m$。

在 Class 3 中，考虑以下 2 种情况。

1) $k=2^m$ 此时，$wt(n)=1$，Class 3 中的函数个数是 0。

2) $k\neq 2^m$ 令 l 是 I_k 中最小的元素，显然 $l\neq m$。证明函数 $f^c(x)$ 达到最大 AI 当且仅当以下 2 个条件同时满足。

① $p=l$。

② 令 A_t 是包含 0 的元素集合，如果 Class 3 中的函数满足，对于任意的 $i,j\in A_t$，$0<i<k<j<n$，下式成立：$v_f(0)\oplus 1=v_f(i)=a_t=v_f(j)\oplus 1=v_f(n)\oplus 1$。

如果 $p\neq l$，则有 $v_f(k(p))\oplus 1=v_f(k)=v_f(n-k(p))\oplus 1$ 和 $v_f(0)\oplus 1=v_f(n)$，于是 $v_{f^c}(k(m))\oplus 1=v_{f^c}(k)=v_{f^c}(n-k(m))\oplus 1$，$v_{f^c}(0)=v_{f^c}(k)\oplus 1=v_{f^c}(n)$，可看出函数 $f^c(x)$ 不属于构造 3.1 中的任何一类函数，故而 $\mathrm{AI}(f^c)=k-1$，$\mathrm{EAI}(f)=k-1$。当 $p=l$ 时，$k(p)=k(l)=0$，易知 $v_f(0)=v_f(k)\oplus 1=v_f(n)$，$v_{f^c}(0)=v_{f^c}(k)=v_{f^c}(n)\oplus 1$ 和 $v_{f^c}(k(m))=v_{f^c}(n-k(m))\oplus 1$，所以 $f^c(x)$ 不属于 Class 2 和 Class 3。令 A_t 是包含 0 的元素集合，为了保证 f^c 属于 Class 1，

对于任意的 $i,j\in A_t$，$i<k<j$，f^c 需要满足 $v_{f^c}(i)=a_t=v_{f^c}(j)\oplus 1$，这与条件②是等价的。注意到如果 $0\in A_t$，则有 $n\in A_t$，则易知如果 Class 3 中的函数同时满足条件①和②，则函数 f 达到最大的扩展代数免疫度，且有 $\mathrm{EAI}(f^r)=k=\mathrm{EAI}(f)$。

综合对 Class 3 的分析，这类函数中共有 2^{m+1} 个函数达到最大扩展代数免疫度。

从以上对三类具有最大 AI 的布尔函数的 EAI 分析可以看出，$(2wt(n)+1)2^{m+1}$ 个具有最大 AI 的对称布尔函数中，仅有 2^{m+2} 个函数具有最大 EAI。在这 2^{m+2} 个具有最大 EAI 的对称函数中，2^{m+1} 个函数具有性质 $\mathrm{EAI}(f^r)=k$，证毕。

4　结束语

由于 2 个布尔函数的代数免疫度仅相差 1，对代数攻击的效率影响很大，所以 EAI 在构造布尔函数时必须考虑。结果无论对于进一步分析其他具有最大 AI 的布尔函数的 EAI，还是构造具有最大 EAI 的布尔函数都很有意义。目前还有很多关于 EAI 的问题值得研究。例如，EAI 和非线性度、相关免疫度之间的关系，如何构造更多具有最大 EAI 的函数，如何更直观的刻画 $\mathrm{EAI}(f)=\mathrm{AI}(f)$ 的充分必要条件等。

参考文献：

[1] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedback[A]. Advances in Cryptology-Eurocrypt 2003, LNCS 2656[C]. Berlin, 2003.345-359.

[2] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[A].Advances in Cryptology-Eurocrypt 2004, LNCS 3027[C]. Berlin, Springer-Verlag, 2004.474-491.

[3] CARLET C. Constructing balanced functions with optimal algebraic immunity[A]. IEEE ISIT 2007[C]. Nice, France, 2007.451-455.

[4] CARLET C, FENG K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity[A]. Advances in Cryptology-Asiacrypt 2008, LNCS 5350[C]. Berlin: Springer-Verlag, 2008.425-440.

[5] DALAI D, MAITRA S, SARKAR S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J] . Des. Codes Cryptogr, 2006, 40(1):41-58.

[6] WANG Q, PENG J, KAN H, *et al*. Constructions of cryptographically significant Boolean functions using primitive polynomials[J]. IEEE Trans Inf Theory, 2010, 56(6):3048-3053.

[7] TU Z, DENG Y. A conjecture on binary string and its applications on constructing Boolean functions of optimal algebraic immunity[J]. Des. Codes Cryptogr, 2011, 60(1): 1-14.

[8] TANG D, CARLET C, TANG X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks[J]. IEEE Trans Inf Theory, 2013, 59(1):653-664.

[9] 李雪莲，胡予濮. 对具有高代数免疫度布尔函数的新型代数攻击[J]. 西安电子科技大学学报, 2009, 36(4): 702-707.
LI X L, HU Y P. Algebraic attack on symmetric Boolean functions with a high algebraic immunity[J]. Journal of Xidian University, 2009, 36(4): 702-707.

[10] ZHANG X, PIEPRZYK J, ZHENG Y. On algebraic immunity and annihilators[A]. ICISC 2006, LNCS 4296[C]. Berlin, Springer-Verlag, 2004.65-80.

[11] WANG C, CHEN X. On extended algebraic immunity[J]. Des Codes Cryptogr, 2010, 57(3):271-281.

[12] 熊晓雯, 屈龙江, 李超. 布尔函数的扩展代数免疫度[J] . 电子与信息学报, 2011, 33(2): 284-288.
XIONG X W, QU L J, LI C. On extended algebraic immunity of Boolean functions[J]. Journal of Electronics & Information Technology, 2011, 33(2): 284-288.

[13] CARLET C. Comment on constructions of cryptographically significant Boolean functions using primitive polynomials[J]. IEEE Trans Inf Theory, 2011, 57(7): 4852-4853.

[14] LI N, QI W. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity[J]. IEEE Trans Inf Theory, 2006, 52(5): 2271-2273.

[15] QU L, LI C, FENG K. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables[J]. IEEE Trans Inf Theory, 2007, 53(8): 2908-2910.

[16] PENG J, WU Q, KAN H. On symmetric Boolean functions with high algebraic immunity on even number of variables[J]. IEEE Trans Inform Theory, 2011, 57(10):7205-7220.

作者简介：

伍高飞（1987-），男，河南灵宝人，西安电子科技大学博士生，主要研究方向为序列设计、密码学。

刘雪峰（1985-），男，安徽亳州人，博士，西安电子科技大学讲师，主要研究方向为应用密码、安全协议设计。

田叶（1987-），女，山西平遥人，西安电子科技大学博士生，主要研究方向为流密码的分析及攻击。

张玉清（1966-），男，陕西宝鸡人，西安电子科技大学教授、博士生导师，主要研究方向为网络攻防与系统攻防、密码学及其应用。